Modulräume und Modulkurven

Vortrag im Rahmen des Seminars der WE AℓZAGK im Sommersemester 2006 an der Universität Bremen

Gerrit Grenzebach

1. Juni 2006

1 Wiederholung

Um alle Begriffe und Bezeichnungen, die in dieser Ausarbeitung verwendet werden, klarzustellen, beginnen wir zunächst mit einer Erinnerung an einige Begriffe, die in vorherigen Vorträgen vorgestellt worden sind.

1.1 Gitter und komplexe elliptische Kurven

Zunächst die wichtigsten Begriffe:

- Mit $\mathcal{H}$ wird die obere Halbebene in $\mathbb{C}$ bezeichnet.
- $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ ist das von $\omega_1, \omega_2 \in \mathbb{C}$ mit $\frac{\omega_1}{\omega_2} \in \mathcal{H}$ aufgespannte **Gitter**.
  Speziell für $\tau \in \mathcal{H}$ schreibt man: $\Lambda_\tau = \tau\mathbb{Z} \oplus \mathbb{Z}$.
- Für ein Gitter Λ heißt der Quotient $E := \mathbb{C}/\Lambda = \{z + \Lambda \mid z \in \mathbb{C}\}$ **komplexe elliptische Kurve** (oder auch **komplexer Torus**).
  Für Λ_τ schreibt man speziell: $E_\tau = \mathbb{C}/\Lambda_\tau$.
- Eine **Äquivalenzrelation** auf $\mathcal{H}$ ist gegeben durch ($\tau, \tau' \in \mathcal{H}$):
  $$\tau \sim \tau' :\Longleftrightarrow \gamma(\tau) = \tau' \text{ für ein } \gamma \in \mathrm{SL}_2(\mathbb{Z}).$$
  Für $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ ist dabei $\gamma(\tau) = \frac{a\tau+b}{c\tau+d}$.

Für Gitter und elliptische Kurven gelten außerdem die folgenden Lemmata:

Lemma 1: *Für zwei Gitter $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$, $\Lambda' = \omega_1'\mathbb{Z} \oplus \omega_2'\mathbb{Z}$ gilt:*

$$\Lambda' = \Lambda \iff \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \gamma \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \quad \textit{für ein } \gamma \in \mathrm{SL}_2(\mathbb{Z}).$$

Lemma 2: *Seien Λ, Λ' zwei Gitter. Zwischen den elliptischen Kurven $\mathbb{C}/\Lambda$ und $\mathbb{C}/\Lambda'$ gibt es genau dann einen holomorphen Gruppenisomorphismus φ, wenn ein $\mu \in \mathbb{C}$ existiert mit $\mu\Lambda = \Lambda'$. Für φ gilt dann: $\varphi(z + \Lambda) = \mu z + \Lambda'$.*

Insbesondere folgt damit für $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$, $\Lambda_\tau = \tau\mathbb{Z} \oplus \mathbb{Z}$ mit $\tau := \frac{\omega_1}{\omega_2} \in \mathcal{H}$:

$$\tfrac{1}{\omega_2}\Lambda = \Lambda_\tau \quad \Rightarrow \quad \varphi_\tau \colon \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda_\tau \quad \text{mit} \quad \varphi_\tau(z + \Lambda) = \tfrac{z}{\omega_2} + \Lambda_\tau$$
$$\text{ist ein Isomorphismus.}$$

1.2 Kongruenzuntergruppen

Einige Kongruenzuntergruppen von $\mathrm{SL}_2(\mathbb{Z})$ sind ($N \in \mathbb{N} - \{0\}$):

$$\Gamma_0(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \pmod{N} \right\},$$
$$\Gamma_1(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \pmod{N} \right\},$$
$$\Gamma(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \pmod{N} \right\}.$$

$\Gamma(N)$ wird auch als Hauptkongruenzuntergruppe bezeichnet.

Für $N = 1$ gilt: $\Gamma_0(1) = \Gamma_1(1) = \Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$, denn $n \equiv m \pmod{1}$ stets.

