# Die Ramanujankonstante
# Sommersemester 2010

Hendrik Kasten

26. September 2018

## 0 Einleitung

Im Jahr 1934 zeigten Gelfond und Schneider (s. [Schn]) unabhängig voneinander den

**Satz von Gelfond-Schneider** *Für zwei algebraische Zahlen $\alpha, \beta$ mit $\alpha \notin \{0,1\}$ und $\beta \notin \mathbb{Q}$ ist $\alpha^\beta$ transzendent.*

Daraus folgt unmittelbar die Transzendenz von

$$2^{\sqrt{2}} \quad \text{und} \quad e^\pi = e^{i(-i)\pi} = (-1)^{-i},$$

was das 7. Problem auf Hilberts berühmter Liste aus dem Jahr 1900 löste. Weniger berühmt aber genauso richtig folgt die Transzendenz der ***Ramanujankonstante*** $e^{\sqrt{163}\pi} = (-1)^{-\sqrt{-163}}$, einer Zahl, die geradezu heimtückisch nahe an der ganzen Zahl 262.537.412.640.768.744 liegt. Genauer gilt

**Hauptbehauptung**

$$262.537.412.640.768.744 - e^{\sqrt{163}\pi} < 10^{-12}.$$

Diese Tatsache lässt sich natürlich numerisch auf einem modernen Computer in Sekundenbruchteilen beweisen. Unser Ziel ist daher auch nicht, die Hauptbehauptung einfach nur irgendwie zu zeigen, sondern vielmehr einen Beweis zu finden, der uns eine strukturelle Erklärung für die Fast-Ganzheit der Ramanujankonstante gibt.

Und tatsächlich liefern uns das Studium von Modulformen und der Theorie der komplexen Multiplikation elliptischer Kurven eine solche befriedigende Antwort. Die Strategie ist dabei die folgende: Zunächst zeigen wir durch Abschätzen von Fourierkoeffizienten, dass sich $e^{\sqrt{163}\pi}$ um weniger als $10^{-12}$ vom Funktionswert der Modulfunktion $j(z)$ an der Stelle $\frac{1+\sqrt{-163}}{2}$ unterscheidet. Es stellt sich heraus, dass $j(z)$ in einem engen Zusammenhang zu elliptischen Kurven steht, genauer ist der untersuchte Funktionswert gerade die so genannte $j$-Invariante einer elliptischen Kurve mit Endomorphismenring $\mathbb{Z}[\frac{1+\sqrt{-163}}{2}]$. Die Hauptbehauptung folgt schließlich, da die $j$-Invariante von elliptischen Kurven, deren Endomorphismenring der Ganzheitsring eines imaginärquadratischen Zahlkörpers mit Klassenzahl 1 ist, ganzzahlig ist.

Der Name „Ramanujankonstante“ entstand übrigens im Jahr 1975 im Rahmen eines Aprilscherzes in einem Artikel des Scientific American, siehe [Gar]. Der Autor, M. Gardner, behauptete dort unter anderem, Ramanujan hätte 1914 die Ganzheit von $e^{\sqrt{163}\pi}$ gezeigt und veröffentlicht. Das tut gleich zwei bekannten Mathematikern unrecht: Zum einen hat Ramanujan natürlich nie diese falsche Behauptung aufgestellt, zum anderen ist die Fast-Ganzheit von $e^{\sqrt{163}\pi}$ schon 1859 von Hermite entdeckt worden. Der Name blieb jedoch haften und ist auch nicht komplett unpassend, da sich Ramanujan in [Ram] tatsächlich intensiv mit ganz ähnlichen Fragestellungen beschäftigt hat. Genauer hat Ramanujan aus der Fast-Ganzheit von $e^{\sqrt{58}\pi}$ gute Näherungen von $\pi$ hergeleitet, was auf $e^{\sqrt{163}\pi}$ übertragen wie folgt funktioniert:

Aus der Hauptbehauptung folgt unmittelbar, dass

$$\frac{\log((640320)^3+744)}{\sqrt{163}}$$

eine plausible Näherung für $\pi$ sein muss. In der Tat ist sie auf 30 Nachkommastellen genau. Die Folge

$$\frac{\log(n\lfloor e^{\sqrt{163n}\pi}\rfloor)}{\sqrt{163n}}$$

konvergiert gegen $\pi$ und approximiert es auf $d(n)$ Nachkommastellen genau mit

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $d(n)$ | 30 | 28 | 31 | 46 | 40 | 44 | 48 | 51 | 61 | 57 | 59 | 62 |

## 1 Modulformen

Die Behauptung ist ja, die Fastganzheit der Ramanujankonstante habe etwas mit einer bestimmten Funktion $j(z)$ auf der oberen komplexen Halbebene zu tun. Bevor wir jedoch diese Funktion einführen, wollen wir an das Konzept der Modulformen zur vollen Modulgruppe $\mathrm{SL}_2(\mathbb{Z})$ erinnern und führen alle wichtigen Begriffe in einem Schnelldurchlauf noch einmal ein.

Für eine invertierbare komplexe $(2\times 2)$-Matrix $\gamma := \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$ betrachten wir die Möbiustransformation

$$z \mapsto \gamma(z) = \frac{az+b}{cz+d}.$$

Wie man leicht zeigt, ist diese ein Automorphismus sowohl von der komplexen oberen Halbebene $\mathbb{H} := \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ als auch von $\mathbb{P}^1(\mathbb{R}) := \mathbb{R}\cup\{\infty\}$. Klar, dass $\mathrm{SL}_2(\mathbb{Z})$ so auf $\mathbb{H}^* := \mathbb{H}\cup\mathbb{P}^1(\mathbb{Q}) = \mathbb{H}\cup\mathbb{Q}\cup\{\infty\}$ operiert. Für den ***Automorphiefaktor*** $(cz+d)$ bezüglich dieser Operation schreibt man auch $j(\gamma,z)$.

Eine ***Modulform*** von Gewicht $k \in \mathbb{Z}$ zur vollen Modulgruppe $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$ ist nun eine holomorphe Funktion auf $\mathbb{H}^*$ mit

$$(f|_k\gamma)(z) := j(\gamma,z)^{-k} f(\gamma(z)) = f(z) \quad \text{für alle } \gamma \in \Gamma(1). \tag{1}$$

Die Holomorphie in den ***Spitzen*** $s \in \mathbb{P}^1(\mathbb{Q})$ erklärt sich hierbei wie folgt. Wegen $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right) \in \Gamma(1)$ und (1) ist jede Modulform $f$ invariant unter der Translation $z \mapsto z+1$ und besitzt daher eine Fourierentwicklung im Punkt $\infty$ der Art

$$f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z} \quad \text{mit } a_n \in \mathbb{C}.$$

Aufgefasst als holomorphe Funktion in $q := e^{2\pi i z}$ konvergiert diese in der punktierten komplexen Einheitskreisscheibe. Unsere Forderung nach Holomorphie von $f(z)$ in $\infty$ ist nun nichts weiter als die Forderung nach holomorpher Fortsetzbarkeit von $f(q)$ nach $q = 0$. Die Holomorphie von $f(z)$ in einer rationalen Zahl $r$ ist nun nichts weiter als die Holomorphie von $f(\gamma_r(z))$ in $\infty$, wo $\gamma_r \in \Gamma(1)$ die Spitze $r$ nach $\infty$ abbilde. Letzteres ist übrigens keine neue Forderung, da $\Gamma(1)$ auf $\mathbb{P}^1(\mathbb{Q})$ operiert und $f$ unter dieser Operation invariant ist.

Wie üblich bezeichnen wir den Raum der Modulformen von Gewicht $k$ mit $M_k$ und den Unterraum der Spitzenformen von Gewicht $k$, also derjenigen Modulformen, die in den Spitzen den Wert 0 annehmen, mit $S_k$. Aus der Definition der Modulformen folgt unmittelbar

$$\begin{aligned} f, g \in M_k \text{ bzw. } S_k &\Longrightarrow f + g \in M_k \text{ bzw. } S_k, \\ f \in M_k, g \in M_\ell &\Longrightarrow f \cdot g \in M_{k+\ell}, \\ f \in S_k, g \in S_\ell &\Longrightarrow f \cdot g \in S_{k+\ell}, \end{aligned}$$

so dass die Mengen $M$ der Modulformen bzw. $S$ der Spitzenformen zur vollen Modulgruppe $\Gamma(1)$ die Struktur einer Algebra tragen.

Besonders interessante Modulformen sind (für $k \geq 4$) die ***Eisensteinreihen***

$$G_k(z) := \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ (c,d)\neq(0,0)}} (cz+d)^{-k} \quad \in M_k \tag{2}$$

und die ***Diskriminante***

$$\Delta(z) = (60G_4)^3 - 27(140G_6)^2 \in S_{12}.$$

Ein Grund dafür ist, dass die Algebra $M$ von $G_4$ und $G_6$ erzeugt wird (das ist der ***Struktursatz***), was zusammen mit der wichtigen ***Valenzformel***

$$\operatorname{ord}_\infty f + \frac{1}{2}\operatorname{ord}_i f + \frac{1}{3}\operatorname{ord}_{e^{2\pi i/3}} + \sum_{\substack{z\in\Gamma(1)\backslash\mathbb{H} \\ z\not\sim i, e^{2\pi i/3}}} \operatorname{ord}_z f = \frac{k}{12} \quad \text{für alle } f \in M_k$$

auf die ***Dimensionsformel***

$$\dim_{\mathbb{C}}(M_k) = \begin{cases} \lfloor \frac{k}{12} \rfloor & \text{für } k > 0 \text{ und } k \equiv 2 \bmod (12), \\ \lfloor \frac{k}{12} \rfloor + 1 & \text{für } k > 0 \text{ und } k \equiv 0,4,6,8,10 \bmod (12), \\ 0 & \text{sonst} \end{cases}$$

führt. Man kann nun noch zeigen, dass die Multiplikation mit $\Delta(z)$ ein Isomorphismus zwischen $M_{k-12}$ und $S_k$ ist; insbesondere gilt $\dim_{\mathbb{C}}(S_k) = \dim_{\mathbb{C}}(M_{k-12})$.

Für den Rest dieses Abschnitts wollen wir nun die oben eingeführten Modulformen $G_k$ und $\Delta$ genauer kennenlernen; wir werden noch einiges Wissen über sie benötigen. Zunächst interessieren wir uns für die Fourierentwicklung der Eisensteinreihen.

**Proposition 1.1** *Für $k \geq 2$ gilt*

$$G_{2k}(z) = 2\zeta(2k) + 2\frac{(2\pi i)^{2k}}{(2k-1)!}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n,$$

*wo $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ die Riemann'sche Zetafunktion und $\sigma_{2k-1}(n) = \sum_{d|n} d^{2k-1}$ die $(2k-1)$-te Teilersumme ist. Insbesondere gilt*

$$G_4(z) = 2 \cdot \frac{\pi^4}{90}\left(1 + 24q + 2160q^2 + \dots\right)$$
$$G_6(z) = 2 \cdot \frac{\pi^6}{945}\left(1 - 504q - 16632q^2 \dots\right).$$

*Beweis.* Aus der Funktionentheorie bekannt sein sollte die Partialbruchzerlegung des Kotangens

$$\pi\cot(\pi z) = \sum_{m\in\mathbb{Z}}\frac{1}{m+z} \quad \text{für alle } z \in \mathbb{C}\setminus\mathbb{Z}.$$

Andererseits lässt sich der Kotangens über die bekannten Reihen von Sinus und Kosinus leicht nach $q = e^{2\pi i z}$ entwickeln, wobei man

$$\pi\cot(\pi z) = \pi i - 2\pi i\sum_{n\geq 0} q^n$$

erhält. Setzen wir diese beiden Darstellungen gleich und leiten $k-1$ Mal ab, so erhalten wir

$$\sum_{m\in\mathbb{Z}}\frac{1}{(m+z)^k} = \frac{(-2\pi i)^k}{(k-1)!}\sum_{n\geq 1} n^{k-1}q^n. \tag{3}$$

Vergleichen wir dies nun mit der Definition der Eisensteinreihe $G_{2k}$, so folgt

$$\begin{aligned} G_{2k}(z) &= 2\zeta(2k) + 2\sum_{n=1}^{\infty}\sum_{m\in\mathbb{Z}}(mz+n)^{-2k} \\ &\overset{(3)}{=} 2\zeta(2k) + 2\cdot\frac{(-2\pi i)^{2k}}{(2k-1)!}\sum_{d=1}^{\infty}\sum_{a=1}^{\infty} d^{2k-1}q^{ad} \\ &= 2\zeta(2k) + 2\cdot\frac{(-2\pi i)^{2k}}{(2k-1)!}\sum_{n\geq 1}\sigma_{k-1}(n)q^n. \end{aligned}$$

□

Ganz mechanisch lässt sich daraus auch die Fourierentwicklung

$$\Delta(z) = (2\pi)^{12}(q - 24q^2 + 252q^3 + \dots)$$

gewinnen. Wir wollen aber noch mehr über die Diskriminante erfahren. Sie hat nämlich folgende Produktentwicklung:

**Proposition 1.2**

$$\Delta(z) = (2\pi)^{12} q \prod_{n=1}^{\infty} (1-q^n)^{24} \quad \text{für alle } z \in \mathbb{H}.$$

*Beweis.* Wir halten uns an eine Arbeit von Kohnen (siehe [Koh]). Sei $M(m)$ für $m \in \mathbb{N}$ die Menge aller $\gamma \in \mathbb{Z}^{2\times 2}$ mit Determinante $m$. Dann ist

$$\{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid ad = m,\ d > 0,\ b \bmod (d)\}$$

ein Vertretersystem von $\Gamma(1)\backslash M(m)$ (Übung!), insbesondere ist $|\Gamma(1)\backslash M(m)| = \sigma_1(m)$.

Für $f \in M_k$ setzen wir nun

$$M_m(f) := \prod_{\gamma \in \Gamma(1)\backslash M(m)} f|_k\gamma,$$

wo $M(m)$ via $(f|_k\gamma)(z) = (\det\gamma)^{k/2} j(\gamma,z)^{-k} f(\gamma(z))$ operiert. $M_m(f)$ ist wohldefiniert und eine Modulform in $M_{k\sigma_1(m)}$,

*denn:* Die Funktion $M_m(f)$ ist unabhängig von der Wahl des Vertretersystems von $\Gamma(1)\backslash M(m)$, denn für $g \in \Gamma(1)$ gilt wegen der Modularität von $f$

$$f|_k(g\gamma) = (f|_k g)|_k\gamma = f|_k\gamma.$$

Zur Überprüfung der Modularität von $M_m(f)$ berechnen wir für $g \in \Gamma(1)$

$$\begin{aligned} M_m(f)(gz) &= \prod_{\gamma \in \Gamma(1)\backslash M(m)} (\det\gamma)^{k/2} j(\gamma, gz)^{-k} f(\gamma(gz)) \\ &= \prod_{\gamma \in \Gamma(1)\backslash M(m)} (\det\gamma)^{k/2} j(\gamma g, z)^{-k} j(g,z)^k f((\gamma g)(z)) \\ &= j(g,z)^{\sigma_1(m)k} M_m(f)(z). \end{aligned}$$

Schließlich ist $M_m(f)$ mit $f$ offensichtlich auf $\mathbb{H}$ holomorph; die Holomorphie in $\infty$ gilt, da sämtliche Matrizen unseres Vertretersystems $\infty$ fix lassen. #

Betrachten wir nun speziell $f = \Delta$. Mit demselben Argument wie für die Holomorphie in $\infty$ gerade eben sehen wir $\mathrm{ord}_\infty(M_m(\Delta)) = \sigma_1(m)$, so dass wir aus der Valenzformel sofort folgern können, dass $M_m(\Delta)$ keine Nullstellen in $\mathbb{H}$ haben kann. Da es außerdem Gewicht $12\sigma_1(m)$ hat, ist $M_m(\Delta)$ proportional zu $\Delta^{\sigma_1(m)}$.[1] Es gibt also ein $c \in \mathbb{C}^\times$ mit

$$c\sigma_1(m)\Delta'\Delta^{\sigma_1(m)-1} = (c\Delta^{\sigma_1(m)})' = M_m(\Delta)' = (\prod_\gamma \Delta|_{12}\gamma)' = \sum_{\tilde\gamma} \prod_{\gamma\neq\tilde\gamma} \Delta|_{12}\gamma \cdot (\Delta|_{12}\tilde\gamma)' \qquad (4)$$

Dabei ist

$$(\Delta|_{12}\tilde\gamma)'(z) = -m^7 j(\tilde\gamma, z)^{-14} \Delta'(\tilde\gamma(z)). \qquad (5)$$

[1] Das kann man aus dem Beweis des Struktursatzes ablesen.

Dividieren wir (4) durch $c\Delta^{\sigma_1(m)} = \prod_\gamma \Delta|_{12}\gamma$, so erhalten wir

$$\sigma_1(m) \cdot \frac{\Delta'}{\Delta} = \sum_{\tilde\gamma} \Big( \prod_{\gamma \neq \tilde\gamma} \Delta|_{12}\gamma \cdot (\Delta|_{12}\tilde\gamma)' \Big) (\prod_\gamma \Delta|_{12}\gamma)^{-1} \overset{(5)}{=} \sum_\gamma (\frac{\Delta'}{\Delta})|_2\gamma.$$

Schreiben wir nun $\frac{\Delta'}{\Delta}(z) = 2\pi i \sum_{n=0}^\infty a_n q^n$, so gilt $\sigma_1(m) a_n = \sum_{d|\mathrm{ggT}(m,n)} d a_{\frac{mn}{d^2}}$,

*denn:*

$$\begin{aligned}
\left( \sum_\gamma (\frac{\Delta'}{\Delta})|_2\gamma \right)(z) &= \sum_{\substack{ad=m,\, d>0 \\ b \bmod (d)}} \left( (\frac{\Delta'}{\Delta})|_2 \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right)(z) \\
&= 2\pi i \sum_{\dots} \frac{m}{d^2} \sum_{n=0}^\infty a_n e^{2\pi i n \frac{az+b}{d}} \\
&= 2\pi i \sum_{ad=m,\, d>0} \frac{m}{d^2} \sum_{n=0}^\infty a_n q^{\frac{an}{d}} \sum_{b \bmod (d)} e^{2\pi i \frac{bn}{d}} \\
&= 2\pi i \sum_{ad=m,\, d>0} \frac{m}{d} \sum_{n=0}^\infty a_{dn} q^{an} \\
&= 2\pi i \sum_{ad=m,\, a>0} a \sum_{n=0}^\infty a_{\frac{mn}{a}} q^{an} \\
&= 2\pi i \sum_{r=0}^\infty \sum_{a>0,\, a|\mathrm{ggT}(m,r)} a \sum_{n=0}^\infty a_{\frac{rm}{a^2}} q^r.
\end{aligned}$$

Die Behauptung folgt per Koeffizientenvergleich. #

Für $n = 1$ ist insbesondere $a_m = \sigma_1(m) a_1$ für alle $m \in \mathbb{N}$. Mit den bekannten Fourierkoeffizienten von $\Delta$ berechnet man leicht $a_0 = 1$ und $a_1 = -24$, so dass folgt

$$\begin{aligned}
(\frac{\Delta'}{\Delta})(z) &= 2\pi i (1 - 24 \sum_{n=1}^\infty \sigma_1(n) q^n) \\
&= 2\pi i (1 - 24 \sum_{m=1}^\infty \sum_{n=1}^\infty m q^{mn}) \\
&= 2\pi i - 24 \sum_{m=1}^\infty \sum_{n=1}^\infty \frac{2\pi i m n q^{mn}}{n} \\
&= 2\pi i + 24 \sum_{m=1}^\infty \frac{d}{dz} \sum_{n=1}^\infty (-1)^{n+1} \frac{(-q^m)^n}{n}.
\end{aligned}$$

Leiten wir das nach $z$ auf, so erhalten wir äquivalent, dass es ein $c \in \mathbb{C}$ gibt mit

$$\log \Delta = \log q + 24 \sum_{n=1}^\infty \log(1 - q^n) + c.$$

In einer kleinen Umgebung der Eins argumentiert ist das äquivalent zur Behauptung der Proposition; die Konstante $c$ können wir dabei leicht aus einem speziellen Funktionswert als $12 \log(2\pi)$ bestimmen. □

## 2 Die *j*-Invariante

Wir interessieren uns nun für die ***j*-Invariante**

$$j(z) := \frac{1728 \cdot (60G_4)^3(z)}{\Delta(z)} = \frac{1728 \cdot (60G_4)^3(z)}{(60G_4)^3 - 27(140G_6)^2}. \tag{6}$$

Diese ist als Quotient holomorpher Funktionen eine meromorphe Funktion auf $\mathbb{H}$. Mit demselben Argument wie für $M_m(\Delta)$ im Beweis von Proposition 1.2 kann man zeigen, dass $\Delta$ in $\mathbb{H}$ keine Nullstellen hat, so dass $j$ sogar holomorph ist. Außerdem sieht man durch Verrechnen der Automorphiefaktoren der beteiligten Funktionen schnell, dass $j$ invariant unter $\Gamma(1)$ ist. Andererseits ist $\Delta$ eine Spitzenform und $G_4$ nicht, was die Vermutung nahelegt, $j$ habe einen Pol in $\infty$. In der Tat gilt

**Satz 2.1**
$$\begin{aligned} j(z) &= q^{-1} + \sum_{n=0}^{\infty} c_n q^n \quad \text{mit } c_n \in \mathbb{Z} \\ &= q^{-1} + 744 + 196884q + \dots \end{aligned}$$

*Beweis.* Mit den Propositionen 1.1 und 1.2 folgt direkt aus der Definition

$$\begin{aligned} j(z) &= \frac{1728 \cdot 60^3 \cdot \left[2\frac{\pi^4}{90} + 2\frac{(2\pi i)^4}{6}\sum_{n=1}^{\infty}\sigma_3(n)q^n\right]^3}{(2\pi)^{12} q \prod_{n=1}^{\infty}(1-q^n)^{24}} \\ &= \frac{[1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n]^3}{q\prod_{n=1}^{\infty}(1-q^n)^{24}}, \end{aligned} \tag{7}$$

woraus sich bereits $c_n = 0$ für $n < -1$, $c_{-1} = 1$ und die Ganzheit der übrigen $c_n$ ablesen lässt. Die expliziten Werte für $c_2$ und $c_3$ ergeben sich aus der expliziten Gestalt der $q$-Entwicklung von $G_4(z)$ in Proposition 1.1. □

**Proposition 2.2** $j(\mathbb{H}) = \mathbb{C}$.

*Beweis.* Das Bild von $j$ ist offen, da $\mathbb{H}$ offen und $j$ holomorph ist. Zum Beweis der Proposition langt es daher zu zeigen, dass $j(\mathbb{H})$ abgeschlossen ist.