2 *N*-Torsionsuntergruppen und Weil-Paarung

Sei Λ ein Gitter, $\mathbb{C}/\Lambda$ eine elliptische Kurve. Auf $\mathbb{C}/\Lambda$ ist die Multiplikation mit N gegeben durch $[N]\colon \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda, z + \Lambda \mapsto Nz + \Lambda$.

Definition 1: *Sei $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ ein Gitter, $\frac{\omega_1}{\omega_2} \in \mathcal{H}$. Die **N-Torsionsuntergruppe $E[N]$ der additiven Torus-Gruppe $\mathbb{C}/\Lambda$** ist erklärt durch:*

$$\begin{aligned} E[N] &:= \left\{ P \in {}^{\mathbb{C}}\!/_{\Lambda} \;\middle|\; [N]P = 0 \right\} = \left\{ (z+\Lambda) \in {}^{\mathbb{C}}\!/_{\Lambda} \;\middle|\; Nz \in \Lambda \right\} \\ &= \left\{ \omega_1 \tfrac{k}{N} + \omega_2 \tfrac{\ell}{N} + \Lambda \;\middle|\; k, \ell \in {}^{\mathbb{Z}}\!/_{N\mathbb{Z}} \right\} \\ &= \left\{ (\omega_1 \tfrac{k}{N} + \Lambda) + (\omega_2 \tfrac{\ell}{N} + \Lambda) \;\middle|\; k, \ell \in {}^{\mathbb{Z}}\!/_{N\mathbb{Z}} \right\} \\ &= \left\langle \tfrac{\omega_1}{N} + \Lambda \right\rangle \times \left\langle \tfrac{\omega_2}{N} + \Lambda \right\rangle. \end{aligned}$$

Folglich wird $E[N]$ von $\frac{\omega_1}{N} + \Lambda$ und $\frac{\omega_2}{N} + \Lambda$ erzeugt. Für $P, Q \in E[N]$ gilt also:

$$\left(\begin{smallmatrix} P \\ Q \end{smallmatrix}\right) = \gamma \begin{pmatrix} \frac{\omega_1}{N} + \Lambda \\ \frac{\omega_2}{N} + \Lambda \end{pmatrix} \qquad \text{für ein } \gamma \in \mathrm{M}_2(\mathbb{Z}/N\mathbb{Z}).$$

Dieses wird für die *Weil-Paarung* benötigt:

Definition 2: *Die **Weil-Paarung** von P und Q ist:*

$$\begin{aligned} e_N\colon E[N] \times E[N] &\to \langle e^{2\pi i/N} \rangle = \{ z \in \mathbb{C} \mid z^N = 1 \}, \\ (P, Q) &\mapsto e^{2\pi i \det\gamma / N}. \end{aligned}$$

Bemerkung: Diese Definition ist sinnvoll, obwohl $\det\gamma \in \mathbb{Z}/N\mathbb{Z}$. Die Weil-Paarung ist unabhängig von der Wahl der Basis $\{\omega_1, \omega_2\}$ des Gitters.

Bei einer festen Basis ist γ eindeutig bestimmt, da alle Komponenten von γ in $\mathbb{Z}/N\mathbb{Z}$ sind.

Sowohl die N-Torsionsuntergruppe als auch die Weil-Paarung werden nur für verschönerte elliptische Kurven zur Kongruenzuntergruppe $\Gamma(N)$ benötigt (☞ Kapitel 4 auf der nächsten Seite).

3 Modulkurven

Definition 3: *Sei $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ eine Kongruenzuntergruppe, die auf der oberen Halbebene von links operiert. Die **Modulkurve $Y(\Gamma)$** ist dann der Quotientenraum der Orbits unter Γ:*

$$Y(\Gamma) := \Gamma \setminus \mathcal{H} = \{\Gamma\tau \mid \tau \in \mathcal{H}\}.$$

Die Modulkurven für $\Gamma_0(N)$, $\Gamma_1(N)$, $\Gamma(N)$ schreiben wir folgendermaßen:

$$Y_0(N) := \Gamma_0(N)\backslash\mathcal{H}, \qquad Y_1(N) := \Gamma_1(N)\backslash\mathcal{H}, \qquad Y(N) := \Gamma(N)\backslash\mathcal{H}.$$

Für $N = 1$ gilt: $Y_0(1) = Y_1(1) = Y(1) = \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H} = \{\mathrm{SL}_2(\mathbb{Z})\tau \mid \tau \in \mathcal{H}\}$.

Bemerkung: Modulkurven sind Riemannsche Flächen und können kompaktifiziert werden.

4 Verschönerte elliptische Kurven und Modulräume

In diesem Abschnitt werden elliptische Kurven $\mathbb{C}/\Lambda$ für die Kongruenzuntergruppen $\Gamma_0(N)$, $\Gamma_1(N)$ und $\Gamma(N)$ mit einer Zusatzstruktur versehen. Diese bezeichnen wir als *verschönerte elliptische Kurven* (engl.: enhanced elliptic curve). Man definiert eine Äquivalenzrelation auf der Menge der verschönerten elliptischen Kurven und nennt die Menge der Äquivalenzklassen *Modulraum*.

Im einzelnen wird folgendes festgelegt:

Definition 4: *Sei $N \in \mathbb{N} - \{0\}$.*

- *Eine verschönerte elliptische Kurve für $\Gamma_0(N)$ ist ein Paar (E, C) mit:*
  - *E: komplexe elliptische Kurve,*
  - *C: zyklische Untergruppe von E der Ordnung N.*

  Für diese Paare wird folgende Äquivalenzrelation eingeführt:

$$(E, C) \sim (E', C') :\Leftrightarrow \exists \text{ hol. Gruppenisomorphismus } \varphi\colon E \xrightarrow{\sim} E' \text{ mit } \varphi(C) = C'.$$

  Die Menge der Äquivalenzklassen wird mit $S_0(N)$ bezeichnet, eine Äquivalenzklasse in $S_0(N)$ wird $[E, C]$ geschrieben.

- *Eine verschönerte elliptische Kurve für $\Gamma_1(N)$ ist ein Paar (E, Q) mit:*
  - *E: komplexe elliptische Kurve,*
  - *Q: Punkt von E der Ordnung N, d. h. $NQ = 0$, $nQ \neq 0$ für $0 < n < N$.*

  Für diese Paare wird folgende Äquivalenzrelation eingeführt:

$$(E, Q) \sim (E', Q') :\Leftrightarrow \exists \text{ hol. Gruppenisomorphismus } \varphi\colon E \xrightarrow{\sim} E' \text{ mit } \varphi(Q) = Q'.$$

  Die Menge der Äquivalenzklassen wird mit $S_1(N)$ bezeichnet, eine Äquivalenzklasse in $S_1(N)$ wird $[E, Q]$ geschrieben.

- *Eine verschönerte elliptische Kurve für $\Gamma(N)$ ist ein Paar $(E,(P,Q))$ mit:*
  - *E: komplexe elliptische Kurve,*
  - *(P,Q): Punktpaar von E, das die N-Torsionsuntergruppe $E[N]$ mit Weil-Paarung $e_N(P,Q) = e^{2\pi i/N}$ generiert.*

  Für diese Paare wird folgende Äquivalenzrelation eingeführt:

  $$(E,(P,Q)) \sim (E',(P',Q')) :\Leftrightarrow \exists \text{ hol. Gruppenisomorphismus } \varphi\colon E \xrightarrow{\sim} E' \text{ mit } \varphi(P)=P',\ \varphi(Q)=Q'.$$

  Die Menge der Äquivalenzklassen wird mit $S(N)$ bezeichnet, eine Äquivalenzklasse in $S(N)$ wird $[E,(P,Q)]$ geschrieben.

*Jede der Mengen $S_0(N)$, $S_1(N)$, $S(N)$ ist ein **Modulraum** von Isomorphieklassen komplexer elliptischer Kurven und sogenannten N-Torsions-Daten. Letztere sind die zyklische Untergruppe C für $S_0(N)$, der Punkt Q für $S_1(N)$ und das Punktepaar (P,Q) für $S(N)$.*

Der folgende Satz liefert eine Beschreibung dieser Modulräume als Quotienten der oberen Halbebene; jeder der Modulräume läßt sich nämlich bijektiv auf die zugehörige Modulkurve abbilden. Damit erhält man auch eine geometrische Beschreibung der formalen Äquivalenzklassen: Jede Klasse von verschönerten elliptischen Kurven entspricht einem Orbit unter der zugehörigen Kongruenzuntergruppe.