Sei also $\eta$ eine komplexe Zahl und $(\eta_i)_{i=1}^{\infty}$ eine Folge in $j(\mathbb{H})$, die gegen $\eta$ konvergiert. Unser Ziel ist natürlich, zu zeigen, dass $\eta$ bereits im Bild von $j$ liegt. Dazu wählen wir zunächst eine Folge $(z_i)_{i=1}^{\infty}$ im Standardfundamentalbereich

$$\mathcal{F} = \{z \in \mathbb{H} \mid |z| \geq 1,\ |\mathrm{Re}(z)| \leq \frac{1}{2}\}$$

von $\Gamma(1)$ in $\mathbb{H}$, die für alle $i$ die Bedingung $j(z_i) = \eta_i$ erfüllt. Wenn wir nun eine in $\mathcal{F}$ konvergente Teilfolge von $(z_i)$ fänden, nennen wir den zugehörigen Grenzwert $z$, dann folgte aus der Stetigkeit von $j$ auch schon $j(z) = \eta$, also die Behauptung.

Leider ist $\mathcal{F}$ nicht kompakt, so dass wir a priori nicht so argumentieren können. Andererseits ist das einzige, was für uns schiefgehen kann, dass die Imaginärteile $\mathrm{Im}(\eta_i)$ für $i$ gegen unendlich beliebig groß werden, was aber nicht vorkommen kann, weil $j$ bei $\infty$ einen Pol hat, also

$$\lim_{\mathrm{Im}(z)\to\infty} j(z) = \infty$$

gilt, so dass in diesem Fall die ursprüngliche Folge $(\eta_i)$ nicht konvergierte. Es gibt also eine Schranke $c$, so dass die $z_i$ in Wirklichkeit schon in einem „abgeschnittenen" Fundamentalbereich

$$\mathcal{F} \cap \{z \in \mathbb{H} \mid \mathrm{Im}(z) \leq c\}$$

liegen. Da letzterer kompakt ist, ist damit die Proposition bewiesen. □

Wir wollen nun eine Abschätzung für die Fourierkoeffizienten $c_n$ von $j$ zeigen, nämlich

**Satz 2.3** *Für alle $n \geq 1$ gilt $c_n \leq 60^3(n+1)^6(n+2)^7\binom{n+3}{2}e^{4\pi\sqrt{n+1}}$.*

*Beweis.* Wir betrachten wieder (7) und bestimmen getrennte Abschätzungen für die Fourierentwicklungen von Zähler und Nenner. Für

$$N(q) := \prod_{n\geq 1}(1-q^n)^{-24} = \sum_{n=1}^{\infty}\gamma_n q^n$$

gilt dabei für alle $n \geq 1$ die Abschätzung $\gamma_n < e^{4\pi\sqrt{n}}$,

*denn:* Wegen Proposition 1.2 und der Holomorphie von $\Delta$ auf der offenen Einheitskreisscheibe $|q| < 1$ konvergiert $N(q)$ ebendort. Damit können wir

$$\log N(q) = -24\sum_{n\geq 1}\log(1-q^n) = 24\sum_{n\geq 1}\sum_{m\geq 1}\frac{q^{mn}}{m} = 24\sum_{m\geq 1}\frac{q^m}{m\cdot(1-q^m)}$$

betrachten, wo die letzte Gleichheit gilt, da die Reihe $\sum_{m\geq 1}\frac{q^{mn}}{m}$ auf jeder kompakten Teilmenge der offenen Einheitskreisscheibe gleichmäßig konvergiert.[2] Für reelle $0 < q < 1$ gilt offensichtlich

$$mq^{m-1}(1-q) < (1+q+\cdots+q^{m-1})(1-q) = (1-q^m),$$

so dass wir abschätzen können

$$\frac{q^m}{m\cdot(1-q^m)} < \frac{q}{m^2\cdot(1-q)}.$$

Daraus folgt direkt

$$\log N(q) < 24\sum_{m\geq 1}\frac{1}{m^2}\cdot\frac{q}{1-q} = 4\pi^2\cdot\frac{q}{1-q}. \tag{8}$$

[2] Betrachte kompakte Teilmengen der Form $\{q \mid 0 \leq |q| \leq c < 1\}$.

Andererseits sind die $\gamma_n$ alle nicht-negativ, so dass (immer noch mit $0 < q < 1$) für jedes von ihnen

$$\gamma_n q^n < \sum_{n\geq 1} \gamma_n q^n = N(q)$$

gilt, woraus wir für $0 < q < 1$ mit (8)

$$\log \gamma_n \leq \log N(q) - n \log q < 4\pi^2 \cdot \frac{q}{1-q} + n \cdot \frac{1-q}{q}$$

folgern können. Um unsere Behauptung zu zeigen setzen wir $q = \frac{\sqrt{n}}{2\pi+\sqrt{n}}$, was wie gewünscht $\log \gamma_n < 4\pi\sqrt{n}$ liefert. #

Betrachten wir nun die Koeffizienten $\beta_n$ der Fourierentwicklung von

$$Z(q) := \left[1 + 240 \sum_{n\geq 1} \sigma_3(n) q^n\right]^3 = \sum_{n=1}^{\infty} \beta_n q^n.$$

Diese schätzen wir (recht grob) wie folgt ab. Wie man induktiv leicht zeigen kann (Übung!) gilt für die dritte Teilersumme

$$\sigma_3(n) \leq \sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}.$$

Wenn wir $\sigma_3(0) = 1$ setzen, folgt daraus

$$\begin{aligned}
\beta_n &\leq 240^3 \sum_{\substack{k+l+m=n \\ 0\leq k,l,m\leq n}} \sigma_3(k)\sigma_3(l)\sigma_3(m) \\
&\ll 240^3 \cdot \left(\frac{n^2(n+1)^2}{4}\right)^3 \cdot \left|\{(k,l,m) \in \mathbb{Z}^3 \mid 0 \leq k,l,m \leq n,\ k+l+m = n\}\right| \\
&= 60^3 n^6 (n+1)^6 \frac{(n+1)(n+2)}{2} \\
&= 60^3 n^6 (n+1)^6 \binom{n+2}{2}.
\end{aligned}$$

Fassen wir diese Abschätzungen zusammen, erhalten wir

$$\begin{aligned}
c_n &\overset{(7)}{=} \sum_{\substack{k+m=n+1 \\ k,m\geq 0}} \gamma_k \beta_m \\
&\leq (n+2) \max_{k\leq n+1} \gamma_k \max_{m\leq n+1} \beta_m \\
&\leq (n+2) e^{4\pi\sqrt{n+1}} \left[60^3 (n+1)^6 (n+2)^6 \binom{n+3}{2}\right],
\end{aligned}$$

wo wir im letzten Schritt ausgenutzt haben, dass die zuvor gewonnenen Abschätzungen für die $\gamma_n$ und die $\beta_n$ monoton in $n$ wachsen. □

**Bemerkung** *Asymptotisch gilt nach Petersson (siehe [Pet])*

$$c_n \sim \frac{e^{4\pi\sqrt{n}}}{\sqrt{2}n^{3/4}} \quad \text{für } n \to \infty,$$

*womit unsere Abschätzung gar nicht einmal so schlecht zu sein scheint.*

Wir wollen nun diese Erkenntnisse auf die Hauptbehauptung anwenden. Dazu bedenken wir, dass $q$ für $z = \frac{1+\sqrt{-163}}{2}$ den Wert $-e^{-\pi\sqrt{163}}$ annimmt. Es lohnt sich also

$$j(\frac{1+\sqrt{-163}}{2}) = -e^{\pi\sqrt{163}} + 744 + \underbrace{\sum_{n=1}^{\infty} c_n(-1)^{n+1}e^{-\pi\sqrt{163}n}}_{=:S} \tag{9}$$

zu betrachten. Hierbei ist $S$ eine betragsmäßig sehr kleine reelle Zahl, genauer $|S| < 10^{-12}$,

*denn:* Nach Satz 2.3 können wir $|S|$ durch

$$|S| \leq \left|196884 \cdot e^{-\pi\sqrt{163}} - c_2 e^{-2\pi\sqrt{163}}\right| + \sum_{n=3}^{\infty} \underbrace{60^3(n+1)^6(n+2)^7\binom{n+3}{2}e^{4\pi\sqrt{n+1}-n\pi\sqrt{163}}}_{=:S_n}$$

abschätzen. Wie man numerisch leicht nachprüft, gilt

- $7 \cdot 10^{-13} < 196884 \cdot e^{-\pi\sqrt{163}} < 8 \cdot 10^{-13}$,
- $10^{-12} < c_2 e^{-2\pi\sqrt{163}} \overset{2.3}{\leq} 60^3 \cdot 3^6 \cdot 4^7 \cdot 10 \cdot e^{(4\sqrt{3}-2\sqrt{163})\pi} < 1,1 \cdot 10^{-12}$,
- Für $n \geq 2$ gilt

$$\begin{aligned}\frac{S_{n+1}}{S_n} &= \frac{(n+3)^6}{(n+1)^6} \cdot \frac{n+3}{n+2} \cdot \frac{n+4}{n+2} \cdot e^{4\pi(\sqrt{n+2}-\sqrt{n+1})-\pi\sqrt{163}} \\ &\leq \frac{5^6}{3^6} \cdot \frac{5}{4} \cdot \frac{6}{4} \cdot e^{4\pi(2-\sqrt{3})-\pi\sqrt{163}} \\ &\approx 4,4 \cdot 10^{-15} \\ &\ll \frac{1}{4},\end{aligned}$$

woraus durch Aufsummieren die Behauptung folgt. #

Hieraus können wir auf die Hauptbehauptung schließen, wenn wir zeigen können, dass der Funktionswert $j(\frac{1+\sqrt{-163}}{2})$ eine ganze Zahl ist. Um dies zu verstehen, müssen wir den Zusammenhang zwischen der $j$-Invariante und elliptischen Kurven verstehen.

## 3 Elliptische Kurven

In diesem Abschnitt führen wir elliptische Kurven über $\mathbb{C}$ ein. Die übliche, algebrogeometrische Definition lautet

**Definition 3.1** *Eine **elliptische Kurve über** $\mathbb{C}$ ist eine glatte über $\mathbb{C}$ definierte algebraische Kurve von Geschlecht 1.*

Wir wollen aber eine leichter zugängliche und für rechnerische Zwecke besser anwendbare Definition verwenden. Dazu betrachten wir den ***n-dimensionalen projektiven Raum*** $\mathbb{P}^n(\mathbb{C})$ über dem Körper der komplexen Zahlen, also die Menge $\mathbb{C}^{n+1} \setminus \{0\}$ modulo der Äquivalenzrelation

$$P \sim Q :\Longleftrightarrow P = tQ \text{ mit } t \in \mathbb{C}^\times.$$

Vertreter von Elementen von $\mathbb{P}^n(\mathbb{C})$ wollen wir als $(n+1)$-Tupel $[z_0 : \ldots : z_n]$ mit $z_0, \ldots, z_n \in \mathbb{C}$ nicht alle Null schreiben.

**Bemerkung** *Man kann sich $\mathbb{P}^n(\mathbb{C})$ als die Menge der Ursprungsgeraden in $\mathbb{C}^{n+1}$ vorstellen.*

Sei nun $I$ ein Ideal im Polynomring $\mathbb{C}[X_0, \ldots, X_n]$, das ein Erzeugendensystem aus homogenen Polynomen hat. Dann setzen wir

$$V_I := \{P \in \mathbb{P}^n(\mathbb{C}) \mid f(P) = 0 \text{ für alle homogenen } f \in I\}$$

und sagen, dass eine Teilmenge $V \subseteq \mathbb{P}^n(\mathbb{C})$ eine ***projektive Varietät*** ist, wenn es ein homogenes Ideal $I$ mit $V = V_I$ gibt. $I = I(V_I)$ heißt dann das ***Verschwindungsideal*** von $V_I$.

**Beispiel**

(a) *Mit $I = (0)$ ist $\mathbb{P}^n(\mathbb{C})$ selbst eine projektive Varietät.*

(b) *Mit $I = (1)$ ist die leere Menge eine projektive Varietät.*

(c) *Betrachten wir $I = (X^2 + Y^2 - Z^2)$. Die Nullstellen von $X^2 + Y^2 - Z^2$ mit $Z \neq 0$ können wir in der Form $[x : y : 1]$ mit $x = \frac{X}{Z}$ und $y = \frac{Y}{Z}$ schreiben, wobei noch $x^2 + y^2 = 1$ gelten soll. Es gibt aber noch weitere Nullstellen, nämlich diejenigen mit $Z = 0$. Diese haben die Form $[X : \pm iX : 0]$ mit $X \neq 0$, da ja $[0 : 0 : 0] \neq \mathbb{P}^2(\mathbb{C})$ gilt; modulo Streckungsfaktoren ergeben sich die zwei Punkte $[1 : \pm i : 0]$.*

Wir können den affinen Raum $\mathbb{C}^n$ (nicht-kanonisch) in den projektiven Raum $\mathbb{P}^n(\mathbb{C})$ einbetten. Sei nun $V$ eine projektive Varietät. Dann ist für jede solche Einbettung die Dimension von $V \cap \mathbb{C}^n$ bestimmt. Man kann zeigen (s. [Har], I.2), dass diese Dimensionen für alle $V \cap \mathbb{C}^n \neq \varnothing$ übereinstimmen, und so die ***Dimension*** einer projektiven Varietät definieren.

**Beispiel** *Im Falle von $V_I$ mit $I = (X^2 + Y^2 - Z^2)$ wählen wir die Einbettung $(x, y) \mapsto [x : y : 1]$. Dann ist nach den Überlegungen des letzten Beispiels $V_I \cap \mathbb{C}^2$ gleich dem „Einheitskreis“ $\{(x, y) \in \mathbb{C}^2 \mid y^2 = 1 - x^2\}$. Dieser hat Dimension 1, was somit auch die Dimension von $V_I$ ist.*

Eine projektive Varietät von Dimension 1 heißt ***projektive Kurve***. Wir wollen nun eine Definition für elliptische Kurven über $\mathbb{C}$ als projektive Kurven mit besonders übersichtlichen Verschwindungsidealen angeben. Dass die beiden hier gegebenen Definitionen auch tatsächlich übereinstimmen, zeigt man mit dem Satz von Riemann-Roch (siehe zum Beispiel in [Sil1], Kapitel III).

**Definition 3.2** *Eine **Weierstraßgleichung** ist eine affine Polynomgleichung der Form*

$$y^2 = 4x^3 - g_2 x - g_3$$

*mit Diskrimininante $\Delta = g_2^3 - 27g_3^2 \neq 0$. Diese definiert offensichtlich eine affine Kurve. Jede Weierstraßgleichung ist ein Pullback einer eindeutigen Polynomgleichung*

$$Y^2 Z = 4X^3 - g_2 XZ^2 - g_3 Z^3$$

*unter der Einbettung $\mathbb{C}^2 \hookrightarrow \mathbb{P}^2(\mathbb{C})$, $(x, y) \mapsto [x : y : 1]$. Eine projektive Kurve $E \subseteq \mathbb{P}^2(\mathbb{C})$, deren Verschwindungsideal durch eine derartige Polynomgleichung gegeben ist, heißt **elliptische Kurve über** $\mathbb{C}$.*

Wir werden in dieser Vorlesung immer nur auf die zweite Definition zugreifen und von nun an verkürzend nur noch von „elliptischen Kurven“ sprechen, wenn wir „elliptische Kurven über $\mathbb{C}$“ meinen.

**Bemerkung** *Die Punkte einer elliptischen Kurve sind genau die „affinen Punkte“ für $Z = 1$ zusammen mit einem „Punkt bei unendlich“ $[0 : 1 : 0]$, so dass man auch einfacher mit der affinen Weierstraßgleichung*

$$y^2 = 4x^3 - g_2 x - g_3$$

*analog zum letzten Beispiel arbeiten kann, wenn man den zusätzlichen Punkt im Hinterkopf behält.*

Der ***affine Koordinatenring*** einer elliptischen Kurve $E$ ist durch

$$\mathbb{C}[E] = \mathbb{C}[X, Y, Z]/I(E)$$

gegeben. Man bemerke, dass ein Element $\phi \in \mathbb{C}[E]$ bis auf ein Polynom, das auf $E$ verschwindet, wohldefiniert ist und so eine Funktion $\phi : E \to \mathbb{C}$ definiert. Der Quotientenkörper $\mathbb{C}(E)$ von $\mathbb{C}[E]$ heißt daher auch der (rationale) ***Funktionenkörper*** von $E$.

Sei nun $P \in E$ ein beliebiger Punkt. Dann ist

$$\mathfrak{m}_P = \{\phi \in \mathbb{C}[E] \mid \phi(P) = 0\}$$

ein maximales Ideal des affinen Koordinatenrings, denn die durch $\phi \mapsto \phi(P)$ gegebene Abbildung ist offensichtlich ein Isomorphismus von $\mathbb{C}[E]/\mathfrak{m}_P$ nach $\mathbb{C}$. Die Lokalisierung $\mathbb{C}[E]_P$ des affinen Koordinatenrings nach $\mathfrak{m}_P$ heißt der ***lokale Ring*** von $E$ in $P$ und ist ein diskreter Bewertungsring (siehe in einem beliebigen guten Buch über kommutative Algebra). Die zugehörige (normierte) Bewertung ist dabei durch

$$\operatorname{ord}_P : \begin{cases} \mathbb{C}[E]_P & \to \mathbb{N}_0 \cup \{\infty\}, \\ \phi & \mapsto \max\{d \in \mathbb{Z} \mid \phi \in \mathfrak{m}_P^d\} \end{cases}$$

gegeben und lässt sich via $\mathrm{ord}_P(\phi/\psi) = \mathrm{ord}_P(\phi) - \mathrm{ord}_P(\psi)$ auf ganz $\mathbb{C}(E)$ fortsetzen.

Eine wichtige Besonderheit von elliptischen Kurven ist, dass man auf ihnen auf natürliche Weise eine Gruppenverknüpfung definieren kann. Sei dafür $E$ ab jetzt eine fixe elliptische Kurve, und bezeichne $O \in E$ den Punkt $[0:1:0]$ bei unendlich. Die ***Divisorengruppe*** $\mathrm{Div}(E)$ von $E$ ist die freie abelsche Gruppe über den Punkten von $E$. Ein ***Divisor*** $D \in \mathrm{Div}(E)$ ist also eine formale Summe

$$D = \sum_{P \in E} n_P(P)$$

mit $n_P \in \mathbb{Z}$ und fast allen $n_P = 0$. Der ***Grad*** eines Divisors ist die Summe $\deg(D) = \sum_{P \in E} n_P$ seiner Koeffizienten. Offensichtlich bilden die Divisoren von Grad 0 eine Untergruppe von $\mathrm{Div}(E)$; diese schreiben wir $\mathrm{Div}^0(E)$. Andererseits definiert jedes $\phi \in \mathbb{C}(E)$ via

$$\mathrm{div}(\phi) = \sum_{P \in E} \mathrm{ord}_P(\phi)(P)$$

einen Divisor in $\mathrm{Div}(E)$, da $\phi$ nur endlich viele Nullstellen und Pole haben kann.[3]

Die Divisoren $\mathrm{div}(\phi)$ für ein $\phi \in \mathbb{C}(E)$ heißen ***Hauptdivisoren*** von $E$. Schließlich heißt $\mathrm{Div}(E)$ modulo den Hauptdivisoren die ***Divisorenklassengruppe*** oder auch ***Picardgruppe*** und wird $\mathrm{Pic}(E)$ geschrieben.

**Proposition 3.3** *Sei $E$ eine elliptische Kurve und $\phi \in \mathbb{C}(E)^\times$. Dann gilt*

(a) $\mathrm{div}(\phi) = 0$ *genau dann, wenn* $\phi \in \mathbb{C}^\times$,

(b) $\deg(\mathrm{div}(\phi)) = 0$.

*Beweis.* (a) Eine ***rationale Abbildung*** zwischen zwei projektiven Kurven $C_1, C_2 \subseteq \mathbb{P}^n(\mathbb{C})$ ist eine Abbildung der Form $f = [\phi_0 : \ldots : \phi_n]$, wo $\phi_0, \ldots, \phi_n \in \mathbb{C}(C_1)$ so gewählt sind, dass für alle $P \in C_1$, an denen alle $\phi_i$ definiert sind (also $\mathrm{ord}_P(\phi_i) \geq 0$ gilt), $f(P) = [\phi_0(P) : \ldots : \phi_n(P)] \in C_2$ gilt. Eine solche Abbildung heißt ein ***Morphismus von Kurven***, wenn zu jedem $P \in E$ ein $\psi \in \mathbb{C}(E)$ existiert, so dass alle $(\psi \circ \phi_i)$ in $P$ regulär sind und es ein $i$ gibt, so dass $(\psi \circ \phi_i)(P) \neq 0$ gilt.

Zu jedem $\phi \in \mathbb{C}(E)$ können wir eine rationale Abbildung

$$\phi : \begin{cases} E & \to \mathbb{P}^1(\mathbb{C}), \\ P & \mapsto [\phi(P) : 1] \end{cases}$$

definieren, die explizit gegeben ist durch

$$\phi(P) = \begin{cases} [\phi(P) : 1] & \text{falls } \phi \text{ regulär in } P \text{ ist,} \\ [1 : 0] & \text{falls } \phi \text{ einen Pol in } P \text{ hat.} \end{cases}$$

Diese rationale Abbildung ist sogar ein Kurvenmorphismus,

[3] Ein Beweis für letztere Aussage findet sich beispielsweise in [Har].

*denn:* Sei $P \in E$ irgendein Punkt und $t \in \mathbb{C}(E)$ beliebig mit Nullstellenordnung 1 in $P$, also ein Erzeuger des maximalen Ideals $\mathfrak{m}_P$.[4] Sei weiter $n = \min\{\mathrm{ord}_P \phi, 0\}$. Dann ist $\mathrm{ord}_P(t^{-n} \circ \phi) \geq 0$ und $\mathrm{ord}_P(t^{-n}) \geq 0$ und (mindestens) eines der beiden sogar gleich Null, so dass nach Konstruktion sowohl $(t^{-n} \circ \phi)$ als auch $t^{-n}$ regulär sind und eine dieser beiden Funktionen in $P$ nicht verschwindet. #

Ein $\phi$ mit $\mathrm{div}(\phi) = 0$ hat keine Pole, so dass der zugehörige Kurvenmorphismus nicht surjektiv ist. Andererseits sind Kurvenmorphismen immer surjektiv oder konstant,[5] also $\phi \in \mathbb{C}^\times$.

Dass jedes $\phi \in \mathbb{C}^\times$ auch $\mathrm{div}(\phi) = 0$ erfüllt, ist klar.

(b) [Sil1], II.3.7. □

Wegen der Proposition ist natürlich auch der Quotient $\mathrm{Div}^0(E)$ modulo Hauptdivisoren wohldefiniert; wir wollen ihn mit $\mathrm{Pic}^0(E)$ bezeichnen.

Die Abbildung

$$\Phi : \begin{cases} E & \to \mathrm{Pic}^0(E) \\ P & \mapsto [(P) - (O)] \end{cases}$$

ist offensichtlich eine Bijektion von Mengen, so dass wir die Gruppenstruktur von $\mathrm{Pic}^0(E)$ auf $E$ übertragen können.