Satz 1: *Sei $N \in \mathbb{N} - \{0\}$. Es gilt:*

I: *Der Modulraum für $\Gamma_0(N)$ ist:*

$$S_0(N) = \left\{ \left[E_\tau, \langle \tfrac{1}{N} + \Lambda_\tau \rangle\right] \;\middle|\; \tau \in \mathcal{H} \right\}.$$

Dabei sind zwei Punkte $\left[E_\tau, \langle \frac{1}{N} + \Lambda_\tau\rangle\right]$ und $\left[E_{\tau'}, \langle \frac{1}{N} + \Lambda_{\tau'}\rangle\right]$ genau dann gleich, wenn $\Gamma_0(N)\tau = \Gamma_0(N)\tau'$ ist, d. h. es existiert die Bijektion:

$$\psi_0\colon S_0(N) \to Y_0(N),\ \left[E_\tau = \mathbb{C}/\Lambda_\tau, \langle \tfrac{1}{N} + \Lambda_\tau\rangle\right] \mapsto \Gamma_0(N)\tau.$$

II: *Der Modulraum für $\Gamma_1(N)$ ist:*

$$S_1(N) = \left\{ \left[E_\tau, \tfrac{1}{N} + \Lambda_\tau\right] \;\middle|\; \tau \in \mathcal{H} \right\}.$$

Dabei sind zwei Punkte $\left[E_\tau, \frac{1}{N} + \Lambda_\tau\right]$ und $\left[E_{\tau'}, \frac{1}{N} + \Lambda_{\tau'}\right]$ genau dann gleich, wenn $\Gamma_1(N)\tau = \Gamma_1(N)\tau'$ ist, d. h. es existiert die Bijektion:

$$\psi_1\colon S_1(N) \to Y_1(N),\ \left[E_\tau = \mathbb{C}/\Lambda_\tau, \tfrac{1}{N} + \Lambda_\tau\right] \mapsto \Gamma_1(N)\tau.$$

III: *Der Modulraum für $\Gamma(N)$ ist:*

$$S(N) = \left\{ \left[E_\tau, (\tfrac{\tau}{N} + \Lambda_\tau, \tfrac{1}{N} + \Lambda_\tau)\right] \;\middle|\; \tau \in \mathcal{H} \right\}.$$

Zwei Punkte $\left[E_\tau, (\frac{\tau}{N} + \Lambda_\tau, \frac{1}{N} + \Lambda_\tau)\right]$ und $\left[E_{\tau'}, (\frac{\tau'}{N} + \Lambda_{\tau'}, \frac{1}{N} + \Lambda_{\tau'})\right]$ sind genau dann gleich, wenn $\Gamma(N)\tau = \Gamma(N)\tau'$ ist, d. h. es existiert die Bijektion:

$$\psi\colon S(N) \to Y(N),\ \left[E_\tau = \mathbb{C}/\Lambda_\tau, (\tfrac{\tau}{N} + \Lambda_\tau, \tfrac{1}{N} + \Lambda_\tau)\right] \mapsto \Gamma(N)\tau.$$

Bemerkung: Für $N = 1$ gilt speziell:

$$S_0(1) = S_1(1) = S(1) = \big\{[\mathbb{C}/\Lambda_\tau, \Lambda_\tau] \;\big|\; \tau \in \mathcal{H}\big\} =: \big\{[\mathbb{C}/\Lambda_\tau] \;\big|\; \tau \in \mathcal{H}\big\}.$$

Nach obigem Satz existiert damit eine Bijektion

$$\psi\colon \big\{[\mathbb{C}/\Lambda_\tau] \;\big|\; \tau \in \mathcal{H}\big\} \xrightarrow{\sim} \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}, \quad [\mathbb{C}/\Lambda_\tau] \mapsto \mathrm{SL}_2(\mathbb{Z})\tau.$$

Jeder Isomorphieklasse komplexer elliptischer Kurven entspricht also genau einer Äquivalenzklasse von Punkten der oberen Halbebene unter der Aktion der Modulgruppe $\mathrm{SL}_2(\mathbb{Z})$.