Mit dem Satz von Riemann-Roch lässt sich zeigen,[6] dass diese Gruppenstruktur eine elegante geometrische Interpretation besitzt. Dieses geometrische Gruppengesetz lässt sich wie folgt erklären: Der Satz von Bézout besagt in dieser Situation, dass der Schnitt von $E$ mit einer beliebigen projektiven Geraden (mit Vielfachheiten) dreielementig ist. Bezeichnen wir nun für zwei beliebige Punkte $P, Q \in E$ die projektive Gerade durch die beiden oder, falls $P = Q$ gilt, die Tangente von $E$ in $P$ mit $PQ$ und weiter den dritten Schnittpunkt von $PQ$ mit $E$ als $R$. Dann ist die Summe $P \oplus Q$ als der dritte Schnittpunkt von $OR$ (wieder Sekante bzw. Tangente) mit $E$ definiert. Folgende Eigenschaften des geometrischen Gruppengesetzes sind sofort klar (Übung!):

- Es ist kommutativ.
- Der ausgezeichnete Punkt $O$ ist das neutrale Element.
- Für einen beliebigen Punkt $P \in E$ ist der dritte Schnittpunkt von $OP$ mit $E$ das Inverse $\ominus P$.

Die Assoziativität des geometrischen Gruppengesetzes lässt sich, wenn auch recht mühsam, ebenfalls direkt nachrechnen; der Beweis über den Isomorphismus von $E$ mit $\mathrm{Pic}^0(E)$ ist aber sowohl angenehmer als auch erhellender.

Eine weitere interessante Eigenschaft von elliptischen Kurven ist, dass man sie mit der Struktur einer kompakten, zusammenhängenden Riemann'schen Fläche versehen kann. Wir wollen dies

[4] So etwas gibt es, da $\mathbb{C}[E]_P$ ein diskreter Bewertungsring ist.

[5] Beweisidee: Kurvenmorphismen schicken abgeschlossene Mengen auf abgeschlossene Mengen, so dass das Bild der ganzen Kurve nur die ganze Kurve oder ein einzelner Punkt sein kann.

[6] Siehe [Sil1], Kapitel III

kurz skizzieren: Sei also $E$ eine elliptische Kurve mit Weierstraßgleichung $y^2 = 4x^3 - g_2x - g_3$. Diese „erbt" eine Hausdorff'sche Topologie vom projektiven Raum $\mathbb{P}^2(\mathbb{C})$, in den sie eingebettet ist. Überdecken wir nun die Kurve mit kleinen offenen Umgebungen $U_P$ um ihre Punkte $P$. Zu jedem $U_P$ können wir den lokalen Parameter $t_P \in \mathbb{C}(E)$, wie wir ihn im Beweis von Proposition 3.3 kennengelernt haben, als Kartenabbildung wählen. Dann sind die Kartenwechselabbildungen $t_Q \circ t_P^{-1}$ offensichtlich analytisch. Explizit können wir wählen

$$\begin{array}{ll} t_P = x(P) & \text{für alle } P = [x : y : 1] \text{ mit } \frac{dy^2}{dy} = 2y \neq 0, \\ t_P = y(P) & \text{für alle } P = [x : y : 1] \text{ mit } \frac{d(4x^3 - g_2x - g_3)}{dx} = 12x^2 - g_2 \neq 0, \\ t_O = \frac{X}{Y}(O). & \end{array} \tag{10}$$

Wir wollen unseren kleinen Steilkurs über elliptische Kurven damit beenden, dass wir geeignete strukturerhaltende Abbildungen zwischen elliptischen Kurven einführen.

**Definition 3.4** *Seien $E_1$ und $E_2$ zwei elliptische Kurven und $O_1$ und $O_2$ die zugehörigen Punkte bei unendlich. Ein Morphismus $f : E_1 \to E_2$ mit $f(O_1) = O_2$ heißt eine **Isogenie**. Die Menge aller Isogenien zwischen $E_1$ und $E_2$ wird mit $\mathrm{Hom}(E_1, E_2)$ bezeichnet. Eine bijektive Isogenie heißt auch **Isomorphismus**; gilt $E_1 = E_2$ und $O_1 = O_2$, so nennen wir eine Isogenie einen **Endomorphismus**. Die Menge aller Endomorphismen einer elliptischen Kurve $E$ wird mit $\mathrm{End}(E)$ bezeichnet.*

**Beispiel** *Sei $E$ eine elliptische Kurve mit Punkt bei unendlich $O$. Für jede ganze Zahl $m$ können wir einen Endomorphismus „Multiplikation mit $m$"*

$$[m] : E \to E$$

*definieren, indem wir setzen*

$$[m](P) = \begin{cases} \oplus_{i=1}^{m} P & \text{für } m > 0, \\ [-m](\ominus P) & \text{für } m < 0, \\ O & \text{für } m = 0. \end{cases}$$

*Dass die $[m]$ Isogenien sind, kann man induktiv daraus herleiten, dass die Gruppenverknüpfung $\oplus : E \times E \to E$ ein Morphismus ist. Um letzteres zu zeigen, kann man aus der Weierstraßgleichung von $E$ eine explizite Formel für $\oplus$ ausarbeiten. Dieser sieht man dann sofort an, dass es sich um eine rationale Abbildung handelt. Dass $\oplus$ auch überall definiert ist, verlangt noch die Betrachtung von vier Sonderfällen. (siehe [Sil1], Theorem III.3.6)*

Für zwei beliebige elliptische Kurven $E_1$ und $E_2$ hat $\mathrm{Hom}(E_1, E_2)$ mit der Verknüpfung

$$(f + g)(P) = f(P) \oplus g(P)$$

die Struktur einer Gruppe, da (wie im Beispiel) die Gruppenverknüpfung von $E_2$ ein Morphismus ist. Endomorphismen einer gegebenen elliptischen Kurve $E$ lassen sich zusätzlich noch komponieren, was $\mathrm{End}(E)$ zu einem Ring macht.

## 4 Die *j*-Invariante einer elliptischen Kurve

Um die Ganzheit von $j(\frac{1+\sqrt{-163}}{2})$ einzusehen, müssen wir den Zusammenhang zwischen der $j$-Invariante und elliptischen Kurven verstehen. Wir beginnen damit in diesem Abschnitt, indem wir jedem Gitter $\Lambda \subset \mathbb{C}$ einen Zahlenwert $j(\Lambda)$ zuweisen und diese Zuordnung mit der bekannten $j$-Invarianten identifizieren.

Sei also $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ mit $\mathbb{R}$-linear unabhängigen $\omega_1, \omega_2 \in \mathbb{C}^\times$ ein beliebiges (vollständiges) Gitter in $\mathbb{C}$. Wir erinnern uns, dass dann für den Körper $K(\Lambda)$ der elliptischen Funktionen bezüglich $\Lambda$

$$K(\Lambda) = \mathbb{C}(\wp_\Lambda) + \mathbb{C}(\wp_\Lambda)\wp'_\Lambda$$

gilt, wo

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda \\ \omega\neq(0,0)}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$$

die Weierstraß'sche $\wp$-Funktion zu $\Lambda$ und $\wp'_\Lambda(z)$ ihre Ableitung ist. Die Laurententwicklung um Null von $\wp_\Lambda(z)$ lautet

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)G_{2n+2}(\Lambda)z^{2n}, \tag{11}$$

wo

$$G_{2n}(\Lambda) = \sum_{\substack{\omega\in\Lambda \\ \omega\neq(0,0)}} \omega^{-2n}$$

für $n \geq 2$ die ***Eisensteinreihe*** vom Gewicht $2n$ zu $\Lambda$ ist. Analog zu (6) führen wir schließlich

$$j(\Lambda) = \frac{1728 \cdot (60G_4(\Lambda))^3}{(60G_4(\Lambda))^3 - 27 \cdot (140G_6(\Lambda))^2} \tag{12}$$

ein.

Offensichtlich lässt sich jedes Gitter $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ wie oben durch Multiplikation mit einem $z \in \mathbb{C}^\times$ in die Form $\Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z}$ mit $\tau \in \mathbb{H}$ bringen.[7] Die Funktion $j$ ist modulo solcher Homothetie wohldefiniert, da für jedes $z \in \mathbb{C}^\times$

$$j(z\Lambda) = \frac{1728 \cdot (60z^{-4}G_4(\Lambda))^3}{(60z^{-4}G_4(\Lambda))^3 - 27 \cdot (140z^{-6}G_6(\Lambda))^2} = j(\Lambda)$$

gilt. Aus der Zuordnung $j : \{\text{Gitter}\}/\text{ Homothetie} \to \mathbb{C}$ lässt sich via $j(z) := j(\Lambda_z)$ eine Funktion auf der oberen Halbebene gewinnen. Dann gilt

**Proposition 4.1** *Diese Funktion $j(z)$ ist identisch mit der gleich benannten Funktion aus (6).*

[7] Nämlich mit $z = \omega_1^{-1}$ oder mit $z = \omega_2^{-1}$

*Beweis.* Die Proposition folgt nach Konstruktion von $j$, da die analog definierten Eisensteinreihen $G_n(z) := G_n(\Lambda_z)$ offensichtlich mit denen in (2) übereinstimmen. □

**Bemerkung** *Halten wir fest, dass wir den Wert $j(\frac{1+\sqrt{-163}}{2})$, dessen Ganzheit wir zeigen wollen, als j-Invariante des Gitters $\mathbb{Z} + \frac{1+\sqrt{-163}}{2}\mathbb{Z}$ auffassen können.*

Nun besteht andererseits ein enger Zusammenhang zwischen Gittern $\Lambda$ und elliptischen Kurven. Genauer gilt ja für $\wp_\Lambda$ die berühmte Funktionalgleichung

$$\wp'_\Lambda(z)^2 = 4\wp_\Lambda(z)^3 - 60G_4(\Lambda)\wp_\Lambda(z) - 140G_6(\Lambda),$$

die sich leicht aus (11) herleiten lässt. Diese sieht gerade so aus wie die affine Weierstraßgleichung einer elliptischen Kurve. In der Tat gilt für die Abbildung

$$\psi : \begin{cases} \mathbb{C}/\Lambda & \to \mathbb{P}^2(\mathbb{C}), \\ z & \mapsto \begin{cases} [\wp_\Lambda(z) : \wp'_\Lambda(z) : 1] & \text{für } z \notin \Lambda, \\ [0:1:0] & \text{für } z \in \Lambda \end{cases} \end{cases}$$

die folgende

**Proposition 4.2** (a) *$E_\Lambda := \mathrm{Bild}(\psi)$ ist eine elliptische Kurve; es gilt also*

$$\Delta(\Lambda) = (60\ G_4(\Lambda))^3 - 27 \cdot (140\ G_6(\Lambda))^2 \neq 0,$$

(b) *$\psi : \mathbb{C}/\Lambda \to E_\Lambda$ ist ein Isomorphismus Riemann'scher Flächen,*

(c) *Die meromorphen Funktionen auf $\mathbb{C}/\Lambda$ entsprechen unter $\psi$ den rationalen Funktionen auf $E_\Lambda$,*

(d) *Das Gruppengesetz auf $E_\Lambda$ liftet sich via $\psi$ zur üblichen Vektoraddition auf $\mathbb{C}/\Lambda$.*

*Beweis.* (a) $\Delta(\Lambda)$ ist die Diskriminante des Polynoms $F(x) = 4x^3 - 60G_4(\Lambda)x - 140G_6(\Lambda)$, so dass es genügt zu überprüfen, dass die drei Nullstellen $e_1, e_2, e_3$ von $F(x)$ paarweise verschieden sind. Nach Voraussetzung haben wir

$$\wp'_\Lambda(z)^2 = 4(\wp_\Lambda(z) - e_1)(\wp_\Lambda(z) - e_2)(\wp_\Lambda(z) - e_3).$$

Nun hat ja $\wp'_\Lambda$ bekanntermaßen modulo $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ genau die Nullstellen $\frac{\omega_1}{2}$, $\frac{\omega_2}{2}$, $\frac{\omega_1+\omega_2}{2}$, so dass offensichtlich

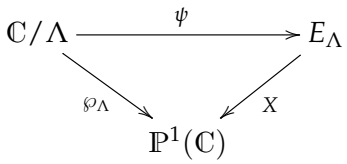
$$\{e_1, e_2, e_3\} = \{\wp_\Lambda(\frac{\omega_1}{2}), \wp_\Lambda(\frac{\omega_2}{2}), \wp_\Lambda(\frac{\omega_1+\omega_2}{2})\}$$

gilt. Die $\wp_\Lambda$-Werte rechts hängen nicht von der Wahl der Gitterbasis ab, da man die Nullstellen von $\wp'_\Lambda$ invariant auch als die komplexen Zahlen beschreiben kann, die in $\frac{1}{2}\Lambda$ aber nicht in $\Lambda$ liegen. Außerdem sind sie paarweise verschieden,

*denn:* Nehmen wir an, zwei von ihnen hätten denselben Wert $b \in \mathbb{C}$. Dann nähme $\wp_\Lambda$ den Wert $b$ mindestens viermal an, nämlich an den zwei verschiedenen Stellen jeweils mit Vielfachheit mindestens 2 – die Ableitung $\wp'_\Lambda$ ist dort ja als verschwindend vorausgesetzt. Die Weierstraß'sche $\wp_\Lambda$-Funktion ist jedoch eine elliptische Funktion der Ordnung 2 und kann daher nach dem 3. Liouville'schen Satz nur zwei $b$-Stellen besitzen. #

(b) Sowohl $\wp_\Lambda$ als auch $\wp'_\Lambda$ sind außerhalb der Gitterpunkte von $\Lambda$ analytisch. Daher ist $\psi$ außerhalb von 0 bezüglich der offensichtlichen Kartenabbildung auf $\mathbb{C}/\Lambda$ und der Kartenabbildungen (10) analytisch. Die Holomorphie in 0 folgt, da $\frac{\wp_\Lambda(z)}{\wp'_\Lambda(z)}$ bei $z = 0$ holomorph ist.

Um zu zeigen, dass $\psi$ ein Isomorphismus ist, nutzen wir aus, dass analytische Abbildungen zwischen kompakten Riemann'schen Flächen entweder konstant oder surjektiv sind[8] und in letzterem Fall eine ***Überlagerung***, das heißt stetig, offen und diskret. Die Diskretheit bedeutet gerade, dass jeder Punkt im Zielraum eine diskrete Teilmenge des Definitionsbereichs ist. Man kann nun zeigen, dass die Anzahl dieser Urbilder (gerechnet mit Vielfachheiten) vom gewählten Punkt unabhängig ist. Diese Größe nennt man den ***Grad*** der jeweiligen Überlagerung. Klar, dass genau dann ein Isomorphismus vorliegt, wenn der Grad der betrachteten Abbildung 1 ist. Betrachten wir nun das folgende kommutative Diagramm




wo $X$ den Kurvenmorphismus zu $X \in \mathbb{C}(E_\Lambda)$ wie im Beweis von Proposition 3.3 bezeichne. Offensichtlich ist $X$ eine zweiblättrige Überlagerung mit Verzweigung in $[0 : 1 : 0]$ und in den Punkten, deren $Y$-Koordinate verschwindet. Andererseits ist auch $\wp_\Lambda$ eine Überlagerung vom Grad 2, da ja $\wp_\Lambda$ als elliptische Funktion Ordnung 2 hat, und hat Verzweigung in $\frac{1}{2}\Lambda$. Es folgt die Behauptung.

(c) Mit (b) folgt die Behauptung daraus, dass die einzigen meromorphen Funktionen auf $\mathbb{C}/\Lambda$ die rationalen Funktionen in $\wp_\Lambda$ und $\wp'_\Lambda$ sind. Andererseits entsprechen die meromorphen Funktionen auf $\mathbb{C}/\Lambda$ ja bijektiv den $\Lambda$-elliptischen Funktionen auf $\mathbb{C}$, für die wir diese Aussage schon kennen.

(d) Seien $z_1, z_2 \in \mathbb{C}$. Nach dem Abel'schen Theorem gibt es eine elliptische Funktion $\phi$ mit Null- und Polstellendivisor

$$(\phi) = (z_1 + z_2) - (z_1) - (z_2) + (0).$$

Nach (c) ist $\phi$ der Pullback $\psi^* f$ einer rationalen Funktion $f$. Da $\psi : \mathbb{C}/\Lambda \to E_\Lambda$ nach (b) ein Isomorphismus von Riemann'schen Flächen ist, ist $\psi^*$ ein Isomorphismus zwischen den Funktionenkörpern, und es gilt für jeden Punkt $z \in \mathbb{C}/\Lambda$

$$\mathrm{ord}_{\psi(z)}(f) = \mathrm{ord}_z(\psi^* f) = \mathrm{ord}_z(\phi).$$

Damit können wir die obige Gleichung via $\psi$ auf die elliptische Kurve $E_\Lambda$ übertragen und erhalten

$$(f) = (\psi(z_1 + z_2)) - (\psi(z_1)) - (\psi(z_2)) + (\psi(0)). \tag{13}$$

[8] Was ja wunderbar zur entsprechenden Aussage über algebraische Kurven passt, die wir schon verwendet haben. Das liegt natürlich daran, dass der hier skizzierte Zusammenhang zwischen algebraischen Kurven und Riemann'schen Flächen in größerer Allgemeinheit gilt. Für einen Beweis der Aussage siehe zum Beispiel [For].

Andererseits gilt für einen beliebigen Divisor $D = \sum_P n_P(P)$ auf $E_\Lambda$

$$D \text{ Hauptdivisor } \implies \bigoplus_P n_P P = O,$$

wo $\oplus$ die Gruppenverknüpfung der elliptischen Kurve bezeichnet,

*denn:* Erinnern wir uns daran, dass das Gruppengesetz auf $E_\Lambda$ vermöge der Abbildung $\Phi$ definiert werden kann, die $P$ auf $(P) - (O)$ schickt. Sei also $D = (\phi)$ ein Hauptdivisor wie in der Behauptung. Dann gilt

$$\Phi(\bigoplus_P n_P P) = \sum_P n_P\big((P) - (O)\big) = (\phi) - \sum_P n_P(O) = (O) = \Phi(O).$$

#

Wenn wir dies auf (13) anwenden, fallen die Terme $(f)$ und $(\psi(0))$ weg und wir erhalten

$$\psi(z_1 + z_2) = \psi(z_1) \oplus \psi(z_2)$$

und damit die Behauptung □

**Bemerkung** *Elliptische Kurven haben auch die Struktur einer Liegruppe, das heißt, sowohl Gruppenverknüpfung als auch Inversenbildung sind stetig. Das führt dazu, dass man entlang Pfaden auf elliptischen Kurven integrieren kann. Das natürliche Differential ist hierbei $\frac{dx}{y}$, denn sein Pullback ist das natürliche Differential $dz$ auf $\mathbb{C}/\Lambda$:*

$$dz = \frac{d\wp_\Lambda(z)}{\wp'_\Lambda(z)} = \psi^*\left(\frac{dx}{y}\right).$$

*Auf diese Weise kann man die Umkehrabbildung zum Isomorphismus $\psi$ konstruieren. Seien $\gamma_1$ und $\gamma_2$ Erzeuger der Fundamentalgruppe der elliptischen Kurve $E_\Lambda$. Dann spannen die Integralwerte*

$$\int_{\gamma_1} \frac{dx}{y} \quad \text{und} \quad \int_{\gamma_2} \frac{dx}{y}$$

*das Gitter $\Lambda \subset \mathbb{C}$ auf. Sie heißen die **Perioden** von $E_\Lambda$ und sind eine wichtige geometrische Invariante. Da elliptische Kurven keine Singularitäten haben, ist die Integration ansonsten wohldefiniert, und man kann zeigen, dass*

$$\psi^{-1} : \begin{cases} E_\Lambda & \to \mathbb{C}/\Lambda, \\ P & \mapsto \int_O^P \frac{dx}{y} \bmod \Lambda \end{cases}$$

*gilt.*

Kehren wir nun zur $j$-Invarianten zurück. In (12) hatten wir jedem Gitter $\Lambda$ einen Wert $j(\Lambda)$ zugewiesen. Dieser hängt nur von den Größen

$$g_2(\Lambda) = 60\ G_4(\Lambda) \quad \text{und} \quad g_3(\Lambda) = 140\ G_6(\Lambda)$$

ab, so dass wir gleich für jedes Paar $(g_2, g_3) \in \mathbb{C}^2$ mit $g_2^3 - 27g_3^2 \neq 0$ einen $j$-Wert

$$j(g_2, g_3) = \frac{1728\ g_2^3}{g_2^3 - 27\ g_3^2}$$

einführen können. Motiviert durch den Isomorphismus in 4.2 (b) wollen wir diesen Wert die ***j-Invariante*** der elliptischen Kurve $E(g_2, g_3)$ mit (affiner) Weierstraßgleichung $y^2 = 4x^3 - g_2x - g_3$ nennen. Wir sollten aber zunächst die Frage der Wohldefiniertheit klären: Damit die $j$-Invariante einer elliptischen Kurve ein sinnvoller Begriff ist, sollte sie für isomorphe elliptische Kurven gleich sein. Wir müssen dafür ein wenig ausholen und zunächst die umgekehrte Folgerung zeigen.

**Proposition 4.3** *Für Paare* $(g_2, g_3), (g_2', g_3') \in \mathbb{C}^2$ *mit* $g_2^3 - 27\, g_3^2 \neq 0 \neq (g_2')^3 - 27\, (g_3')^2$ *gilt*

$$j(g_2, g_3) = j(g_2', g_3') \implies E(g_2, g_3) \cong E(g_2', g_3').$$

*Beweis.* Nehmen wir an, es gelte $g_2', g_3' \neq 0$. Nach Voraussetzung gilt

$$\frac{g_2^3}{g_2^3 - 27\, g_3^2} = \frac{(g_2')^3}{(g_2')^3 - 27\, (g_3')^2}.$$

Mit $g_2'$ ist dann auch $g_2$ ungleich Null, so dass wir auf die Gleichheit der Kehrwerte schließen können und damit auf

$$\left(\frac{g_3}{g_3'}\right)^2 = \left(\frac{g_2}{g_2'}\right)^3 = c^{-6} \in \mathbb{C}^\times.$$

Die Abbildung $f : (x, y) \mapsto (cx, c^{\frac{3}{2}} y)$ bildet dann die Weierstraßgleichung von $E(g_2, g_3)$ auf die von $E(g_2', g_3')$ ab und ist offensichtlich ein Isomorphismus von elliptischen Kurven.