Beweis: Wir beweisen nur II, die Beweise für I und III sind ähnlich. Der Beweis erfolgt in drei Schritten: Zunächst wird der Modulraum $S_1(N)$ behandelt, danach werden beide Richtungen der Äquivalenz bewiesen.

Zu zeigen: $S_1(N) = \Big\{\big[E_\tau, \frac{1}{N} + \Lambda_\tau\big] \;\Big|\; \tau \in \mathcal{H}\Big\}$.

Beweis: Sei $[E, Q] \in S_1(N)$ beliebig. Ohne Einschränkung läßt sich $E = \mathbb{C}/\Lambda_{\tau'}$ für ein $\tau' \in \mathcal{H}$ wählen, da für jede elliptische Kurve $\mathbb{C}/\Lambda$ mit $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ gilt (vgl. Lemma 2):

$$\mathbb{C}\big/_{\Lambda} \cong \mathbb{C}\big/_{\Lambda_\tau} \qquad \text{für ein } \tau \in \mathcal{H},\ \Lambda_\tau = \tau\mathbb{Z} \oplus \mathbb{Z}.$$

Für Q können wir daher $Q = \frac{c\tau'+d}{N} + \Lambda_{\tau'}$ setzen mit geeigneten $c, d \in \mathbb{Z}$. Dabei ist $\mathrm{ggT}(c, d, N) = 1$, denn sonst hätte man:

$$\begin{aligned} & \mathrm{ggT}(c, d, N) = n \text{ mit } 1 < n \le N \\ \Rightarrow\quad & c = \tilde{c}n, d = \tilde{d}n, N = \tilde{N}n \\ \Rightarrow\quad & \tilde{N}Q = \tilde{N}\tfrac{c\tau'+d}{N} + \Lambda_{\tau'} = \tilde{N}\tfrac{\tilde{c}\tau'+\tilde{d}}{\tilde{N}} + \Lambda_{\tau'} = \Lambda_{\tau'} \quad \lightning \end{aligned}$$

Widerspruch zu „Q Punkt der Ordnung N“.

Es gibt nun $a, b, k \in \mathbb{Z}$ so, daß $1 = ad - bc - kN \equiv ad - bc \pmod{N}$. Für die Matrix $\gamma := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{M}_2(\mathbb{Z})$ folgt dann:

$$\gamma \bmod N \in \mathrm{SL}_2\Big(\mathbb{Z}\big/_{N\mathbb{Z}}\Big).$$

Da die Abbildung $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ surjektiv ist (☞ Anhang), können wir auch $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ wählen. Dabei muß man die Einträge von γ nur um Vielfache von N ändern, was den Punkt Q invariant läßt.

Sei $\tau := \gamma(\tau') = \frac{a\tau'+b}{c\tau'+d}$ und $\mu := c\tau' + d$. Dann ist $\mu\tau = a\tau' + b$ und also:

$$\mu\Lambda_\tau = \mu(\tau\mathbb{Z} \oplus \mathbb{Z}) = (a\tau' + b)\mathbb{Z} \oplus (c\tau' + d)\mathbb{Z} = \Lambda_{\tau'}, \tag{1}$$

wobei für das letzte Gleichheitszeichen das Lemma 1 von Seite 1 angewendet worden ist. Nach Lemma 2 existiert nun ein Isomorphismus $\varphi\colon \mathbb{C}/\Lambda_\tau \xrightarrow{\sim} \mathbb{C}/\Lambda_{\tau'}$ mit $\varphi(z + \Lambda_\tau) = \mu z + \Lambda_{\tau'}$. Man hat also speziell:

$$\varphi(\tfrac{1}{N} + \Lambda_\tau) = \mu\tfrac{1}{N} + \Lambda_{\tau'} = \tfrac{c\tau'+d}{N} + \Lambda_{\tau'} = Q,$$

weshalb für die Äquivalenzklasse $[E, Q]$ gilt:

$$\boxed{[E,Q] = \left[\mathbb{C}/\Lambda_{\tau'}, \tfrac{c\tau'+d}{N} + \Lambda_{\tau'}\right] = \left[\mathbb{C}/\mu\Lambda_{\tau}, \mu(\tfrac{1}{N} + \Lambda_{\tau})\right] = \left[\mathbb{C}/\Lambda_{\tau}, (\tfrac{1}{N} + \Lambda_{\tau})\right]}$$

□

Zu zeigen: $\left[E_\tau, \frac{1}{N} + \Lambda_\tau\right] = \left[E_{\tau'}, \frac{1}{N} + \Lambda_{\tau'}\right] \iff \Gamma_1(N)\tau = \Gamma_1(N)\tau'$.