Für $g_2' g_3' = 0$ ist die Argumentation eine ganz ähnliche. □

Wir haben hiermit gezeigt, dass eine beliebige elliptische Kurve $E(g_2, g_3)$ die Gestalt eines komplexen Torus hat. Wir können nämlich wegen der Surjektivität von $j$ und Proposition 4.1 stets ein Gitter $\Lambda$ wählen, dessen $j$-Invariante gleich $j(g_2, g_3)$ ist. Dann gilt nach der Proposition

$$E(g_2, g_3) \cong E(g_2(\Lambda), g_3(\Lambda)) \cong \mathbb{C}/\Lambda.$$

**Proposition 4.4** (a) *Die analytischen Abbildungen* $g : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ *mit* $g(0) = 0$ *sind genau die Abbildungen, die von Multiplikationsabbildungen der Art*

$$m_\alpha : \begin{cases} \mathbb{C} & \to \mathbb{C}, \\ z & \mapsto \alpha z \end{cases}$$

*herkommen, wo* $\alpha\Lambda_1 \subseteq \Lambda_2$ *gilt.*

(b) *Seien* $E_1$ *und* $E_2$ *zwei elliptische Kurven und* $O_1$ *und* $O_2$ *die zugehörigen Punkte bei unendlich. Für* $i = 1, 2$ *sei* $E_i$ *isomorph zum Gitter* $\mathbb{C}/\Lambda_i$ *mit entsprechendem Isomorphismus* $\psi_i$ *wie in Proposition 4.2. Dann ist die Abbildung* $g$ *im kommutativen Diagramm*

$$\begin{array}{ccc} \mathbb{C}/\Lambda_1 & \xrightarrow{g} & \mathbb{C}/\Lambda_2 \\ {\scriptstyle\psi_1}\downarrow & & \downarrow{\scriptstyle\psi_2} \\ E_1 & \xrightarrow[f]{} & E_2 \end{array}$$

*genau dann eine analytische Abbildung mit $g(0) = 0$, wenn $f$ eine Isogenie ist. Analytische Abbildungen, die Null fixieren, und Isogenien sind also im Prinzip dasselbe.*

*Beweis.* (a) Jede analytische Abbildung $g : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ mit $g(0) = 0$ hat einen ***Lift*** $\tilde{g}$, also eine analytische Abbildung $\tilde{g} : \mathbb{C} \to \mathbb{C}$ mit $\tilde{g}(0) = 0$, für die das Diagramm

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\tilde{g}} & \mathbb{C} \\ {\scriptstyle \pi_1}\downarrow & & \downarrow{\scriptstyle \pi_2} \\ \mathbb{C}/\Lambda_1 & \xrightarrow[g]{} & \mathbb{C}/\Lambda_2 \end{array}$$

kommutiert. Wegen dieser Kommutativität gilt dann für ein festes $\omega \in \Lambda_1$

$$\pi_2(\tilde{g}(z+\omega)) = g(\pi_1(z+\omega)) = g(\pi_1(z)) = \pi_2(\tilde{g}(z)). \tag{14}$$

$\tilde{g}$ ist stetig und $\Lambda_2$ ist diskret, weshalb es nach (14) für jedes $\omega \in \Lambda_1$ eine Konstante $c_\omega$ gibt mit

$$\tilde{g}(z+\omega) - \tilde{g}(z) = c_\omega.$$

Daraus folgt durch Ableiten, dass $\tilde{g}'$ eine $\Lambda_1$-elliptische Funktion ist. Andererseits ist sie als Ableitung einer holomorphen Funktion aber auch holomorph und somit nach dem 1. Liouville'schen Satz konstant. Da wir $\tilde{g}(0) = 0$ vorausgesetzt hatten, folgt $\tilde{g} = m_\alpha$ mit einem $\alpha \in \mathbb{C}$. Eine weitere Anwendung von (14) zeigt, dass $\alpha\Lambda_1 \subseteq \Lambda_2$ gelten muss. Umgekehrt ist klar, dass jede solche Abbildung $m_\alpha$ tatsächlich eine analytische Abbildung von $\mathbb{C}/\Lambda_1$ nach $\mathbb{C}/\Lambda_2$ induziert.

(b) Eine Isogenie ist insbesondere ein Morphismus, also eine überall definierte rationale Funktion, so dass mit der Form der Kartenabbildungen (10) klar ist, dass die induzierte Abbildung $g$ holomorph sein muss, wenn $f$ eine Isogenie ist. Wir wollen nun auch die Umkehrung zeigen.

Nach (a) genügt es, Funktionen $g$ mit $\tilde{g} = m_\alpha$ mit $\alpha \in \mathbb{C}^\times$ zu betrachten, für die $\alpha\Lambda_1 \subseteq \Lambda_2$ gilt. Die induzierte Funktion auf den Weierstraßgleichungen sieht dann wie folgt aus:

$$f : \begin{cases} E_1 & \to E_2, \\ [\wp_{\Lambda_1}(z) : \wp'_{\Lambda_1}(z) : 1] & \mapsto [\wp_{\Lambda_2}(\alpha z) : \wp'_{\Lambda_2}(\alpha z) : 1], \end{cases}$$

wo wir die Funktionen $\pi_1$ und $\pi_2$ in der Notation unterschlagen, da die Weierstraßfunktionen ja schon als Funktionen auf ganz $\mathbb{C}$ definiert sind. Dass $f$ überall definiert ist, folgt wie für die andere Richtung, und dass $f(O_1) = O_2$ gilt, ist mit $\alpha\Lambda_1 \subseteq \Lambda_2$ klar. Wir müssen nun noch zeigen, dass $\wp_{\Lambda_2}(\alpha z)$ und $\wp'_{\Lambda_2}(\alpha z)$ als Funktionen in $\wp_{\Lambda_1}(z)$ und $\wp'_{\Lambda_1}(z)$ rational sind. Aber wenn wir $\alpha\Lambda_1 \subseteq \Lambda_2$ ausnutzen, sehen wir, dass für jedes $\omega \in \Lambda_1$

$$\wp_{\Lambda_2}(\alpha(z+\omega)) = \wp_{\Lambda_2}(\alpha z + \alpha\omega) = \wp_{\Lambda_2}(\alpha z)$$

gilt und ebenso die analoge Aussage für $\wp'_{\Lambda_2}$. Es sind also $\wp_{\Lambda_2}(\alpha z)$ und $\wp'_{\Lambda_2}(\alpha z)$ in $K(\Lambda_1) = \mathbb{C}(\wp_{\Lambda_1}, \wp'_{\Lambda_1})$, was die Behauptung zeigt. □

**Korollar 4.5** *Zwei elliptische Kurven $E_1 \cong \mathbb{C}/\Lambda_1$ und $E_2 \cong \mathbb{C}/\Lambda_2$ sind genau dann isogen, wenn es ein $\alpha \in \mathbb{C}^\times$ gibt mit $\alpha\Lambda_1 \subseteq \Lambda_2$, und genau dann isomorph, wenn $\Lambda_1$ und $\Lambda_2$ homothetisch sind.*

Wir können nun endlich zeigen, dass der oben eingeführte Begriff der $j$-Invariante einer elliptischen Kurve wohldefiniert ist. Dies gilt,

*denn:* Seien $E(g_2, g_3)$ und $E(g_2', g_3')$ zwei isomorphe elliptische Kurven. Wegen der Surjektivität der $j$-Funktion und Proposition 4.1 können wir Gitter $\Lambda$ und $\Lambda'$ mit $j(g_2, g_3) = j(\Lambda)$ und $j(g_2', g_3') = j(\Lambda')$ wählen. Nach den Propositionen 4.2 und 4.3 gilt dann

$$\mathbb{C}/\Lambda \cong E(g_2, g_3) \cong E(g_2', g_3') \cong \mathbb{C}/\Lambda'.$$

Nach Proposition 4.4 (b) sind also $\Lambda$ und $\Lambda'$ homothetisch und haben so dieselbe $j$-Invariante. #

Insgesamt haben wir in diesem Abschnitt gezeigt

**Satz 4.6** *Jede Isomorphieklasse von elliptischen Kurven entspricht einem komplexen Torus $\mathbb{C}/\Lambda$, genauer gilt für je zwei elliptische Kurven $E, E'$*

$$j(E) = j(E') \quad \Longleftrightarrow \quad E \cong E'.$$

Unseren Wert $j(\frac{1+\sqrt{-163}}{2})$ können wir nun als die $j$-Invariante einer geeigneten Isomorphieklasse elliptischer Kurven auffassen. Im nächsten Abschnitt wird sich herausstellen, dass die $j$-Invarianten von elliptischen Kurven mit besonders vielen Endomorphismen algebraische Zahlen sind, was gut ist, wollen wir in unserem Spezialfall doch zeigen, dass $j(\frac{1+\sqrt{-163}}{2})$ eine ganze Zahl ist!

## 5 Komplexe Multiplikation

Am Ende des Abschnitts über elliptische Kurven haben wir Endomorphismen eingeführt und als Beispiel die Multiplikation $[m]$ mit einer ganzen Zahl betrachtet. Üblicherweise hat eine elliptische Kurve $E$ keine weiteren Endomorphismen mehr, so dass $\mathrm{End}(E) \cong \mathbb{Z}$ gilt. Ist $\mathrm{End}(E)$ echt größer als $\mathbb{Z}$, so sagen wir, $E$ habe ***komplexe Multiplikation***. Wir werden bald sehen, wie sich diese Bezeichnung rechtfertigt.

**Beispiel** *Betrachten wir*

$$E : y^2 = x^3 - x.$$

*Dann enthält* $\mathrm{End}(E)$ *offensichtlich ein Element*

$$[i] : (x, y) \mapsto (-x, iy)$$

*mit $[i] \circ [i] = [-1]$, so dass der Endomorphismenring den Ring $\mathbb{Z}[i]$ enthält. Tatsächlich gilt sogar* $\mathrm{End}(E) \cong \mathbb{Z}[i]$.

Eine direkte Folgerung aus Proposition 4.4 ist, dass für eine beliebige elliptische Kurve $E_\Lambda$ wie in Proposition 4.2

$$\mathrm{End}(E_\Lambda) \cong \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subseteq \Lambda\}$$

gilt. $\mathrm{End}(E_\Lambda)$ ist also ein kommutativer, torsionsfreier $\mathbb{Z}$-Modul, dessen genaue Gestalt (von der Homothetieklasse von) $\Lambda$ abhängt. Da es ja immer ein $\tau \in \mathbb{H}$ gibt, so dass $\Lambda$ zu $\mathbb{Z} + \tau\mathbb{Z}$ homothetisch ist, nehmen wir von ab jetzt ohne Einschränkung an, dass $\Lambda$ von dieser Gestalt ist. Damit können wir nun die Bedingung $\alpha\Lambda \subseteq \Lambda$ für die Elemente des Endomorphismenrings umschreiben in

$$\alpha \cdot 1 \in \Lambda \quad \text{und} \quad \alpha \cdot \tau \in \Lambda,$$

also in

$$\exists a, b, c, d \in \mathbb{Z}: \quad \alpha = a\tau + b \quad \text{und} \quad (a\tau + b)\tau = c\tau + d. \tag{15}$$

Es gibt nun zwei Fälle:

**Fall 1:** Wenn $\tau$ nicht gerade Nullstelle eines quadratischen Polynoms mit ganzen Koeffizienten ist, gilt offensichtlich $a = 0$ und also $\alpha \in \mathbb{Z}$, so dass $\mathrm{End}(E_\Lambda) \cong \mathbb{Z}$ gilt.

**Fall 2:** Nehmen wir nun an, $\tau \in \mathbb{H}$ habe ein quadratisches Minimalpolynom $AX^2 + BX + C \in \mathbb{Z}[X]$, wobei wir ohne Einschränkung annehmen, dass $\mathrm{ggT}(A, B, C) = 1$ gilt. Aus (15) können wir dann sofort

$$\alpha\Lambda \subseteq \Lambda \quad \Longleftrightarrow \quad \Big(\alpha = a\tau + b \text{ mit } a, b \in \mathbb{Z} \ \wedge \ A \mid a\Big)$$

ablesen,

*denn:* „$\Rightarrow$“: Wir können die Bedingung in (15) umformulieren zu

$$\exists a, b, e, f \in \mathbb{Z}: \quad \alpha = a\tau + b \quad \text{und} \quad a\tau^2 + e\tau + f = 0. \tag{16}$$

Letztere quadratische Gleichung muss ein Vielfaches von der minimalen Gleichung zu $\tau$ sein, so dass wir $A \mid aB$ und $A \mid aC$ haben, und insbesondere $A \mid (a \ \mathrm{ggT}(B, C))$. Da aber nach Voraussetzung $ggT(A, \mathrm{ggT}(B, C)) = 1$ gilt, folgt $A \mid a$.

„$\Leftarrow$“: Wir zeigen (16). Es gilt $A \mid a$, wir können also $a = Ag$ schreiben mit einem $g \in \mathbb{Z}$. Es gilt

$$0 = A\tau^2 + B\tau + C = a\tau^2 + gB\tau + gC,$$

was zu zeigen war. #

Es folgt

$$\mathrm{End}(E_\Lambda) \cong \mathbb{Z} \oplus (A\tau)\mathbb{Z}.$$

**Bemerkung** *Aus dem bisher gesagten lässt sich bereits eine Aussage über die möglichen Grade von Endomorphismen einer elliptischen Kurve $E_\Lambda$ herleiten. Geometrisch ist nämlich klar, dass der Grad des Endomorphismus', der zur Multiplikationsabbildung $m_\alpha : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$ mit $\alpha \in \mathbb{C}$ gehört, $|\alpha|^2$ ist. Beispielsweise ist der Grad der Isogenie $[m]$ durch $m^2$ gegeben. Im Fall 2 durften wir außerdem ohne*

*Einschränkung annehmen, dass $\Lambda = \mathbb{Z} \oplus \tau\mathbb{Z}$ mit $A\tau^2 + B\tau + C = 0$ und paarweise teilerfremden $A, B, C \in \mathbb{Z}$ gilt. Dann war ja $\mathrm{End}(E_\Lambda) \cong \mathbb{Z} \oplus (A\tau)\mathbb{Z}$, so dass die möglichen Grade von Endomorphismen von $E_\Lambda$ nach der geometrischen Vorüberlegung gerade die Werte der quadratischen Form*

$$Q(X, Y) = X^2 + A(\tau + \bar{\tau})XY + A^2|\tau|^2Y^2$$

*sind.*

Unser Überblick über die Endomorphismen elliptischer Kurven lässt sich mit ein wenig Vokabular noch hübscher formulieren. Dafür führen wir ein:

**Definition 5.1** *Eine **Ordnung** in einem Zahlkörper K ist ein Teilring $\mathcal{O}$, der folgenden Bedingungen genügt:*

(i) $1 \in \mathcal{O}$,

(ii) *$\mathcal{O}$ ist als $\mathbb{Z}$-Modul endlich erzeugt,*

(iii) $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q} = K$.

*Die Menge der Ordnungen von K ist bezüglich der Inklusion geordnet und hat ein maximales Element, den **Ganzzahlring** $\mathcal{O}_K$ von K.*

**Bemerkung** *Der Ganzzahlring heißt so, weil er aus den Elementen von K besteht, die **ganz** über $\mathbb{Z}$, also Nullstelle eines normierten Polynoms mit ganzzahligen Koeffizienten sind. Das ist die „richtige" Entsprechung von Algebraizität auf Ringniveau, denn auf diese Weise spielt $\mathcal{O}_K$ in K in vielen Fragen der Zahlentheorie die gleiche Rolle wie $\mathbb{Z}$ in $\mathbb{Q}$. Insbesondere gibt es immer auch eine Basis des $\mathbb{Q}$-Vektorraums K, die bereits aus Elementen von $\mathcal{O}_K$ besteht. Diese ist dann auch eine Basis des freien $\mathbb{Z}$-Moduls $\mathcal{O}_K$ und heißt eine **Ganzheitsbasis** von $\mathcal{O}_K$.*

**Beispiel** *Es stellt sich heraus, dass man für imaginär-quadratische Zahlkörper stets eine Ganzheitsbasis der Form $\{1, \tau\}$ mit $K = \mathbb{Q}(\tau)$ wählen kann. Diese findet man, indem man mit einem allgemeinen Element $r + \tau s \in \mathbb{Q}(\tau)$ mit $r, s \in \mathbb{Q}$ ansetzt und annimmt, dass dieses eine Ganzheitsgleichung $\tau^2 + A\tau + B = 0$ mit $A, B \in \mathbb{Z}$ erfüllt. Daraus lassen sich dann Bedingungen an $r, s$ ablesen.*

(a) *Der Ganzzahlring des imaginär-quadratischen Zahlkörpers $\mathbb{Q}(i)$ ist $\mathbb{Z}[i] = \mathbb{Z} \oplus i\mathbb{Z}$, eine Ganzheitsbasis ist durch $\{1, i\}$ gegeben.*

(b) *Anders ist das im Fall des imaginär-quadratischen Zahlkörpers $\mathbb{Q}(\sqrt{-163})$, wo $\mathbb{Z}[\sqrt{-163}]$ keine maximale Ordnung ist, da zum Beispiel $\alpha = \frac{1}{2}(1 + \sqrt{-163})$ die Ganzheitsgleichung*

$$\alpha^2 - \alpha + 41 = 0$$

*erfüllt. Hier ist $\mathbb{Z}[\alpha]$ der Ganzheitsring und $\{1, \alpha\}$ eine Ganzheitsbasis.*

Wenden wir dies auf die Situation im zweiten Fall an, so sehen wir, dass $\mathrm{End}(E_\Lambda) \cong \mathbb{Z} \oplus (A\tau)\mathbb{Z}$ offensichtlich eine Ordnung im Zahlkörper $\mathbb{Q}(\tau)$ ist. Zusammengefasst erhalten wir

**Satz 5.2** *Sei $E_\Lambda$ eine elliptische Kurve, und bezeichne $\iota : \mathrm{End}(E_\Lambda) \to \mathbb{C}$ die in Proposition 4.4 beschriebene Abbildung mit Bild $\{\alpha \in \mathbb{C} \mid \alpha\Lambda \subseteq \Lambda\}$. Dann ist $\iota(\mathrm{End}(E))$ entweder $\mathbb{Z}$ oder eine Ordnung in einem imaginär-quadratischen Zahlkörper.*[9]

Interessant ist jetzt auch die umgekehrte Frage: Wann ist $\mathrm{End}(E_\Lambda)$ isomorph zu einer gegebenen Ordnung $\mathcal{O}$ eines imaginär-quadratischen Zahlkörpers $K$? Wir nähern uns dieser Frage in einer Reihe von Lemmata.

Um nicht Ordnungen in Zahlkörpern in aller Ausführlichkeit studieren zu müssen, schränken wir uns zur Beantwortung dieser Frage auf den Fall $\mathcal{O} = \mathcal{O}_K$ ein. Da alle Körpererweiterungen von $\mathbb{Q}$ separabel sind, folgt mit dem Satz vom primitiven Element, dass $K$ von der Gestalt $\mathbb{Q}(\tau)$ mit $\tau \in \mathbb{C}$ ist. Da $K$ als imaginär-quadratisch angenommen war, ist $\tau$ nicht reell, und wir können ohne Einschränkung annehmen, dass $\{1, \tau\}$ eine Ganzheitsbasis von $\mathcal{O}_K$ ist.

**Lemma 5.3** *Ist ein Ring $R \subseteq \mathbb{C}$ isomorph zu $\mathcal{O}_K$, dann gilt schon $R = \mathcal{O}_K$.*

*Beweis.* Nennen wir den Isomorphismus $\varphi : R \to \mathcal{O}_K$. Da $\mathcal{O}_K$ ein Ring mit Eins ist, gilt $\varphi(1) = 1_R$. Da $\varphi$ ein Isomorphismus ist, folgt $\varphi(\mathbb{Z}) \cong \mathbb{Z}$. Andererseits hatten wir ja $R \subseteq \mathbb{C}$ angenommen, weshalb $1_R = 1 \in \mathbb{Z}$ ist und sogar $\varphi(\mathbb{Z}) = \mathbb{Z}$ gilt.

Jedes $\eta \in \mathcal{O}_K \setminus \mathbb{Z}$ ist nun Nullstelle eines irreduziblen normierten quadratischen Polynoms $P_\eta(X) = X^2 + AX + B \in \mathbb{Z}[X]$. Die andere Nullstelle[10] dieses Polynoms lautet $\eta' := -A - \eta$, was ebenfalls in $\mathcal{O}_K$ liegt. Wenden wir nun $\varphi$ auf $P_\eta$ an, so sehen wir, dass $\{\varphi(\eta), \varphi(\eta')\} = \{\eta, \eta'\}$ gilt. $\varphi$ vertauscht also schlimmstenfalls Nullstellen von quadratischen Polynomen miteinander, und es gilt in jedem Fall $R = \mathcal{O}_K$. □

**Lemma 5.4** *Falls $\mathrm{End}(E_\Lambda) \cong \mathcal{O}_K$ gilt, so gibt es eine Homothetie zwischen $\Lambda$ und einem Untergitter von $\mathcal{O}_K$.*

*Beweis.* Sei ohne Einschränkung $\Lambda = \mathbb{Z} \oplus \eta\mathbb{Z}$. Aus der Annahme folgt mit dem vorigen Lemma sofort $\iota(\mathrm{End}(E_\Lambda)) = \mathcal{O}_K$, so dass insbesondere $\tau \subseteq \Lambda$ gilt, oder ausgeschrieben, dass es $a, b \in \mathbb{Z}$, $b \neq 0$, gibt mit $\tau = a \cdot 1 + b \cdot \eta$. Wir können dies umformen zu

$$\eta = \frac{1}{b}(\tau - a).$$

Ganz offensichtlich ist also $\Lambda$ homothetisch zu einem Untergitter von $\mathcal{O}_K$. □

Ein Untergitter von $\mathcal{O}_K$ ist eine abelsche Gruppe. Außerdem ist das hier relevante Untergitter abgeschlossen unter Multiplikation mit Elementen von $\mathcal{O}_K$, denn wir haben soeben im Beweis von Lemma 5.4 gesehen, dass es ganze $a, b$ mit $\tau = a \cdot 1 + b \cdot \eta$ gibt, so dass in der Notation von Lemma 5.3 gilt:

$$\tau \cdot 1 = a \cdot 1 + b \cdot \eta \in \Lambda \quad \text{und} \quad \tau \cdot \eta = a \cdot \eta + b \cdot \eta^2 = (-B) \cdot 1 + (a - A) \cdot \eta \in \Lambda.$$

Das fragliche Untergitter ist also ein Ideal von $\mathcal{O}_K$. Es gilt sogar

[9] Die Bezeichnung „komplexe Multiplikation“ sollte nun klar sein.

[10] Das sieht man leicht mit Polynomdivision.

**Lemma 5.5** *Genau dann ist $\iota(\mathrm{End}(E_\Lambda)) = \mathcal{O}_K$, wenn es eine Homothetie zwischen $\Lambda$ und einem Ideal $\Lambda'$ von $\mathcal{O}_K$ gibt.*

*Beweis.* Die Hinrichtung haben wir bereits gezeigt. Gibt es andererseits eine Homothetie zwischen $\Lambda$ und einem Ideal $\Lambda' \trianglelefteq \mathcal{O}_K$, so folgt mit der Idealeigenschaft und $\iota(\mathrm{End}(E_\Lambda)) = \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subseteq \Lambda\}$ sofort, dass $\mathcal{O}_K$ eine Untergruppe von $\iota(\mathrm{End}(E_\Lambda))$ ist. Es bleibt zu zeigen, dass $\iota(\mathrm{End}(E_\Lambda))$ nicht größer als $\mathcal{O}_K$ sein kann.