Beweis:

„⇐": Es gebe $\tau, \tau' \in \mathcal{H}$ mit $\Gamma_1(N)\tau = \Gamma_1(N)\tau'$, d. h. für jedes $\gamma_1 \in \Gamma_1(N)$ gibt es ein $\gamma_2 \in \Gamma_1(N)$, so daß $\gamma_1\tau = \gamma_2\tau'$. Also existiert ein $\gamma := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(\mathbb{Z})$ mit $\tau = \gamma(\tau')$.

Für $\mu := c\tau' + d$ hat man wie oben:

$$\mu\Lambda_\tau = \Lambda_{\tau'}, \quad \mu(\tfrac{1}{N} + \Lambda_\tau) = \tfrac{c\tau'+d}{N} + \Lambda_{\tau'}.$$

Da $(c, d) \equiv (0, 1) \pmod N$, ist $\mu(\frac{1}{N} + \Lambda_\tau) = \frac{1}{N} + \Lambda_{\tau'}$. Dieses gibt:

$$\left[\mathbb{C}/\Lambda_\tau, \tfrac{1}{N} + \Lambda_\tau\right] = \left[\mathbb{C}/\Lambda_{\tau'}, \tfrac{1}{N} + \Lambda_{\tau'}\right].$$

„⇒": Sei nun $\left[\mathbb{C}/\Lambda_\tau, \frac{1}{N} + \Lambda_\tau\right] = \left[\mathbb{C}/\Lambda_{\tau'}, \frac{1}{N} + \Lambda_{\tau'}\right]$ für $\tau, \tau' \in \mathcal{H}$; es existiert also ein holomorpher Gruppenisomorphismus $\varphi\colon \mathbb{C}/\Lambda_\tau \xrightarrow{\sim} \mathbb{C}/\Lambda_{\tau'}$ mit $\varphi(\frac{1}{N} + \Lambda_\tau) = \frac{1}{N} + \Lambda_{\tau'}$. Gemäß Lemma 2 gilt außerdem für ein $\mu \in \mathbb{C}$:

- $\varphi(\frac{1}{N} + \Lambda_\tau) = \mu(\frac{1}{N} + \Lambda_\tau)$,
- $\mu\Lambda_\tau = \Lambda_{\tau'}$, also: $\mu\tau\mathbb{Z} \oplus \mu\mathbb{Z} = \tau'\mathbb{Z} \oplus \mathbb{Z}$.

Nach Lemma 1 existiert nun $\gamma := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ mit

$$\begin{pmatrix} \mu\tau \\ \mu \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \tau' \\ 1 \end{pmatrix} = \begin{pmatrix} a\tau' + b \\ c\tau' + d \end{pmatrix}. \tag{2}$$

Folglich ist $\mu = c\tau' + d$; daher gilt:

$$\tfrac{c\tau'+d}{N} + \Lambda_{\tau'} = \tfrac{1}{N} + \Lambda_{\tau'} \quad \Rightarrow \quad (c, d) \equiv (0, 1) \pmod N.$$

Wegen

$$1 = ad - bc \;\equiv\; a \cdot 1 - b \cdot 0 \pmod N \;=\; a \pmod N$$

folgt insgesamt $\gamma \in \Gamma_1(N)$.