Sei dafür $\Lambda' = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ und $\alpha \in \iota(\mathrm{End}(E_\Lambda))$. Dann gibt es $c, d \in \mathbb{Z}$ mit

$$\alpha\omega_1 = c\omega_1 + d\omega_2,$$

da ja $\alpha\Lambda \subseteq \Lambda$ gilt und $\Lambda'$ und $\Lambda$ sich nur um einen Faktor aus $\mathbb{C}^\times$ unterscheiden. Insbesondere gilt also $\alpha \in \mathbb{Q}(\omega_1, \omega_2) \subseteq \mathbb{Q}(\tau) = K$. Andererseits ist $\alpha$ nach Satz 5.2 als Element einer Ordnung eines algebraischen Zahlkörpers ganz über $\mathbb{Z}$, so dass $\alpha$ bereits in $\mathcal{O}_K$ liegen muss. □

Um diese Ergebnisse nett zusammenzufassen, lohnt es sich, den Ganzzahlring $\mathcal{O}_K$ noch besser kennenzulernen und dafür ein paar Begriffe aus der algebraischen Zahlentheorie einzuführen.

Als Gitter in $\mathbb{C}$ ist $\mathcal{O}_K$ nullteilerfrei und ***noethersch***, das heißt, jedes Ideal ist endlich erzeugt. Da für drei Ringe $R, S, T$ mit $S$ ganz über $R$ und $T$ ganz über $S$ immer auch $T$ ganz über $R$ ist (siehe Satz (2.4) in [Neu], Kapitel I), ist $\mathcal{O}_K$ auch ***ganzabgeschlossen*** in seinem Quotientenkörper, also $K$, enthält also alle Elemente von $K$, die ganz über $\mathcal{O}_K$ sind. Zu guter Letzt ist in $\mathcal{O}_K$ jedes von Null verschiedene Primideal ein maximales Ideal,

*denn:* Sei $\mathfrak{p}$ ein solches Primideal. Dann ist $\mathfrak{p} \cap \mathbb{Z}$ ein von Null verschiedenes Primideal $(p) \trianglelefteq \mathbb{Z}$: Die Primidealeigenschaft ist klar, und andererseits gibt es immer ein $0 \neq \alpha \in \mathfrak{p}$, das eine Ganzheitsgleichung

$$\alpha^2 + A\alpha + B = 0$$

mit $A, B \in \mathbb{Z}$ und $B \neq 0$ erfüllt. Das zugehörige $B$ liegt dann bereits in $\mathfrak{p} \cap \mathbb{Z}$, so dass $\mathfrak{p} \cap \mathbb{Z}$ nicht Null ist. Der nullteilerfreie Ring $\mathcal{O}_K/\mathfrak{p}$ entsteht aus $\mathbb{Z}/p\mathbb{Z}$ durch Ringadjunktion eines algebraischen Elements, nämlich der Restklasse modulo $\mathfrak{p}$ der Elemente der Ganzheitsbasis, und ist also ein Körper. Daher ist $\mathfrak{p}$ ein maximales Ideal. #

Ein Ring mit den aufgezählten Eigenschaften heißt auch ***Dedekindring***. Für diese gilt eine sehr schöne Verallgemeinerung der eindeutigen Primfaktorzerlegung, die wir von den ganzen Zahlen kennen. Definieren wir nämlich das ***Produkt*** zweier Ideale $\mathfrak{a}, \mathfrak{b}$ eines Dedekindrings $R$ als

$$\mathfrak{ab} = \{\sum_i \alpha_i\beta_i \mid \alpha_i \in \mathfrak{a},\ \beta_i \in \mathfrak{b}\},$$

so gilt

**Proposition 5.6** *Jedes von $(0)$ und $(1)$ verschiedene Ideal $\mathfrak{a}$ eines Dedekindrings $R$ besitzt eine bis auf die Reihenfolge eindeutige Zerlegung*

$$\mathfrak{a} = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$$

*in Primideale $\mathfrak{p}_i$ von $R$.*

*Beweis.* [Neu], §I.3 □

**Bemerkung** *Das kompliziertere Konzept einer Zerlegung in Primideale und nicht Primelemente ist nötig, da für Zahlkörper K letztere nicht eindeutig wäre. So hat zum Beispiel die Zahl 6 zum Beispiel in* $\mathbb{Z}[\sqrt{-5}]$ *zwei Zerlegungen in irreduzible Elemente:*

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

*Das liegt daran, dass beispielsweise das Ideal* $(2)$ *nicht prim ist, sondern von*

$$(2, 1 - \sqrt{-5}) = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z},\ a \equiv b \bmod (2)\}$$

*geteilt wird. Ein Grund für das Missglücken der elementweisen eindeutigen Primfaktorzerlegung ist also, dass* $\mathbb{Z}[\sqrt{-5}]$ *kein Hauptidealring ist.*

Man kann zu einem Ideal $\mathfrak{a} \neq (0)$ eines Dedekindrings $R$ ein multiplikatives Inverses

$$\mathfrak{a}^{-1} = \{\alpha \in \mathrm{Quot}(R) \mid \alpha\mathfrak{a} \subseteq R\}$$

einführen. Die Menge der Ideale samt ihrer Inversen ist gerade die Menge der endlich erzeugten $R$-Untermoduln von $\mathrm{Quot}(R)$ und heißt die Menge der ***gebrochenen Ideale*** von $\mathrm{Quot}(R)$. Die Multiplikation und Inversenbildung lassen sich auf diese Menge fortsetzen und geben ihr die Struktur einer Gruppe, der ***Idealgruppe*** $I_K$ von $K$ (siehe Satz (3.8) in [Neu], Kapitel I). Wie wir in der Bemerkung gesehen haben, kann das Vorhandensein von Idealen, die keine Hauptideale sind, ein Anzeichen dafür sein, dass die elementweise eindeutige Primfaktorzerlegung schiefgeht. Daher studiert man die ***Idealklassengruppe***

$$\mathcal{C}\ell_K = I_K / \{\text{Hauptideale}\}$$

und betrachtet ihre Ordnung, die ***Klassenzahl*** $h_K$ von $K$, als ein Maß dafür, „wie sehr" $\mathcal{O}_K$ nicht faktoriell ist. Mit Minkowskitheorie kann man zeigen, dass sie immer eine endliche Zahl ist, siehe zum Beispiel Theorem (6.3) in [Neu], Kapitel I.

Wieder zurück bei unserem eigentlichen Problem sehen wir direkt aus der Definition der Idealklassengruppe, dass zwei Gitter $\Lambda, \Lambda' \trianglelefteq \mathcal{O}_K$ genau dann zu isomorphen Kurven $E_\Lambda \cong E_{\Lambda'}$ führen, wenn sie in derselben Idealklasse liegen. Zusammengefasst haben wir in den Lemmata 5.3 bis 5.5 gezeigt:

**Satz 5.7** *Sei K ein imaginär-quadratischer Zahlkörper mit Ganzzahlring* $\mathcal{O}_K$*. Dann gibt es eine* $(1:1)$*-Korrespondenz zwischen den Isomorphieklassen elliptischer Kurven mit Endomorphismenring isomorph zu* $\mathcal{O}_K$ *und der Idealklassengruppe* $\mathcal{C}\ell_K$*. Insbesondere ist die Anzahl der Isomorphieklassen gerade die Klassenzahl* $h_K$*.*

Wir wollen nun diesen Satz nutzen, um zu zeigen, dass die $j$-Invarianten von elliptischen Kurven mit komplexer Multiplikation algebraische Zahlen sind. Dazu sei $\sigma$ ein beliebiger Automorphismus in $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{C})$. Dieser operiert auf der Menge aller elliptischen Kurven (über $\mathbb{C}$) durch

$$E = E(g_2, g_3) \mapsto E^\sigma = E(g_2^\sigma, g_3^\sigma),$$

was zwei wichtige Konsequenzen hat:

- Sei $f = [\phi_0 : \phi_1 : \phi_2]$ mit $\phi_i \in \mathbb{C}[E] = \mathbb{C}[X, Y, Z]/I(E)$ ein Endomorphismus von $E$. $\sigma$ operiert über die Koeffizienten auf $\mathbb{C}[X, Y, Z]$ und schickt offensichtlich $I(E)$ nach $I(E^\sigma)$. Das führt zu wohldefinierten Elementen $\phi_i^\sigma$ von $\mathbb{C}(E^\sigma)$ und also zu einer rationalen Abbildung
$$f^\sigma = [\phi_0^\sigma : \phi_1^\sigma : \phi_2^\sigma]$$
auf $E^\sigma$, die $f^\sigma(P^\sigma) = f(P)^\sigma$ für alle $P \in E$ erfüllt, also auch Werte in $E^\sigma$ annimmt. Dass $f^\sigma$ auch eine Isogenie ist, folgt, weil $\sigma$ invertierbar ist und $O_{E^\sigma}$ festlässt. Insgesamt haben wir also gezeigt:
$$\mathrm{End}(E) \cong \mathrm{End}(E^\sigma).$$
- Da $j(E)$ eine rationale Funktion in $g_2, g_3$ ist, gilt auch
$$j(E^\sigma) = (j(E))^\sigma.$$

Diese können wir benutzen, um den folgenden Satz zu zeigen:

**Satz 5.8** *Sei $K$ ein imaginär-quadratischer Zahlkörper und $E$ eine elliptische Kurve mit* $\mathrm{End}(E) \cong \mathcal{O}_K$. *Dann ist $j(E)$ eine algebraische Zahl, genauer gilt*
$$[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq h_K,$$
*wo $h_K$ die Klassenzahl von $K$ ist.*

*Beweis.* Wie wir gerade eingesehen haben, gilt für alle $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{C})$
$$\mathrm{End}(E^\sigma) \cong \mathrm{End}(E) \cong \mathcal{O}_K.$$
Andererseits gibt es nach Satz 5.7 genau $h_K$ verschiedene Isomorphieklassen von elliptischen Kurven, deren Endomorphismenring zu $\mathcal{O}_K$ isomorph ist, so dass
$$|\{ \text{ Isomorphieklasse von } E^\sigma \mid \sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{C})\}| \leq h_K$$
gilt. Da $j$ nach Satz 4.6 Isomorphieklassen elliptischer Kurven parametrisiert, folgt
$$|\{j(E^\sigma) \mid \sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{C})\}| \leq h_K$$
und damit wegen $j(E^\sigma) = (j(E))^\sigma$ der Satz. □

## 6 Riemann'sche Flächen

Bevor wir nun zeigen können, dass die $j$-Invarianten von elliptischen Kurven mit komplexer Multiplikation sogar ganze algebraische Zahlen sind, also eine Ganzheitsgleichung mit Koeffizienten in $\mathbb{Z}$ erfüllen, müssen wir ein bisschen ausholen und erkennen, dass die Quotienten $\Gamma\backslash\mathbb{H}$ für diskrete Untergruppen $\Gamma$ von $\mathrm{SL}_2(\mathbb{R})$ „fast" die Struktur einer Riemann'sche Fläche tragen. Wir werden in diesem Abschnitt nicht alles beweisen und vereinfachend immer $\Gamma$ als Untergruppe von $\mathrm{SL}_2(\mathbb{Z})$ von endlichem Index ansehen.

Wir betrachten nun statt der oberen Halbebene $\mathbb{H}$ die ***erweiterte obere Halbebene***

$$\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}).$$

Wir können die $\mathrm{SL}_2(\mathbb{R})$-Struktur von $\mathbb{H}$ auf die erweiterte obere Halbebene fortsetzen, indem wir für die Matrizen $\sigma := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$

$$\begin{aligned} &\sigma(-\frac{d}{c}) = \infty \text{ und } \sigma(\infty) = \frac{a}{c} && \text{falls } c \neq 0, \\ &\sigma(\infty) = \infty && \text{falls } c = 0 \end{aligned}$$

setzen. $\mathrm{SL}_2(\mathbb{R})$ operiert auf diese Weise sogar transitiv auf $\mathbb{P}^1(\mathbb{R})$ und $\mathrm{SL}_2(\mathbb{Z})$ ebenso auf $\mathbb{P}^1(\mathbb{Q})$,

*denn:* Klar, dass $\mathrm{SL}_2(\mathbb{Z})$ operiert. Die Transitivität folgt, da für $a \in \{-1, 0, 1\}$

$$\begin{pmatrix} 0 & -1 \\ 1 & -a \end{pmatrix}(a) = \infty$$

gilt und es für $\frac{r}{s} \in \mathbb{Q}$ mit teilerfremden $r, s \in \mathbb{Z}$ ganze Zahlen $a, b$ mit $ar + bs = 1$ gibt, so dass $\frac{r}{s}$ von

$$\begin{pmatrix} a & b \\ -s & r \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

nach $\infty$ geschickt wird. Die Behauptung für $\mathrm{SL}_2(\mathbb{R})$ lässt sich genauso zeigen. #

Wir wollen nun den Quotienten $\Gamma\backslash\mathbb{H}^*$ mit einer Topologie versehen. Dazu geben wir zunächst zu jedem Punkt von $\mathbb{H}^*$ eine Umgebungsbasis an: Wir betrachten die Umgebungen

- offene Kreisscheiben in $\mathbb{H}$ mit Mittelpunkt $z \in \mathbb{H}$,
- $\{\infty\} \cup \{z \in \mathbb{H} \mid \mathrm{Im}(z) > c\}$ für alle positiven $c \in \mathbb{R}$,
- offene Kreisscheiben in $\mathbb{H}$ mit Tangentialpunkt $s \in \mathbb{Q}$.

Auf diese Weise sind die offenen Umgebungen von rationalen $s$ gerade die Bilder der offenen Umgebungen von $\infty$ unter $\Gamma$. Wir erhalten so offensichtlich eine Hausdorff'sche Topologie auf $\mathbb{H}^*$, und jedes Element von $\Gamma$ operiert als Homöomorphismus auf $\mathbb{H}^*$.

Wir statten $\Gamma\backslash\mathbb{H}^*$ mit der Quotiententopologie zu der auf $\mathbb{H}^*$ eingeführten Topologie aus. Deren offene Mengen sind durch

$$\{U \subseteq \Gamma\backslash\mathbb{H}^* \mid \pi^{-1}(U) \text{ ist offen in } \mathbb{H}^*\}$$

gegeben, wo $\pi$ die kanonische Projektion von $\mathbb{H}^*$ nach $\Gamma\backslash\mathbb{H}^*$ ist. Dann ist $\Gamma\backslash\mathbb{H}^*$ mit der gerade eingeführten Topologie ein zusammenhängender, kompakter Hausdorffraum (siehe Abschnitt 4.5 in [Kas] für den Beweis der Hausdorff-Eigenschaft).

Bevor wir nun eine komplexe Struktur auf $\Gamma\backslash\mathbb{H}^*$ definieren, teilen wir noch die Punkte der erweiterten oberen Halbebene in Klassen ein. Wir werden zu jedem Bildpunkt $\pi(z)$ mit $z \in \mathbb{H}^*$

eine Karte definieren, und das wird innerhalb jeder solchen Klasse auf dieselbe Art und Weise geschehen. Man unterteilt zunächst die Elemente von $\mathrm{SL}_2(\mathbb{R})$ in drei Typen. $\sigma \in \mathrm{SL}_2(\mathbb{R})$ heißt

$$\begin{aligned} \textbf{\textit{parabolisch}}, \text{ falls } & \operatorname{tr}(\sigma) = \pm 2 \text{ und } \sigma \neq \pm I_2, \\ \textbf{\textit{elliptisch}}, \text{ falls } & |\operatorname{tr}(\sigma)| < 2, \\ \textbf{\textit{hyperbolisch}}, \text{ falls } & |\operatorname{tr}(\sigma)| > 2. \end{aligned}$$

Für eine Untergruppe $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ von endlichem Index nennt man dann einen Punkt $z \in \mathbb{H}$ ***elliptischen bzw. parabolischen Punkt*** von $\Gamma$, wenn es ein elliptisches bzw. parabolisches Element $\sigma \in \Gamma$ gibt mit $\sigma(z) = z$. Parabolische Elemente heißen auch ***Spitzen***.

**Beispiel** *Sei $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. Dann ist $\infty$ eine Spitze, denn*

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}(\infty) = \infty \quad \text{und} \quad \operatorname{tr}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = 2.$$

*Wegen der Transitivität der Operation von $\mathrm{SL}_2(\mathbb{Z})$ auf $\mathbb{P}^1(\mathbb{Q})$ und der Konjugationsinvarianz der Spur ist damit auch jede rationale Zahl eine Spitze von $\mathrm{SL}_2(\mathbb{Z})$. Mit dem Satz von der Jordan'schen Normalform sieht man ein, dass dies alle Spitzen sind, was die bisherige Sprachregelung rechtfertigt.*

*Außerdem ist $\varrho = e^{2\pi i/3}$ ein elliptischer Punkt, denn*

$$\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}(\varrho) = \varrho \quad \text{und} \quad \operatorname{tr}\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} = 1.$$

*Man kann zeigen, dass $\varrho$ und $i$ bis auf $\mathrm{SL}_2(\mathbb{Z})$-Aktion die einzigen elliptischen Punkte sind.*

Für jedes $z \in \mathbb{H}^*$ gibt es eine Umgebung $U$, so dass für den Stabilisator $\Gamma_z = \{\sigma \in \Gamma \mid \sigma(z) = z\}$ von $z$ in $\Gamma$

$$\Gamma_z = \{\sigma \in \Gamma \mid \sigma(U) \cap U \neq \varnothing\}$$

gilt,

*denn:* Der Stabilisator $\Gamma_\infty$ von $\infty$ besteht offensichtlich genau aus den Matrizen $\sigma \in \Gamma$, deren Eintrag $c$ unten links gleich Null ist. Daraus folgt, dass $\Gamma_\infty$ zyklisch ist und modulo $\pm I_2$ von einem Element der Form $\pm\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)$ erzeugt wird. So hängt dann $|c|$ nur von der Doppelnebenklasse $\Gamma_\infty \sigma \Gamma_\infty$ ab, denn

$$\begin{pmatrix} 1 & rh \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 & sh \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} * & * \\ c & * \end{pmatrix}.$$

Wegen $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ gilt $|c| \geq 1$ für alle $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma \setminus \Gamma_\infty$. Es folgt also für jedes solche $\sigma$

$$\operatorname{Im}(\sigma(z)) = \frac{\operatorname{Im}(z)}{|cz+d|^2} = \frac{\operatorname{Im}(z)}{(c^2\operatorname{Re}(z)^2 + 2cd\operatorname{Re}(z) + d^2) + c^2\operatorname{Im}(z)^2} \leq \frac{\operatorname{Im}(z)}{c^2\operatorname{Im}(z)^2} \leq \frac{1}{\operatorname{Im}(z)}.$$

Wir setzen $U = \{z \in \mathbb{H}^* \mid \operatorname{Im}(z) > 1\}$. Für $\sigma \in \Gamma \setminus \Gamma_\infty$ und $z \in U$ gilt dann $\operatorname{Im}(\sigma(z)) < 1$, was die Behauptung für $z = \infty$ zeigt.

Für eine beliebige Spitze $s$ von $\Gamma$, gilt $s \in \mathbb{Q}$, da ja $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ angenommen war. Es gibt daher eine Matrix $\varrho \in \mathrm{SL}_2(\mathbb{Z})$, die $s$ nach $\infty$ schickt. Die Behauptung für $s$ folgt, wenn wir mit $\varrho$ konjugieren.

Sei nun $z \in \mathbb{H}$. Wegen der Transitivität der $\mathrm{SL}_2(\mathbb{R})$-Aktion auf $\mathbb{H}$ gibt es ein $\tau \in \mathrm{SL}_2(\mathbb{R})$ mit $\tau(i) = z$. Wegen $\mathrm{Stab}(\mathrm{SL}_2(\mathbb{R}); i) = \mathrm{SO}_2(\mathbb{R})$ ist der Stabilisator von $z$ in $\mathrm{SL}_2(\mathbb{R})$ durch $\tau \cdot \mathrm{SO}_2(\mathbb{R}) \cdot \tau^{-1}$ gegeben, also isomorph zu $\mathbb{R}/\mathbb{Z}$, also kompakt. $\Gamma_z$ ist nun der Durchschnitt dieses Kompaktums mit der diskreten Menge $\Gamma$ und von daher endlich und als Untergruppe von $\mathbb{R}/\mathbb{Z}$ sogar zyklisch.

Andererseits sind die einzigen Matrizen in $\mathrm{SL}_2(\mathbb{C})$ mit endlicher Ordnung diejenigen, deren Jordan'sche Normalform die Gestalt $\left(\begin{smallmatrix}\zeta & 0\\ 0 & \bar{\zeta}\end{smallmatrix}\right)$ mit einer Einheitswurzel $\zeta$ annimmt; solche Matrizen sind also immer gleich $\pm I_2$ oder elliptisch. Es folgt daher, dass $\Gamma_z$ für nicht elliptisches $z \in \mathbb{H}$ maximal $\pm I_2$ enthält.

Sei nun $F$ ein Fundamentalbereich von $\Gamma$ in $\mathbb{H}$, dessen Abschluss $z$ enthält. Ist $z$ nicht elliptisch, so ist der Stabilisator ja (mehr oder weniger) trivial, und wir können ohne Einschränkung annehmen, dass $z$ im Inneren von $F$ liegt. Ist $z$ elliptisch, so betrachten wir

$$\Gamma_z(F) = \{\sigma(w) \mid \sigma \in \Gamma_z,\ w \in F\}.$$

Das ist offensichtlich eine zusammenhängende Teilmenge von $\mathbb{H}$, die $z$ enthält. Da $\Gamma_z$ ja schon alle $\sigma \in \Gamma$ enthält, die $z$ fest lassen, können wir ohne Einschränkung annehmen, dass $z$ im Inneren von $\Gamma_z(F)$ liegt. In beiden Fällen wählt man nun $U$ als eine Umgebung von $z$, die bereits gänzlich in $F$ bzw. $\Gamma_z(F)$ liegt. Die Behauptung folgt nach Konstruktion. #

Daraus folgt, dass wir eine natürliche Einbettung $\Gamma_z\backslash U \to \Gamma\backslash\mathbb{H}^*$ haben, und dass $\Gamma_z\backslash U$ eine offene Umgebung von $\pi(z)$ in $\Gamma\backslash\mathbb{H}^*$ ist, wo $\pi : \mathbb{H}^* \to \Gamma\backslash\mathbb{H}^*$ die kanonische Projektion bezeichnet,

*denn:* Die vorige Behauptung zeigt gerade, dass Punkte in $U$ genau dann $\Gamma$-äquivalent sind, wenn sie $\Gamma_z$-äquivalent sind. Auf diese Weise können wir $\Gamma_z\backslash U$ mit der Teilmenge $\pi(U)$ von $\Gamma\backslash\mathbb{H}^*$ identifizieren. #

Wir definieren eine offene Überdeckung von $\Gamma\backslash\mathbb{H}^*$, indem wir zu jedem Punkt $z$ eine offene Umgebung samt Homöomorphismus nach $\mathbb{C}$ konstruieren. Dies handhaben wir unterschiedlich, je nachdem, ob der Punkt $z$ elliptisch, parabolisch oder keines von beiden ist.

(a) Ist $z$ weder elliptisch noch parabolisch, so ist $\Gamma_z$ trivial oder gleich $\{\pm I_2\}$, so dass die Abbildung $\pi : U \to \Gamma_z\backslash U$ ein Homöomorphismus ist.[11] Wir nehmen die Karte $(\Gamma_z\backslash U, \pi^{-1})$ in die komplexe Struktur von $\Gamma\backslash\mathbb{H}^*$ auf.

(b) Ist $z$ elliptisch, so betrachten wir die zum Stabilisator $\Gamma_z$ gehörige Gruppe $\bar{\Gamma}_z := (\Gamma_z \cdot \{\pm I_2\})/\{\pm I_2\}$ der Möbiustransformationen. Sei $\lambda$ der holomorphe Isomorphismus von $\mathbb{H}$ auf die Einheitskreisscheibe $D$, der $z$ auf 0 schickt. Ist $\bar{\Gamma}_z$ von Ordnung $n$, so besteht offensichtlich $\lambda\bar{\Gamma}_z\lambda^{-1}$ aus den Transformationen

$$w \mapsto \zeta^k w \quad \text{mit } k = 0, 1, \ldots, n-1 \text{ und } \zeta = e^{2\pi i/n}.$$

Dann ist durch $\varphi(\pi(z)) := \lambda(z)^n$ ein Homöomorphismus $\varphi : \Gamma_z\backslash U \to \mathbb{C}$ mit offenem Bild gegeben; wegen der $n$-ten Potenz ist das wohldefiniert. Wir nehmen auch $(\Gamma_z\backslash U, \varphi)$ in unsere komplexe Struktur auf.

[11] Bemerke, dass $I_2$ trivial operiert!

(c) Ist $z = s$ schließlich eine Spitze von $\Gamma$, so gibt es ja ein $\varrho \in \mathrm{SL}_2(\mathbb{Z})$ mit $\varrho(s) = \infty$. Dann ist

$$\varrho\Gamma_s\varrho^{-1} \cdot \{\pm I_2\} = \{\pm \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}^m \mid m \in \mathbb{Z}\}$$

für eine *positive* ganze Zahl $h$. Wir können einen Homöomorphismus $\varphi$ von $\Gamma_s\backslash U$ in eine offene Teilmenge von $\mathbb{C}$ definieren, indem wir $\varphi(\pi(z)) := e^{2\pi i(\varrho\circ z)/h}$ setzen, und $(\Gamma_s\backslash U, \varphi)$ in unsere komplexe Struktur aufnehmen.

Wir müssen nun noch zeigen, dass die Kartenwechselabbildungen holomorph sind. Das ist klar für zwei Karten, die beide weder zu einem elliptischen Punkt noch zu einer Spitze gehören. Sei also nun $z \in \mathbb{H}$ weder elliptisch noch parabolisch mit einer Umgebung $U_z$ wie in (a) und außerdem $s$ eine Spitze von $\Gamma$ mit $\varrho(s) = \infty$ und Umgebung $U_s$ wie in (c). Dann ist die Kartenwechselabbildung $\varphi \circ \pi$ für ein $w \in \pi^{-1}((\Gamma_z\backslash U_z) \cap (\Gamma_s\backslash U_s))$ durch

$$(\varphi \circ \pi)(w) = e^{2\pi i\varrho(w)/h}$$

gegeben und offensichtlich holomorph. Der Rest wird genauso gezeigt, so dass wir zusammengefasst erhalten:

**Satz 6.1** $\Gamma\backslash\mathbb{H}^*$ *ist eine zusammenhängende, kompakte Riemann'sche Fläche.*

Beim Studium von Riemann'schen Flächen wird man unweigerlich auf das Studium ihres ***Funktionenkörpers***, also des Körpers der meromorphen Funktionen auf ihnen, gestoßen. Dieser sieht wie folgt aus:

**Korollar 6.2** *Die meromorphen Funktionen auf* $\Gamma\backslash\mathbb{H}^*$ *entsprechen bijektiv den* $\Gamma$*-invarianten meromorphen Funktionen* $\mathbb{H}^* \to \mathbb{C}$*, also den* $\Gamma$***-modularen Funktionen auf*** $\mathbb{H}^*$*.*

*Beweis.* Das kann man mit den jeweiligen Kartenabbildungen nachrechnen. □

Besonders interessiert uns hier natürlich der Fall von $\Gamma = \Gamma(1)$. In diesem Fall gilt:

**Lemma 6.3** *Der Körper der* $\Gamma(1)$*-modularen Funktionen wird über* $\mathbb{C}$ *von der j-Invarianten erzeugt.*

*Beweis.* In Abschnitt 4 haben wir gezeigt, dass die $j$-Invariante zweier Gitter genau dann gleich ist, wenn es eine Homothetie zwischen ihnen gibt, und dass diese Homothetieklassen von Gittern der Form $\mathbb{Z} + \tau\mathbb{Z}$ mit $\tau \in \mathbb{H}$ repräsentiert werden. Seien andererseits $\mathbb{Z} + \tau\mathbb{Z}$ und $\mathbb{Z} + \tau'\mathbb{Z}$ zwei solche Gitter. Sind diese zueinander homothetisch, so gibt es ein $\alpha \in \mathbb{C}^\times$ mit

$$\begin{aligned} \{\alpha\tau, \alpha\} &\text{ ist Basis von } \mathbb{Z} + \tau'\mathbb{Z} \\ \{\tau', 1\} &\text{ ist Basis von } \alpha\,(\mathbb{Z} + \tau\mathbb{Z})\,. \end{aligned}$$

Da die Basiswechsel eines (vollständigen) Gitters in $\mathbb{C}$ durch ganzzahlige Matrizen gegeben sein müssen, gibt es dann $M, N \in \mathbb{Z}^{2\times 2}$ mit

$$\begin{pmatrix} \tau' \\ 1 \end{pmatrix} = \alpha \cdot M \begin{pmatrix} \tau \\ 1 \end{pmatrix} \quad \text{und} \quad \alpha \cdot \begin{pmatrix} \tau \\ 1 \end{pmatrix} = N \begin{pmatrix} \tau' \\ 1 \end{pmatrix}, \tag{17}$$

also

$$\begin{pmatrix}\tau\\1\end{pmatrix} = NM\begin{pmatrix}\tau\\1\end{pmatrix}.$$

Da $\{1,\tau\}$ eine $\mathbb{R}$-Basis von $\mathbb{C}$ ist, folgt damit $NM = I_2$ und insbesondere $\det(M) = \det(N) = \pm 1$. Da $\tau$ und $\tau'$ beide in der oberen Halbebene liegen, folgt $\det(M) = \det(N) = 1$, also $M, N \in \mathrm{SL}_2(\mathbb{Z})$. Liest man nun (17) zeilenweise, so folgt, dass zwei Gitter $\mathbb{Z}+\tau\mathbb{Z}$ und $\mathbb{Z}+\tau'\mathbb{Z}$ mit $\tau, \tau' \in \mathbb{H}$ genau dann zueinander homothetisch sind, wenn es ein $\sigma \in \Gamma(1)$ mit $\sigma(\tau) = \tau'$ gibt.

Andererseits haben wir in Proposition 2.2 bereits $j(\mathbb{H}) = \mathbb{C}$ gesehen. Damit definiert die $j$-Invariante offensichtlich eine Bijektion

$$\hat{j} : \Gamma(1)\backslash\mathbb{H} \to \mathbb{C}.$$

Diese wollen wir nun ausnutzen, um zu zeigen,[12] dass jede $\Gamma(1)$-modulare Funktion $f$ bereits eine rationale Funktion in $j$ ist. Tatsächlich wird dank der Bijektivität von $\hat{j}$ durch die Gleichung

$$R(j(z)) := f(z)$$

eine Funktion $R : \mathbb{C} \to \mathbb{P}^1(\mathbb{C})$ wohldefiniert. Sei nun $z_0 \in \mathbb{H}$ ein Punkt, in dem die Ableitung von $j$ nicht verschwindet. Wenn außerdem $f(z_0)$ endlich ist, folgt aus dem Satz für umkehrbare Funktionen, dass $R$ in einer offenen Umgebung von $j(z_0)$ analytisch ist. Aus der bekannten Reihenentwicklung von $j$ schließt man, dass es eine Konstante $C > 0$ gibt, so dass für alle $z$ mit $\mathrm{Im}(z) > C$ die Ableitung von $j$ nicht Null wird. Da die Ableitung einer Modulfunktion eine meromorphe Modulform vom Gewicht 2 ist,[13] hat somit $f'(z)$ im Standardfundamentalbereich $\mathcal{F}$ nur endlich viele Nullstellen. Da andererseits $f$ in $\mathcal{F}$ nur endlich viele Pole haben kann, folgt mit der obigen Argumentation, dass $R$ im Komplement einer endlichen Punktmenge analytisch ist. Mit dem Satz von Casorati-Weierstraß folgt, dass diese Ausnahmepunkte keine wesentlichen Singularitäten sein können,

*denn:* Sei $U \subseteq \mathbb{H}$ eine offene Umgebung eines Punktes $z_0 \in \mathbb{H}$ mit $f(z_0) \neq \infty$. Nach dem Satz von der Gebietstreue ist dann auch $j(U)$ offen. Wählt man $U$ klein genug, so ist $R(j(U)) = f(U)$ nicht dicht in $\mathbb{C}$. #

Ersetzt man $f$ durch $1/f$, so erhält man, dass $R$ in $\mathbb{C}$ meromorph ist. Analog erhält man auch die Meromorphie in $\infty$, was die Behauptung zeigt. □

## 7 Ganzheit

Im Abschnitt über komplexe Multiplikation haben wir gezeigt, dass die $j$-Invariante $j(E)$ einer elliptischen Kurve $E$ mit komplexer Multiplikation eine algebraische Zahl ist. Aber es gilt noch mehr, nämlich

**Satz 7.1** *Die $j$-Invariante $j(E)$ einer elliptischen Kurve $E$ mit komplexer Multiplikation ist eine ganze algebraische Zahl, erfüllt also eine Ganzheitsgleichung über $\mathbb{Z}$.*

[12] Vergleiche Theorem 2.11 in Kapitel VI von [FB].

[13] Denn aus $f(\sigma(z)) = f(z)$ folgt mit der Kettenregel $f'(z) = f'(\sigma(z))\sigma'(z) = (cz+d)^{-2}f'(\sigma(z))$.

Es gibt mehrere bekannte Beweise für diesen Satz; allein in [Sil2] lassen sich drei verschiedene finden. Derjenige, den wir führen werden, hat den Vorteil, nicht allzu tief in die Theorie der elliptischen Kurven einzudringen. Die Beweisstrategie wird die folgende sein.

Sei $E \cong \mathbb{C}/\Lambda$ eine elliptische Kurve mit $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$ für ein $\tau \in \mathbb{H}$. Wir wissen ja aus Abschnitt 5, dass $E$ genau dann komplexe Multiplikation hat, wenn $\tau$ eine quadratische Ganzheitsgleichung mit Koeffizienten in $\mathbb{Z}$ erfüllt. In diesem Fall gibt es eine nicht-triviale Beziehung der Form

$$\tau = \frac{a\tau + b}{c\tau + d} \tag{18}$$

mit $a, b, c, d \in \mathbb{Z}$. Das können wir als die Aktion einer Matrix $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ auffassen und

$$j(\tau) = j(M(\tau))$$

folgern, wo wir die von den Möbiustransformationen bekannte Schreibweise auf beliebige Matrizen aus $\mathbb{Z}^{2\times 2}$ ausdehnen. Wir können uns nun von diesem speziellen $\tau$ lösen und uns fragen, wie sich für beliebiges $z \in \mathbb{H}$ die Werte $j(z)$ und $j(M(z))$ zueinander verhalten. In der Tat werden wir für alle $M$ ein Polynom $P_M \in \mathbb{Z}[X, Y]$ finden, das auf der gesamten oberen Halbebene $P_M(j(z), j(M(z))) = 0$ erfüllt. Spezialisiert auf $z = \tau$ lautet das $P_M(j(\tau), j(\tau)) = 0$, was cum grano salis eine Ganzheitsgleichung für $j(\tau)$ liefert.

Studieren wir also die Funktion

$$j_M : \begin{cases} \mathbb{H} & \to \mathbb{C}, \\ z & \mapsto j(M(z)) \end{cases}$$

und versuchen, einen Zusammenhang zwischen ihr und $j$ zu finden. Hierbei sei

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{Z}^{2\times 2} \quad \text{mit } \det(M) = m \neq 0 \text{ und } \operatorname{ggT}(a, b, c, d) = 1.$$

**Bemerkung** *Dass nur diese Matrizen zu betrachten keine echte Einschränkung bedeutet, kann man sich leicht überlegen. In der Tat kann* $\det(M) = 0$ *nicht auftreten, da dann* $\tau$ *schon in* $\mathbb{Q}$ *liegen müsste (Übung!). Und ist* $\operatorname{ggT}(a, b, c, d) = g > 1$*, so ist offensichtlich* $\frac{M}{g}$ *ebenfalls eine Matrix mit ganzen Einträgen, die* (18) *erfüllt.*

Wäre $j_M$ eine $\Gamma(1)$-modulare Funktion, so wären wir bereits hier fertig. Nun ist $j_M$ zwar meromorph auf $\mathbb{H}^*$, aber im Allgemeinen nicht $\Gamma(1)$-invariant,

*denn:* Nehmen wir an, $j_M$ sei invariant unter $\sigma \in \Gamma(1)$. Dann gälte

$$j_M(z) = j_M(\sigma(z)) \iff j(M(z)) = j((M \circ \sigma)(z)).$$

In Abschnitt 4 haben wir gesehen, dass $j$ genau dann für zwei Gitter $\mathbb{Z} + \tau\mathbb{Z}$ und $\mathbb{Z} + \tau'\mathbb{Z}$ den gleichen Wert annimmt, wenn diese zueinander homothetisch sind, also wie im Beweis von Lemma 6.3 genau dann, wenn $\tau$ und $\tau'$ in derselben $\Gamma(1)$-Bahn liegen. Genau dann hätten demnach $z$ und $\sigma(z)$ die gleichen $j_M$-Werte, wenn

$$M(z) = (\tilde{\sigma} \circ M \circ \sigma)(z) \quad \text{für ein } \tilde{\sigma} \in \Gamma(1)$$

gälte, also $\sigma \in \left(M^{-1}\Gamma(1)M\right) \cap \Gamma(1)$. Letzteres ist im Allgemeinen eine echte Untergruppe von $\Gamma(1)$, wir möchten sie mit $G(M)$ bezeichnen. #

**Lemma 7.2** *Seien $M, M' \in \mathbb{Z}^{2\times 2}$ jeweils mit Determinante $m$ und teilerfremden Einträgen. Dann gilt*

(a) *Falls $M' = \sigma \circ M$ mit einem $\sigma \in \Gamma(1)$ gilt, so folgt $j_M = j_{M'}$ und $G(M) = G(\sigma \circ M)$.*
(b) *Falls $M' = M \circ \sigma$ mit einem $\sigma \in \Gamma(1)$ gilt, so folgt $G(M') = \sigma^{-1} \circ G(M) \circ \sigma$.*

*Beweis.* (a) Dies folgt aus der $\Gamma(1)$-Invarianz von $j$:

$$j_{M'}(z) = j(M'(z)) = j((\sigma \circ M)(z)) = j(M(z)) = j_M(z).$$

(b) Es gilt:

$$\begin{aligned} G(M') &= \left((M')^{-1} \circ \Gamma(1) \circ M'\right) \cap \Gamma(1) \\ &= \left((M \circ \sigma)^{-1} \circ \Gamma(1) \circ M \circ \sigma\right) \cap \Gamma(1) \\ &= \left(\sigma^{-1} \circ \left(M^{-1} \circ \Gamma(1) \circ M\right) \circ \sigma\right) \cap \left(\sigma^{-1} \circ \Gamma(1) \circ \sigma\right) \\ &= \sigma^{-1} \circ G(M) \circ \sigma. \end{aligned}$$

□

Das Lemma legt nahe, statt der Matrix $M$ gleich die Doppelnebenklasse $\Gamma(1) \circ M \circ \Gamma(1)$ zu betrachten. Man beachte, dass letztere in

$$M_0(m) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{Z}^{2\times 2} \mid ad - bc = m,\ \mathrm{ggT}(a,b,c,d) = 1\}$$

enthalten ist. Aus dem Beweis von Proposition 1.2 wissen wir bereits, dass

$$V_m = \{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid ad = m,\ d > 0,\ b \bmod (d)\}$$

ein Vertretersystem der Linksaktion von $\Gamma(1)$ auf $M(m)$ ist, weshalb

$$\{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid ad = m,\ d > 0,\ b \bmod (d),\ \mathrm{ggT}(a,b,d) = 1\}$$

eines für die Linksaktion von $\Gamma(1)$ auf $M_0(m)$ ist. Andererseits ist jetzt die Rechtsaktion von $\Gamma(1)$ auf den Bahnen der Linksaktion transitiv; für je zwei Matrizen $M, M' \in M_0(m)$ gibt es also $\sigma, \tilde{\sigma} \in \Gamma(1)$ mit $M' = \tilde{\sigma} \circ M \circ \sigma$,

*denn:* Der Elementarteilersatz besagt, dass sich jedes $M \in M_0(m)$ durch Rechts- und Linksmultiplikation mit Matrizen aus $\mathrm{GL}_2(\mathbb{Z})$ in die Form $\left(\begin{smallmatrix} 1 & 0 \\ 0 & m \end{smallmatrix}\right)$ bringen lässt. Hierbei haben aufgrund der Multiplikativität der Determinante entweder beide operierende Matrizen Determinante 1 oder beide $-1$. In letzterem Fall können wir mit $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ konjugieren, so dass wir darauf reduziert sind, die Aussage für $M = \left(\begin{smallmatrix} 1 & 0 \\ 0 & m \end{smallmatrix}\right)$ und $M' = \left(\begin{smallmatrix} m & 0 \\ 0 & 1 \end{smallmatrix}\right)$ zu zeigen. Dies stimmt aber wegen

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \circ \begin{pmatrix} 1 & 0 \\ 0 & m \end{pmatrix} \circ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix}.$$

#

Also haben wir gerade gezeigt, dass die Gruppen $G(M)$ mit $M \in M_0(m)$ gerade die Konjugierten in $\Gamma(1)$ von

$$G(\begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix}) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) \mid c \equiv 0 \bmod (m)\}$$

sind. Diese Gruppe wird üblicherweise mit $\Gamma_0(m)$ bezeichnet. Fassen wir zusammen:

**Proposition 7.3** *Für $M \in M_0(m)$ ist die Funktion $j_M$ $G(M)$-modular, und $G(M) = \left(M^{-1} \circ \Gamma(1) \circ M\right) \cap \Gamma(1)$ ist ein Konjugiertes von $\Gamma_0(m)$ in $\Gamma(1)$.*

**Bemerkung** *Wir sollten an dieser Stelle präzisieren, was wir unter einer $G(M)$-modularen Funktion verstehen. Die offensichtlichen Forderungen sollten sein:*

(a) *Sie muss $G(M)$-invariant sein,*

(b) *Sie muss auf ganz $\mathbb{H}^*$ meromorph sein.*

*Der erste Punkt ist klar; der zweite enthält jedoch noch eine Subtilität. Es sind nämlich im Allgemeinen nicht alle Spitzen in $\mathbb{P}^1(\mathbb{Q})$ unter einer Matrix aus $G(M)$ zueinander äquivalent, wie es für $\Gamma(1)$ der Fall war. Beispielsweise gibt es für $\Gamma_0(p)$ mit einer Primzahl $p$ zwei Bahnen*

$$\{\frac{r}{s} \in \mathbb{Q} \mid \mathrm{ggT}(r,s) = 1,\ r \not\equiv 0 \bmod (p)\} \cup \{\infty\},$$
$$\{\frac{r}{s} \in \mathbb{Q} \mid \mathrm{ggT}(r,s) = 1,\ r \equiv 0 \bmod (p)\}$$

*in $\mathbb{P}^1(\mathbb{Q})$. Hier muss man an einem Vertretersystem dieser Bahnen jeweils eine Fourierentwicklung durchführen und dort die Meromorphie wie in Abschnitt 1 überprüfen.*

Unser Ziel war ja, ein Polynom $P_M \in \mathbb{Z}[X,Y]$ finden, das auf der gesamten oberen Halbebene $P_M(j(z), j(M(z))) = 0$ erfüllt. Dies können wir nun angehen. Dazu stellen wir zunächst fest, dass die $j$-Invariante offenbar selbst auch schon eine $G(M)$-modulare Funktion ist. Betrachten wir nun die Riemann'sche Flächen $X(M) := G(M)\backslash\mathbb{H}^*$ mit $M \in M_0(m)$. Nach Korollar 6.2 entsprechen die meromorphen Funktionen auf $X(M)$ gerade den $G(M)$-modularen Funktionen auf $\mathbb{H}^*$. Nun sind $j$ und $j_M$ beides solche Funktionen, so dass es nach einem Satz aus der Theorie der Riemann'schen Flächen ein solches Polynom $P_M$ gibt, über dessen Koeffizienten wir allerdings nicht viel wissen.[14]

Wir wollen nun zeigen, dass solch ein $P_M$ gar nicht von $M$ sondern nur von $\det(M) = m$ abhängen kann. Tatsächlich, wenn $M$ und $M'$ in derselben Bahn der Linksaktion von $\Gamma(1)$ auf $M_0(m)$ liegen, dann gilt $G(M) = G(M')$ und also $X(M) = X(M')$. Es sind sogar alle $X(M)$ mit $M \in M_0(M)$ zueinander und damit insbesondere zu $X_0(m) := \Gamma_0(m)\backslash\mathbb{H}^*$ isomorph,

*denn:* Da $\Gamma(1)$ von rechts transitiv auf den Bahnen der Linksaktion operiert, genügt es zu zeigen, dass für $M' = M \circ \sigma$ mit $\sigma \in \Gamma(1)$ tatsächlich $X(M') \cong X(M)$ gilt. Aber wir haben in

[14] Das ist nur eine allgemeine Bemerkung; wir werden das Polynom $P_M$ in unserem Spezialfall ganz explizit konstruieren.

diesem Fall ja $G(M') = \sigma^{-1} \circ G(M) \circ \sigma$ gezeigt, so dass wir wissen, dass $z, z' \in \mathbb{H}^*$ genau dann $G(M')$-äquivalent sind, wenn $\sigma(z)$ und $\sigma(z')$ $G(M)$-äquivalent sind. Das führt auf folgendes kommutatives Diagramm

$$\begin{array}{ccc} \mathbb{H}^* & \xrightarrow{\sigma} & \mathbb{H}^* \\ \downarrow{\scriptstyle \pi_{M'}} & & \downarrow{\scriptstyle \pi_M} \\ X(M') & \xrightarrow{\iota} & X(M) \end{array}$$

wo $\pi_{M'}, \pi_M$ die jeweiligen kanonischen Projektionen sind und $\iota$ bijektiv. Da nun außerdem die kanonischen Projektionen analytisch sind[15], folgt die Behauptung. #

Sei wieder $M' = M \circ \sigma$ mit einem $\sigma \in \Gamma(1)$. Dann gilt

$$\sigma^* j(z) = j(\sigma(z)) = j(z) \quad \text{und} \quad \sigma^* j(M(z)) = j((M \circ \sigma)(z)) = j(M'(z)).$$

Die meromorphe Funktion $j$ entspricht also unter $\iota^*$ sich selbst, während $j_M$ auf $X(M)$ via $\iota^*$ zu $j_{M'}$ auf $X(M')$ wird. Da $\iota^*$ ein Isomorphismus auf den Funktionenkörpern ist, gilt

$$P_M(j(z), j(M(z))) = 0 \iff P_M(j(z), j(M'(z))) = 0,$$

was aufgrund der Transitivität der Rechtsaktion von $\Gamma(1)$ auf den Linksnebenklassen von $\Gamma(1)$ in $M_0(m)$ nahelegt, dass unser gesuchtes Polynom in $\mathbb{Z}[X, Y]$ gar nicht von $M$ selbst sondern nur von seiner Determinante $\det(M) = m$ abhängt. Das ist tatsächlich auch der Fall: Das gesuchte Polynom heißt die ***Modulargleichung*** der Stufe $m$ und wird üblicherweise mit $\Phi_m$ bezeichnet. Wir werden es jetzt konstruieren.

Dafür sei zunächst

$$\Psi_m(X; z) := \prod_{M \in \Gamma(1) \backslash M_0(m)} (X - j_M(z)) = \prod_{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in V_m} \left(X - j\left(\frac{az + b}{d}\right)\right).$$

Es gibt nun ein Polynom $\Phi_m \in \mathbb{C}[X, Y]$, unser gesuchtes Polynom, mit $\Psi_m(X; z) = \Phi_m(X; j(z))$,

*denn:* Wenn wir $\Psi_m(X; z)$ als Polynom $\sum_i a_i(z) X^i$ schreiben, dann sind die Koeffizienten $a_i$ symmetrische Funktionen in den $j_M$ und insbesondere meromorph. Andererseits ist für ein Vertretersystem $M_1, \ldots, M_r$ der Linksaktion von $\Gamma(1)$ auf $M_0(m)$ auch $M_1 \circ \sigma, \ldots, M_r \circ \sigma$ mit einem beliebigen $\sigma \in \Gamma(1)$ wieder ein solches Vertretersystem, so dass

$$\{j_{M_1 \circ \sigma}, \ldots, j_{M_r \circ \sigma}\}$$

nur eine Permutation von

$$\{j_{M_1}, \ldots, j_{M_r}\}$$

ist. Es folgt, dass die Koeffizienten $a_i$ als Funktionen in $z$ invariant unter $\Gamma(1)$ sind, wegen der Meromorphie also $\Gamma(1)$-modular. Nach Lemma 6.3 sind die Koeffizienten $a_i$ damit rationale Funktionen in $j$. Nun liegen die $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in V_m$ aber im Stabilisator von $\infty$, so dass keine der Funktionen $j_M$ mit $M \in V_m$ einen Pol in $\mathbb{H}$ hat und die $a_i$ bereits Polynome in $j$ sein müssen, was die Behauptung zeigt. #

[15] Benutze, dass $G(M)$ bzw. $G(M')$ einen Fundamentalbereich in $\mathbb{H}^*$ haben.

Nach Definition verschwindet $\Psi_m(X;z)$ in $X = j_M(z)$ für alle $M \in M_0(m)$, so dass folgt:

$$0 = \Psi_m(j_M(z);z) = \Phi_m(j_M(z);j(z)) \quad \text{für alle } z \in \mathbb{H},\ M \in M_0(m). \tag{19}$$

Wenn wir nun noch

**Satz 7.4** *$\Phi_m(X,Y)$ liegt in $\mathbb{Z}[X,Y]$.*

zeigen können, haben wir ein Polynom wie gewünscht gefunden. Dafür müssen wir ein wenig Vorarbeit leisten. Nach Konstruktion von $\Phi_m$ langt es zu zeigen, dass eine beliebige symmetrische Funktion $a_i$ in den Funktionen $j_M$ mit $M \in V_m$ bereits in $\mathbb{Z}[j]$ liegt. Dazu zeigen wir zunächst das folgende Lemma.

**Lemma 7.5** *Jede symmetrischen Funktion $a_i$ in den Funktionen $j_M$ mit $M \in V_m$ hat eine $q$-Entwicklung in $\mathbb{Z}[\![q,q^{-1}]\!]$.*

*Beweis.* Sei im Folgenden $\zeta = e^{2\pi i/m}$. Mit $M = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in V_m$ gilt dann in einem Ringgebiet $0 < q^{\frac{1}{m}} < C_M$

$$j_M(z) = \zeta^{-ab} q^{\frac{-a^2}{m}} + \sum_{k=0}^{\infty} c_k \zeta^{abk} q^{\frac{a^2 k}{m}},$$

wo $c_k$ die Koeffizienten der $q$-Entwicklung von $j$ sind,

*denn:* Wegen $j_M(z) = j(M(z))$ genügt es, $M(z) = \frac{az+b}{d}$ in die $q$-Entwicklung von $j(z)$ einzusetzen. Mit $ad = m$ folgt

$$e^{2\pi i M(z)} = e^{2\pi i \frac{b}{d}} \cdot e^{2\pi i \frac{a}{d} z} = \zeta^{ab} \cdot q^{\frac{a^2}{m}}$$

und die Behauptung. #

Wir können diese Reihen für alle $M$ gliedweise addieren und multiplizieren und bekommen so in einem Gebiet $0 < q^{\frac{1}{m}} < C$ eine Reihenentwicklung von $a_i$ in $\mathbb{Z}[\zeta][\![q^{\frac{1}{m}}, q^{-\frac{1}{m}}]\!]$. Da $a_i$ als $\Gamma(1)$-modulare Funktion 1-periodisch ist, liegt diese Reihenentwicklung bereits in $\mathbb{Z}[\zeta][\![q,q^{-1}]\!]$. Dass die Reihe sogar schon in $\mathbb{Z}[\![q,q^{-1}]\!]$ liegt, zeigt man am elegantesten mit etwas Galoistheorie: Zu jedem $\sigma$ aus der Galoisgruppe $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ gibt es ein zu $m$ teilerfremdes $r$ mit $\sigma(\zeta) = \zeta^r$. Lassen wir nun $\sigma$ gliedweise auf der $q^{\frac{1}{m}}$-Entwicklung von $j_M$ operieren, wobei wir $q^{\frac{1}{m}}$ als Variable ansehen, so gilt

$$\begin{aligned}
(j_M(z))^\sigma &= \zeta^{-rab} q^{\frac{-a^2}{m}} + \sum_{k=0}^{\infty} c_k \zeta^{abrk} q^{\frac{a^2 k}{m}} \\
&= j_{M'}(z) \quad \text{mit } M' = \begin{pmatrix} a & rb \\ 0 & d \end{pmatrix} \\
&= j_{M''}(z) \quad \text{mit } M'' = \begin{pmatrix} a & rb \bmod (d) \\ 0 & d \end{pmatrix},
\end{aligned}$$

da $M'$ und $M''$ in derselben $\Gamma(1)$-Linksbahn von $M_0(m)$ liegen (sie unterscheiden sich lediglich um eine geeignete Potenz von $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$). Diese Zuordnung von $M$ nach $M''$ induziert eine Permutation auf $V_m$,

*denn:* Wegen $\mathrm{ggT}(r,m) = 1$ ist auch $\mathrm{ggT}(r,d) = 1$, so dass die Zuordnung $b \mapsto br$ modulo $d$ eine Bijektion ist. Außerdem ist

$$\mathrm{ggT}(a, br \bmod (d), d) = \mathrm{ggT}(a, br, d) \overset{\mathrm{ggT}(r,d)=1}{=} \mathrm{ggT}(a, b, d) = 1,$$

so dass die Matrix $M''$ wieder in $V_m$ liegt. #

Die Koeffizienten der $q$-Entwicklung von $a_i$ sind also $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$-invariante Elemente von $\mathbb{Z}[\zeta]$, liegen also schon in $\mathbb{Z}$, was das Lemma zeigt. □

*Beweis von Satz 7.4.* Wir betrachten $a_i$ als Polynom $\sum_{k=0}^{n} a_{ik} j^k$ in $j$. Mit der $q$-Entwicklung der $j$-Invarianten (siehe Satz 2.1) können wir

$$a_i(z) = a_{in} q^{-n} + \{ \text{ Terme in } q^{-t} \text{ mit } t < n \}$$

schreiben. Nach Lemma 7.5 ist dann $a_{in} \in \mathbb{Z}$. Die $q$-Entwicklung von $j^n$ ist die $n$-fache formale Potenz der $q$-Entwicklung von $j$. Mit letzterer liegt erstere wieder in $\mathbb{Z}[\![q, q^{-1}]\!]$, es gilt also

$$a_i - a_{in} j^n = \sum_{k=0}^{n-1} a_{ik} j^k \quad \in \mathbb{Z}[\![q, q^{-1}]\!].$$

Induktiv können wir auf diese Weise zeigen, dass alle $a_{ik}$ ganzzahlig sind. Es folgt $a_i \in \mathbb{Z}[j]$, was zu zeigen war. □

Wir haben jetzt ein Polynom $\Phi_m \in \mathbb{Z}[X,Y]$ gefunden, das für alle $M \in M_0(m)$ auf ganz $\mathbb{H}$ die Bedingung $\Phi_m(j_M(z); j(z)) = 0$ erfüllt. Das wollen wir nun nutzen, um eine Ganzheitsgleichung für $j$ zu finden.

*Beweis von Satz 7.1.* Erinnern wir uns an unsere Ausgangssituation. Gegeben ist eine elliptische Kurve $E \cong \mathbb{C}/\Lambda$ mit $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$. $E$ hat komplexe Multiplikation, weshalb es ein $M \in M_0(m)$ mit einer nicht-trivialen Relation $M(\tau) = \tau$ gibt. Daraus folgt mit (19)

$$\Phi_m(j(\tau), j(\tau)) = \Phi_m(j(M\tau), j(\tau)) = \Phi_m(j_M(\tau), j(\tau)) = 0.$$

Der Satz ist bewiesen, wenn wir zeigen können, dass $\Phi_m$ normiert ist, denn mit Satz 7.4 ist dann ja eine Ganzheitsgleichung für $j(\tau)$ gefunden. Das zerlegen wir in zwei Teilbehauptungen.

**Behauptung** *Angenommen, $m > 1$ sei kein Quadrat. Dann ist der Leitkoeffizient von $\Phi_m(j(\tau), j(\tau))$ tatsächlich $\pm 1$.*

*denn:* Wie wir schon im Beweis zu Satz 7.4 gesehen haben, ist der Leitkoeffizient in $j$ von $\Phi_m(j,j)$ genau der Leitkoeffizient der $q$-Entwicklung von $\Phi_m(j,j)$, also der Koeffizient der „negativsten“ Potenz von $q$ dort. Aber nach Definition von $\Phi_m$ gilt

$$\Phi_m(j,j) = \prod_{M \in V_m} (j - j_M).$$

Wenn wir die $q$-Entwicklung von $j$ und die $q^{\frac{1}{m}}$-Entwicklung von $j_M$ einsetzen, bekommen wir

$$\left( \frac{1}{q^{\frac{m}{m}}} + \sum_{k=0}^{\infty} c_k q^{\frac{km}{m}} \right) - \left( \frac{1}{\zeta^{ab} q^{\frac{a^2}{m}}} + \sum_{k=0}^{\infty} c_k \zeta^{abk} q^{\frac{ka^2}{m}} \right) \tag{20}$$

als $q^{\frac{1}{m}}$-Entwicklung von $j - j_M$. Da $m$ als Nichtquadrat ungleich $a^2$ sein muss, können sich die beiden Leitterme $q^{-\frac{m}{m}}$ und $\zeta^{-ab}q^{\frac{a^2}{m}}$ nicht wegheben, und der Leitkoeffizient von (20) ist entweder 1 oder $-\zeta^{-ab}$. In beiden Fällen ist der Leitkoeffizient eine Einheitswurzel. Wenn wir also all diese Ausdrücke aufmultiplizieren, bekommen wir eine $q^{\frac{1}{m}}$-Entwicklung von $\Phi_m(j,j)$ mit einer Einheitswurzel $\xi$ als Leitkoeffizient. Da diese $q^{\frac{1}{m}}$-Entwicklung in Wirklichkeit jedoch eine $q$-Entwicklung mit ganzen Koeffizienten ist, muss $\xi$ schon $\pm 1$ sein, was zu zeigen war. #

**Behauptung** *Ohne Einschränkung können wir m so wählen, dass es kein Quadrat ist.*

*denn:* Nehmen wir an, es gebe teilerfremde ganze Zahlen $A, B, C$ mit $A\tau^2 + B\tau + C = 0$ und $\Delta := B^2 - 4AC < 0$. Damit $\tau = M(\tau)$ gilt, ist es dann hinreichend für $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$,

$$b = -C,\ c = A,\ d - a = B$$

zu erfüllen; denn aus $\mathrm{ggT}(A, B, C) = 1$ folgt sofort die Bedingung $\mathrm{ggT}(a, b, c, d) = 1$. Für jedes solche 4-Tupel $(a, b, c, d) \in \mathbb{Z}^4$ gilt

$$\det(M) = ad - bc = a^2 + Ba + AC.$$

Wenn dies eine Quadratzahl $\lambda^2$ ist, so folgt

$$(2a + B)^2 - (2\lambda)^2 = \Delta < 0.$$

Da die Differenz $n^2 - (n-1)^2 = 2n - 1$ benachbarter Quadrate mit $n \in \mathbb{Z}$ beliebig groß wird, kann es nur endlich viele Paare $(2a + B, 2\lambda) \in \mathbb{Z}^2$ geben, die diese Bedingung erfüllen. Andererseits gibt es zu einem festen $\lambda$ maximal 2 mögliche $a$, so dass es nur endlich viele Werte von $a$ gibt, für die $\det(M)$ ein Quadrat ist. Wir können also ein Nicht-Quadrat $m$ und eine Matrix $M \in M_0(m)$ finden, für die $\tau = M(\tau)$ gilt. #

□

## 8 Heegnerzahlen

Sei $K$ ein imaginär-quadratischer Zahlkörper mit Klassenzahl 1 und $E$ eine elliptische Kurve, die komplexe Multiplikation mit dem Ganzzahlring von $K$ hat. Die Sätze 5.8 und 7.1 besagen dann, dass die $j$-Invariante $j(E)$ schon in $\mathbb{Z}$ liegt. Die Frage ist nun, welche imaginär-quadratischen Zahlkörper Klassenzahl 1 haben, und für uns ganz speziell, ob $\mathbb{Q}(\sqrt{-163})$ dabei ist. Das wurde 1952 von Heegner beantwortet und soll in diesem Abschnitt nachvollzogen werden.[16] Wir folgen dabei der Arbeit von Stark, der in [Sta] Heegners Beweis korrigiert,[17] beweisen allerdings nicht alle Aussagen dort.

Sei ab jetzt $K = \mathbb{Q}(\sqrt{d})$ mit $d \in \mathbb{Z}_{<0}$ fest gewählt. Unser Ziel ist es, die Grade der algebraischen ganzen Zahlen $J := j(\sqrt{d})$ und $j := j(\frac{1+\sqrt{d}}{2})$ zu verstehen. Dafür zeigen wir

[16] Einen schönen Überblick über die Frage nach der Klassenzahl eines imaginär-quadratischen Zahlkörpers ganz allgemein gibt übrigens der Artikel [Gol] von Goldfeld.

[17] Alternativ kann man auch die Analytische Klassenzahlformel verwenden, um das Problem auf die lineare Unabhängigkeit bestimmter Logarithmenwerte zurückzuführen.

**Proposition 8.1** *Sei $h_K = 1$ und $d < -60$. Dann gilt $[\mathbb{Q}(J,j) : \mathbb{Q}] = [\mathbb{Q}(J) : \mathbb{Q}] = 3$.*

*Beweis.* Laut [Dic], Seite 184, gilt für $h_K = 1$ und $d < -8$ die Kongruenz $|d| \equiv 3 \bmod (8)$, also insbesondere $d \equiv 1 \bmod (4)$. Nach Abschnitt I.2 in [Neu] ist daher $\{1, \frac{1+\sqrt{d}}{2}\}$ eine Ganzheitsbasis von $\mathcal{O}_K$, so dass $j$ nach der Konstruktion in Abschnitt 5 die $j$-Invariante einer elliptischen Kurve mit komplexer Multiplikation ist. Nach den Sätzen 5.8 und 7.1 ist demnach $j \in \mathbb{Z}$. Zu zeigen bleibt $[\mathbb{Q}(J) : \mathbb{Q}] = 3$.

Zeigen wir zunächst $[\mathbb{Q}(J) : \mathbb{Q}] \geq 3$. Da die Matrizen

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$$

wie in Abschnitt 7 ein Vertretersystem von $\Gamma(1)$ in $M_0(2)$ bilden, ist die Funktion

$$F_2(X;z) = \big(X - j(\frac{z}{2})\big) \cdot \big(X - j(\frac{1+z}{2})\big) \cdot \big(X - j(2z)\big)$$

eine $\Gamma(1)$-modulare Funktion in $z$ und als solche nach Lemma 6.3 eine rationale Funktion in $j(z)$. Da sie auf ganz $\mathbb{H}$ holomorph ist, ist sie sogar eine ganz-rationale Funktion in $j(z)$; wir schreiben auch $F_2(X; j(z))$. Für $z = \frac{1+\sqrt{d}}{2}$ haben wir deshalb

$$F_2(X;j) = \big(X - j(\frac{1+\sqrt{d}}{4})\big) \cdot \big(X - j(\frac{-1+\sqrt{d}}{4})\big) \cdot \big(X - J\big) \in \mathbb{Z}[X].$$

Nehmen wir nun an, $J$ sei rational oder quadratisch über $\mathbb{Q}$. Das Minimalpolynom von $J$ wäre dann in $\mathbb{Q}[X]$ ein Teiler von $F_2(X;j)$, so dass letzteres reduzibel wäre und also eine rationale Nullstelle haben müsste. Da für $d < -16$ die Argumente $\frac{\pm 1+\sqrt{d}}{4}$ im Innern des Standardfundamentalbereichs $\mathcal{F}$ von $\Gamma(1)$ auf $\mathbb{H}$ liegen, können die Werte $j(\frac{\pm 1+\sqrt{d}}{4})$ nicht rational sein, so dass $J$ die rationale Nullstelle von $F_2(X;j)$ sein müsste und insbesondere $J \in \mathbb{Z}$ wäre.

Wir betrachten nun die $q$-Entwicklung von $j(z)$, um zu zeigen, dass dies nicht sein kann. Mit $t := -e^{-\pi\sqrt{|d|}}$ gilt

$$\begin{aligned} (j-744)^2 &= \big(t^{-1} + 196884t + \sum_{n=2}^{\infty} c_n t^n\big)^2, \\ J - 744 &= t^{-2} + 196884t^2 + \sum_{n=2}^{\infty} c_n t^{2n}. \end{aligned}$$

Durch Subtraktion folgt daraus sofort

$$\begin{aligned} &(j-744)^2 - (J-744) - 393768 \\ &= 38763112572t^2 + 2t^{-1} \cdot \sum_{n=2}^{\infty} c_n t^n + 393768t \cdot \sum_{n=2}^{\infty} c_n t^n + (\sum_{n=2}^{\infty} c_n t^n)^2 - \sum_{n=2}^{\infty} c_n t^{2n}. \end{aligned} \tag{21}$$

Die linke Seite haben wir hierbei als Element von $\mathbb{Z}$ angenommen; andererseits kann man zeigen, dass die rechte Seite für hinreichend kleines $d$ echt zwischen $-1$ und $0$ liegt, und bekommt

so einen Widerspruch. Das ist so, denn man hat dort eine Entwicklung nach Potenzen von $t$ der Form

$$\text{rechte Seite} = \sum_{n=1}^{\infty} b_n t^n,$$

die für $t \to 0$ offensichtlich gegen Null geht.[18] Andererseits ist dann $b_1 t = 2c_2 t$ der dominante Term, weshalb die Werte für hinreichend kleines $d$ immer negativ sind. Mit Abschätzungen wie am Ende von Abschnitt 2 kann man zeigen, dass tatsächlich schon $d < -60$ ausreicht.

Um zu zeigen, dass $J$ über $\mathbb{Q}$ höchstens Grad 3 haben kann, studiert man die Ordnungen in Ganzzahlringen von Zahlkörpern genauer. Unter der Voraussetzung $h_K = 1$ und $d < -8$ folgt dann analog zu Satz 5.8

$$[\mathbb{Q}(J) : \mathbb{Q}] = [\mathbb{Q}(j(\mathbb{Z} + \sqrt{d}\mathbb{Z})) : \mathbb{Q}] \leq 3.$$

Einen, allerdings wenig erhellenden, Beweis für diese Tatsache[19] kann man auf Seite 138 von [Dic] suchen. □

Betrachten wir nun die ***Dedekind'sche $\eta$-Funktion***

$$\eta(z) = \sqrt{2\pi} \cdot q^{\frac{1}{24}} \cdot \prod_{n=1}^{\infty} (1 - q^n).$$

Diese erfüllt offensichtlich (vgl. Proposition 1.2) die Funktionalgleichung

$$\eta(z)^{24} = \Delta(z)$$

und kann so als „Modulform von Gewicht $\frac{1}{2}$" angesehen werden. Wir definieren

$$\begin{aligned}
f(z) &= \frac{e^{-\frac{\pi i}{24}} \eta(\frac{z+1}{2})}{\eta(z)} = q^{-\frac{1}{48}} \cdot \prod_{n=1}^{\infty} (1 + q^{\frac{2n-1}{2}}), \\
g(z) &= \frac{\eta(\frac{z}{2})}{\eta(z)} = q^{-\frac{1}{48}} \cdot \prod_{n=1}^{\infty} (1 - q^{\frac{2n-1}{2}}), \\
h(z) &= \sqrt{2} \cdot \frac{\eta(2z)}{\eta(z)} = \sqrt{2} \cdot q^{\frac{1}{24}} \cdot \prod_{n=1}^{\infty} (1 + q^n).
\end{aligned}$$

Durch eine längliche Rechnung mit Thetareihen kann man zeigen, dass sich die $j$-Invariante durch $f, g, h$ darstellen lässt; nach §54 in [Web] gilt nämlich

$$j(z) = \left( \frac{f(z)^{24} - 16}{f(z)^8} \right)^3 = \left( \frac{g(z)^{24} + 16}{g(z)^8} \right)^3 = \left( \frac{h(z)^{24} + 16}{h(z)^8} \right)^3.$$

Wenn wir nun $\gamma_2(z)$ als diejenige dritte Wurzel von $j(z)$ verstehen, die auf der imaginären Achse reelle Werte annimmt, so folgt daraus

[18] Wir können ohne Einschränkung Konvergenz annehmen, da Divergenz sofort einen Widerspruch zur Folge hätte.

[19] Formuliert in der Sprache der Äquivalenzklassen binärer quadratischer Formen: Aus $h_K = 1$ und $d < -8$ folgert man $|d| \equiv 3 \bmod (8)$ und $d \neq -3$ (siehe Seite 184 in [Dic]). Es gibt dann 3 Mal soviele Äquivalenzklassen quadratischer Formen $ax^2 + bxy + cy^2$, $\mathrm{ggT}(a, b, c) = 1$ mit Determinante $4d = b^2 - 4ac$ als mit Determinante $d$.

**Lemma 8.2** *$f(z)^8, -g(z)^8, -h(z)^8$ sind die Lösungen der kubischen Gleichung*

$$X^3 - \gamma_2(z)X - 16 = 0.$$

Führen wir zur Abkürzung noch ein wenig Notation ein. Sei also

$$F := f(\sqrt{d}) \quad \text{und} \quad h := e^{\frac{\pi i}{8}} h(\frac{-3+\sqrt{d}}{2}).$$

Dann gilt

**Proposition 8.3** $\mathbb{Q}(h^2) = \mathbb{Q}(F^2) = \mathbb{Q}(J)$.

*Beweis.* Zeigen wir zuerst das erste Gleichheitszeichen. Wenn man ausnutzt, dass $\eta$ eine Modulform vom Gewicht $\frac{1}{2}$ ist, erhält man die folgenden Transformationseigenschaften der Funktionen $f, g, h$ unter $\mathrm{SL}_2(\mathbb{Z})$:

$$\begin{aligned} f(z+1) &= e^{\frac{-\pi i}{24}} g(z), \quad g(z+1) = e^{\frac{-\pi i}{24}} f(z), \quad h(z+1) = e^{\frac{\pi i}{12}} h(z), \\ f(-\frac{1}{z}) &= f(z), \qquad g(-\frac{1}{z}) = h(z), \qquad h(-\frac{1}{z}) = g(z). \end{aligned} \tag{22}$$

Nun folgt unmittelbar aus der Definition von $g$ und $h$

$$g(2z)h(z) = \sqrt{2},$$

woraus man mit (22)

$$f(z)h(\frac{z-3}{2}) = e^{\frac{-\pi i}{8}}\sqrt{2}$$

erhält, wenn man $z$ durch $\frac{z-3}{2}$ ersetzt. Es folgt $h^2 = \frac{2}{F^2}$ und damit die Behauptung.

Aus Lemma 8.2 und der Definition von $\gamma_2(z)$ folgt andererseits sofort $J \in \mathbb{Q}(F^2)$. Dass $F^2$ auch schon in $\mathbb{Q}(J)$ liegt, war die umstrittene Aussage im Beweis von Heegner, die Stark in seinem Artikel richtigstellte. Der Beweis ist zu lang, um ihn hier vorzuführen und kann in § 3 von [Sta] nachgelesen werden. Die Hauptidee ist, $-g(z)^8$ und $-h(z)^8$ durch spezielle Funktionswerte von $f$ auszudrücken und so aus der Gleichung $X^3 - \gamma_2(z)X - 16 = 0$ die verlangte Relation herzuleiten. □

Sei zunächst wieder $h_K = 1$ und $d < -60$. Aus den Propositionen 8.1 und 8.3 folgt dann, dass $h^2$ kubisch über $\mathbb{Q}$ ist. Andererseits ist $\gamma := \gamma_2(\frac{-3+\sqrt{d}}{2})$ ganz über $\mathbb{Z}$, $h^2$ nach Lemma 8.2 also auch. Insgesamt folgt, dass $h^2$ über $\mathbb{Q}$ ein normiertes Minimalpolynom der Form

$$X^3 + \lambda X^2 + \mu X + \nu \quad \text{mit } \lambda, \mu, \nu \in \mathbb{Z}$$

hat. Offensichtlich ist dann $X^3 - \lambda X^2 + \mu X - \nu$ ein solches von $-h^2$, so dass

$$X^3 + \delta X^2 + \varepsilon X + \varphi = 0 \quad \text{mit } \delta = 2\mu - \lambda^2,\ \varepsilon = \mu^2 - 2\lambda\nu,\ \varphi = -\nu^2 \in \mathbb{Z}$$

eine Gleichung für $h^4$ ist. Auf dieselbe Weise erhalten wir, dass $h^8$ eine Nullstelle von

$$X^3 + (2\varepsilon - \delta^2)X^2 + (\varepsilon^2 - 2\delta\varphi)X - \varphi^2 \tag{23}$$

ist. Andererseits gilt $\mathbb{Q}(h^8) = \mathbb{Q}(h^2)$, da $h^2$ über $\mathbb{Q}$ Grad 3 hat, so dass (23) das eindeutig bestimmte normierte Minimalpolynom von $h^8$ ist. Das kennen wir aber mit Lemma 8.2 schon, so dass

$$2\varepsilon - \delta^2 = 0,\ 2\delta\varphi - \varepsilon^2 = \gamma,\ \varphi^2 = 16.$$

folgt. Wegen $\nu \in \mathbb{Z}$ ist $\varphi = -\nu^2 < 0$, also $\varphi = -4$ und $\nu = \pm 2$. Wir erhalten die diophantische Gleichung

$$(2\mu - \lambda^2)^2 = \delta^2 = 2\varepsilon = 2(\mu^2 \mp 4\lambda),$$

aus der wir sofort entnehmen, dass $\lambda$ und deshalb auch $\mu$ gerade ist. Schreiben wir $\mp\lambda = 2\alpha$ und $\mu = 2\beta$ und setzen dies ein, haben wir Heegners Gleichung

$$2\alpha(\alpha^3 + 1) = (\beta - 2\alpha^2)^2. \tag{24}$$

**Proposition 8.4** *Die Lösungen von (24) sind genau die Paare*

$$(\alpha, \beta) \in \{(0,0), (1,0), (-1,2), (2,2), (1,4), (2,14)\}.$$

*Beweis.* Für $\alpha = 0$ gibt es offensichtlich genau die eine Lösung $\beta = 0$. Betrachten wir also ab sofort nur noch $\alpha \neq 0$.

Man entnimmt (24) sofort, dass $\beta$ gerade sein muss, dass also $\frac{\alpha(\alpha^3+1)}{2}$ eine ganze Quadratzahl ist. Nehmen wir an, eine ungerade Primzahl $p$ komme genau $\nu_p \in \mathbb{Z}$ Mal in der Primfaktorzerlegung von $\alpha$ vor. Dann folgt trivialerweise

$$p^{\nu_p} \mid \frac{\alpha(\alpha^3+1)}{2} \quad \text{und} \quad p^{\nu_p+1} \nmid \frac{\alpha(\alpha^3+1)}{2},$$

so dass $2 \mid \nu_p$ folgt. Analog erhalten wir $\nu_2 \in \mathbb{Z} \setminus 2\mathbb{Z} \cup \{0\}$. $|\alpha|$ ist also eine (ungerade) Quadratzahl oder das Doppelte einer Quadratzahl.

**Fall 1.** Nehmen wir an, es gelte $|\alpha| = 2a^2$ mit einem $a \in \mathbb{Z}$. Eingesetzt in (24) erhalten wir, dass $\alpha^3 \pm 1$ eine Quadratzahl ist, es also ein $b \in \mathbb{Z}$ gibt mit $\alpha^3 - b^2 = \mp 1$. Dies hat bekanntermaßen nur für $\alpha \in \{-1, 0, 1, 2\}$ eine Lösung, nämlich die trivialen mit $\alpha = 0$ oder $b = 0$ und die Lösung $3^2 - 2^3 = 1$.

**Fall 2.** Gelte nun $|\alpha| = a^2$ mit einem ungeraden $a \in \mathbb{Z}$. Eingesetzt in (24) erhalten wir $a^6 \pm 1 = 2b^2$ mit einem $b \in \mathbb{Z}$, wofür wir $4 \mid (\beta - 2\alpha^2)^2$ berücksichtigen. $a^6 - 1 = 2b^2$ hat nur die trivialen Lösungen $(a, b) = (\pm 1, 0)$,

*denn:* Es genügt offensichtlich zu zeigen, dass abgesehen vom Punkt bei unendlich $(1, 0)$ der einzige Punkt der elliptische Kurve $2b^2 = a^3 - 1$ ist, dessen Koordinaten ganzzahlig sind. Im Hauptidealring $\mathbb{Z}[\sqrt{-2}]$ gilt

$$a^3 = 2b^2 + 1 = (1 + \sqrt{-2}b)(1 - \sqrt{-2}b).$$

Da der größte gemeinsame Teiler in $\mathbb{Z}[\sqrt{-2}]$ der beiden Faktoren rechts sicher ein Teiler ihrer Summe, also 2, ist, gibt es ein $\zeta \in \mathbb{Z}[\sqrt{-2}]$ mit

$$1+\sqrt{-2}b \in \{\zeta^3, \sqrt{-2}\zeta^3\} \quad \text{und} \quad 1-\sqrt{-2}b \in \{\bar{\zeta}^3, -\sqrt{-2}\bar{\zeta}^3\},$$

wo man die letzte Gleichheit durch komplexes Konjugieren einsieht. Es folgt also

$$a^3 = 2b^2+1 \in \{(\zeta\bar{\zeta})^3, 2(\zeta\bar{\zeta})^3\}.$$

Wegen $\zeta\bar{\zeta} \in \mathbb{Z}$ kann nur der erste Fall zutreffen, so dass wir

$$1+\sqrt{-2}b = \zeta^3 \quad \text{und} \quad 1-\sqrt{-2}b = \bar{\zeta}^3$$

erhalten. Durch Aufsummieren ergibt sich

$$2 = \zeta^3+\bar{\zeta}^3 = (\zeta+\bar{\zeta})(\zeta^2-\zeta\bar{\zeta}+\bar{\zeta}^2) = 2m(m^2-6n^2),$$

wo wir $\zeta = m+\sqrt{-2}n$ mit $m,n \in \mathbb{Z}$ gesetzt haben. Offensichtlich lässt sich dies in ganzen Zahlen nur für $(m,n) = (\pm 1, 0)$ lösen, woraus sofort die Behauptung folgt. #

Im anderen Fall können wir das Problem zerlegen; es gilt

$$2\cdot(a^2+1)\cdot(a^4-a^2+1) = 2\cdot(a^6+1) = 4b^2,$$

was äquivalent ist zu

$$\exists c,d \in \mathbb{Z} : 2(a^2+1) = 4c^2 \quad \text{und} \quad |a^2+e^{\frac{2\pi i}{3}}|^2 = a^4-a^2+1 = d^2, \tag{25}$$

*denn:* Es gilt $(a^4-a^2+1)-(a^2+1)(a^2-2) = 3$, so dass der größte gemeinsame Teiler von $(a^4-a^2+1)$ und $(a^2+1)$ ein Teiler von 3 ist. Da $a^6+1$ nicht durch 3 geteilt wird, sind $(a^2+1)$ und $(a^4-a^2+1)$ teilerfremd. #

Betrachten wir die zweite Gleichung in (25). Für $a^2 \neq 0,1$ sind dort die Faktoren $a^2+e^{\frac{\pm 2\pi i}{3}}$ teilerfremd in $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$,[20] so dass wir stattdessen zwei Gleichungen

$$(a^2+e^{\frac{\pm 2\pi i}{3}}) = (u+e^{\frac{\pm 2\pi i}{3}}v)^2 \quad \text{mit } u,v \in \mathbb{Z}$$

erhalten. Beim Vergleichen von Real- und Imaginärteil erhalten wir diophantische Gleichungen, die sich nur für $a^2 = 1$ lösen lassen. Zusammenfassend kann es in diesem Fall höchstens für $\alpha \in \{-1,0,1\}$ Lösungen geben.

Setzt man nun $\alpha = -1,0,1,2$ in (24) ein, erhält man die behaupteten Lösungen. □

[20] $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ zusammen mit dem komplexen Betrag ist euklidisch, wie man leicht nachprüft (vgl. (1.2) Satz in [Neu]), und insbesondere faktoriell. Man klassifiziert die Primelemente dann modulo 3 und erhält so die Behauptung. Dass wir hier schon $h_{\mathbb{Q}(\sqrt{-3})} = 1$ verwenden, bringt übrigens unseren Beweis nicht durcheinander, da wir uns mit der gegenwärtigen Argumentation nur auf eine endliche Menge von Beispielen reduzieren, die wir per Hand überprüfen müssen. Wir werden das allerdings nur für $\mathbb{Z}[\frac{1+\sqrt{-163}}{2}]$ durchführen, wo es tatsächlich schwieriger ist als hier, da dort der Ring nicht euklidisch ist.

Aus diesen Lösungen können wir durch Rückwärtsrechnen die möglichen Werte des Ausdrucks $\gamma_2(\frac{-3+\sqrt{d}}{2})$ als

$$0, -32, -96, -960, -5280, -640320$$

bestimmen. Aus dem zugehörigen $j$-Wert lässt sich jeweils eindeutig ein $d$ bestimmen; als Werte von $d$ kommen demnach nur infrage:

$$d \in \{-3, -11, -19, -43, -67, -163\} \cap \{n \in \mathbb{Z} \mid n < -60\} = \{-67, -163\}.$$

Insgesamt haben wir gezeigt, dass es nur eine endliche Menge von (quadratfreien) $d < 0$ gibt, für die $\mathbb{Q}(\sqrt{d})$ Klassenzahl 1 hat. Diese endliche Menge ist enthalten in

$$\begin{aligned}&\Big(\{-8 < d\} \cup \{-60 < d \leq -8 \mid |d| \equiv 3 \bmod (8)\} \cup \{-67, -163\}\Big) \cap \{d \text{ quadratfrei}\} \\ =&\{-1, -2, -3, -5, -6, -7\} \cup \{-11, -19, -35, -43, -59\} \cup \{-67, -163\}.\end{aligned}$$

Nicht alle Werte von $d$ gehören schon zu Körpern der Klassenzahl 1, zum Beispiel hatten wir in der Bemerkung nach Proposition 5.6 schon eingesehen, dass $\mathbb{Q}(\sqrt{-5})$ kein Hauptidealring ist. Genauso lässt sich dies für $d = -6, -35, -59$ zeigen. Für die restlichen neun Werte von $d$ kann man nun per Hand nachrechnen, dass Klassenzahl 1 vorliegt. Wir führen dies nur im Fall $d = -163$ durch, der uns besonders interessiert. Für die anderen Werte von $d$ lässt sich unser Beweis fast genauso durchführen; wie in Fußnote[20] angemerkt geht es in einigen Fällen allerdings auch einfacher.

**Lemma 8.5** *Die Klassenzahl von* $\mathbb{Q}(\sqrt{-163})$ *ist* 1.

*Beweis.* Wegen der eindeutigen Primfaktorzerlegung für Dedekindringe genügt es zu zeigen, dass alle Primideale im Ganzheitsring $\mathcal{O} = \mathbb{Z}[\frac{1+\sqrt{-163}}{2}]$ Hauptideale sind. Wir hatten bereits eingesehen, dass es für jedes Primideal $\mathfrak{p}$ von $\mathcal{O}$ eine Primzahl $p \in \mathbb{Z}$ mit $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ gibt. Offensichtlich gilt dann umgekehrt $\mathfrak{p} \supseteq p\mathcal{O}$, also $\mathfrak{p} \mid p\mathcal{O}$. Gehen wir also von den Primzahlen $p \in \mathbb{Z}$ aus und studieren die zugehörigen Primteiler in $\mathcal{O}$.

Wie viele Primfaktoren kann das Ideal $p\mathcal{O} \trianglelefteq \mathcal{O}$ haben? Betrachten wir die Abbildung $\mathfrak{N}$, die einem Ideal $\mathfrak{a} \trianglelefteq \mathcal{O}$ den Index $[\mathcal{O} : \mathfrak{a}]$ zuordnet; das ist die ***Absolutnorm***. Aus dem chinesischen Restsatz und $\mathfrak{p}^i/\mathfrak{p}^{i+1} \cong \mathcal{O}/\mathfrak{p}$ folgt, dass $\mathfrak{N}$ multiplikativ ist, dass also

$$\mathfrak{N}(\mathfrak{a} \cdot \mathfrak{b}) = \mathfrak{N}(\mathfrak{a}) \cdot \mathfrak{N}(\mathfrak{b})$$

für alle $\mathfrak{a}, \mathfrak{b} \trianglelefteq \mathcal{O}$ gilt. Da offensichtlich $\mathcal{O}$ selbst das einzige Ideal mit Absolutnorm 1 ist und $\mathfrak{N}(p\mathcal{O}) = p^2$ gilt, kann $p\mathcal{O}$ in $\mathcal{O}$ höchstens in zwei Primfaktoren zerfallen. Die drei Fälle sind:

- $p\mathcal{O}$ ist wieder ein Primideal. Dann heißt $p$ ***träge*** in $K$.
- Es gilt $p\mathcal{O} = \mathfrak{p}_1 \cdot \mathfrak{p}_2$ mit Primidealen $\mathfrak{p}_1 \neq \mathfrak{p}_2 \trianglelefteq \mathcal{O}$. Dann heißt $p$ ***zerlegt*** in $K$.
- Es gilt $p\mathcal{O} = \mathfrak{p}^2$ mit einem Primideal $\mathfrak{p} \trianglelefteq \mathcal{O}$. Dann heißt $p$ ***verzweigt*** in $K$.

Den ersten Fall müssen wir nicht weiter studieren, denn $p\mathcal{O}$ ist offensichtlich ein Hauptideal in $\mathcal{O}$. Sei also $p \in \mathbb{Z}$ eine Primzahl, für die $p\mathcal{O}$ nicht prim ist, und seien $\mathfrak{p}_1, \mathfrak{p}_2$ die nicht notwendig verschiedenen zugehörigen Primfaktoren. Dann ist wegen der Multiplikativität der Absolutnorm $\mathfrak{N}(\mathfrak{p}_1) = \mathfrak{N}(\mathfrak{p}_2) = p$.

Studieren wir noch die Absolutnorm von Hauptidealen. Sei dafür $\alpha = a + b\frac{1+\sqrt{-163}}{2}$ mit $a, b \in \mathbb{Z}$. Dann gilt

$$\alpha\mathcal{O} = \left(a + b\frac{1+\sqrt{-163}}{2}\right)\mathbb{Z} + \left(-41b + (a+b)\frac{1+\sqrt{-163}}{2}\right)\mathbb{Z},$$

wo wir das Minimalpolynom $f(X) = X^2 - X + 41$ von $\frac{1+\sqrt{-163}}{2}$ über $\mathbb{Z}$ benutzt haben, also

$$\mathfrak{N}(\alpha\mathcal{O}) = [\mathcal{O} : \alpha\mathcal{O}] = \det\begin{pmatrix} a & b \\ -41b & a+b \end{pmatrix} = a^2 + ab + 41b^2 = |\alpha|^2.$$

Es bleibt zu zeigen, dass jede Primzahl $p \in \mathbb{Z}$, für die $p\mathcal{O} \trianglelefteq \mathcal{O}$ nicht prim ist, von der Form $p = a^2 + ab + 41b^2$ mit $a, b \in \mathbb{Z}$ ist, denn mit $\alpha = a + b\frac{1+\sqrt{-163}}{2}$ folgt dann $p = \alpha\mathcal{O} \cdot \bar{\alpha}\mathcal{O}$, also die Behauptung.

Man zeigt zunächst mit dem Quadratischen Reziprozitätsgesetz, dass eine Primzahl $p$ genau dann von der gewünschten Form ist, wenn sie kein quadratischer Nichtrest modulo 163 ist (siehe Satz 2.4.4 in [Schm]). Andererseits ist $(\frac{p}{163}) = (\frac{-163}{p})$, und $f$ zerfällt modulo $p$ genau dann, wenn man in $\mathbb{F}_p$ aus $-163$ eine Quadratwurzel ziehen kann. Letzteres ist genau dann der Fall, wenn $p\mathcal{O} \trianglelefteq \mathcal{O}$ nicht prim ist (siehe Satz 6.5.14 in [Schm]), was zu zeigen war. □

Insgesamt können wir die Ergebnisse dieses Abschnitts im folgenden Satz von Stark-Heegner zusammenfassen.

**Satz 8.6** *Sei $\mathbb{Q}(\sqrt{d})$ mit $d \in \mathbb{Z}_{<0}$ quadratfrei ein imaginär-quadratischer Zahlkörper mit Klassenzahl 1. Dann ist $d$ eine der neun* ***Heegnerzahlen***

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

## Literatur


[Dic] Leonard Dickson. *History of the Theory of Numbers, Vol. III*. Stechert, 1934.

[For] O. Forster. *Riemannsche Flächen*. Heidelberger Taschenbücher, Nr. **184**. Springer, 1977.

[FB] E. Freitag, R. Busam. *Funktionentheorie (2. Auflage)*. Springer, 1995.

[Gar] M. Gardner. *Mathematical Games: Six Sensational Discoveries that Somehow or Another have Escaped Public Attention*. Sci. Amer. **232** (1975), pages 127-131.

[Gol] D. Goldfeld. *Gauss' Class Number Problem for Imaginary Quadratic Fields*. Bull. Amer. Math. Soc. **13** (1985), pages 23-37.

[Gre] B. J. Green. *The Ramanujan Constant*.
online: `www-math.mit.edu/~green/ramanujanconstant.pdf`

[Har] R. Hartshorne. *Algebraic Geometry*. GTM, Nr. **52**. Springer, 1977.

[Kas] H. Kasten. *Funktionentheorie 2*.
online auf: `www.mathi.uni-heidelberg.de/~kasten/files/Skripte`

[Koh] W. Kohnen. *A Very Simple Proof of the $q$-Product Expansion of the $\Delta$-Function*. The Ramanujan J. **10** (2005), pages 71-73.

[Neu] J. Neukirch. *Algebraische Zahlentheorie*. Springer, 1992.

[Pet] H. Petersson. *Über die Entwicklungskoeffizienten der automorphen Formen*. Acta Math. **58** (1932), pages 169-215.

[Ram] S. Ramanujan. *Modular Equations and Approximations to $\pi$*. Quart. J. Pure Appl. Math. **45** (1914), pages 350-372.

[Schm] A. Schmidt. *Einführung in die algebraische Zahlentheorie*. Springer, 2007.

[Schn] T. Schneider. *Transzendenzuntersuchungen periodischer Funktionen I. Transzendenz von Potenzen*. J. reine angew. Math. **172** (1934), pages 65-69.

[Sil1] J. H. Silverman. *The Arithmetic of Elliptic Curves*. GTM, Nr. **106**. Springer, 1986.

[Sil2] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. GTM, Nr. **151**. Springer, 1994.

[Sta] H. M. Stark. *On the "Gap" in a Theorem of Heegner*. J. Number Theory **1** (1969), pages 16-27.

[Web] H. Weber. *Lehrbuch der Algebra, Vol. III*. Chelsea Publishing Company, 1908.