Aus Gleichung (2) geht außerdem $\tau = \gamma(\tau') = \frac{a\tau'+b}{c\tau'+d}$ hervor; insgesamt erhält man damit:

$$\Gamma_1(N)\tau = \Gamma_1(N)\gamma(\tau') = \Gamma_1(N)\tau'. \qquad \square$$

Die Existenz der Bijektion ψ_1 ist klar. ■

5 Weitere Modulformen

Definition 5: (a) *Sei $k \in \mathbb{Z}$, $\Gamma \in \{\Gamma_0(N), \Gamma_1(N), \Gamma(N)\}$. Eine komplexwertige Funktion F der verschönerten elliptischen Kurven für Γ ist* ***unter Γ homogen vom Grad k****, wenn für jedes $\mu \in \mathbb{C} - \{0\}$ gilt:*

$$\begin{aligned} F\big(\mathbb{C}/\mu\Lambda, \mu C\big) &= \tfrac{1}{\mu^k} F\big(\mathbb{C}/\Lambda, C\big) && \text{für } \Gamma = \Gamma_0(N), \\ F\big(\mathbb{C}/\mu\Lambda, \mu Q\big) &= \tfrac{1}{\mu^k} F\big(\mathbb{C}/\Lambda, Q\big) && \text{für } \Gamma = \Gamma_1(N), \\ F\big(\mathbb{C}/\mu\Lambda, (\mu P, \mu Q)\big) &= \tfrac{1}{\mu^k} F\big(\mathbb{C}/\Lambda, (P, Q)\big) && \text{für } \Gamma = \Gamma(N). \end{aligned}$$

(b) *Für eine solche Funktion F läßt sich eine korrespondierende* ***dehomogenisierte Funktion*** *$f\colon \mathcal{H} \to \mathbb{C}$ festlegen durch:*

$$f(\tau) = \begin{cases} F\big(\mathbb{C}/\Lambda_\tau, \langle \frac{1}{N} + \Lambda_\tau \rangle\big) & \text{für } \Gamma = \Gamma_0(N), \\ F\big(\mathbb{C}/\Lambda_\tau, \frac{1}{N} + \Lambda_\tau\big) & \text{für } \Gamma = \Gamma_1(N), \\ F\big(\mathbb{C}/\Lambda_\tau, (\frac{\tau}{N} + \Lambda_\tau, \frac{1}{N} + \Lambda_\tau)\big) & \text{für } \Gamma = \Gamma(N). \end{cases}$$

Satz 2: *Sei $\Gamma \in \{\Gamma_0(N), \Gamma_1(N), \Gamma(N)\}$. Dann ist eine wie in Definition 5 dehomogenisierte Funktion $f\colon \mathcal{H} \to \mathbb{C}$ unter Γ invariant vom Gewicht k, d. h. für alle $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ ist $f(\gamma(\tau)) = (c\tau + d)^k f(\tau)$.*

Beweis: Wir zeigen den Satz nur für den Fall $\Gamma = \Gamma_1(N)$.
Sei $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(N)$, also $\gamma \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \pmod N$. Für ein beliebiges $\tau \in \mathcal{H}$ sei $\mu := \frac{1}{c\tau + d}$. Dann ist $\gamma(\tau) = \mu(a\tau + b)$. Für das Gitter $\Lambda_{\gamma(\tau)} = \gamma(\tau)\mathbb{Z} \oplus \mathbb{Z}$ gilt dann:

$$\Lambda_{\gamma(\tau)} = \mu(a\tau + b)\mathbb{Z} \oplus \mu(c\tau + d)\mathbb{Z} = \mu(\tau\mathbb{Z} \oplus \mathbb{Z}) = \mu\Lambda_\tau,$$

wobei wegen $\left(\begin{smallmatrix} a\tau + b \\ c\tau + d \end{smallmatrix}\right) = \gamma\left(\begin{smallmatrix} \tau \\ 1 \end{smallmatrix}\right)$ einmal das Lemma 1 Anwendung fand.

Somit folgt:

$$\begin{aligned} f(\gamma(\tau)) &= F\big(\mathbb{C}/\Lambda_{\gamma(\tau)}, \tfrac{1}{N} + \Lambda_{\gamma(\tau)}\big) \\ &= F\big(\mathbb{C}/\mu\Lambda_\tau, \tfrac{\mu(c\tau+d)}{N} + \Lambda_\tau\big) \\ &= \tfrac{1}{\mu^k} F\big(\mathbb{C}/\Lambda_\tau, \underbrace{\tfrac{c\tau+d}{N} + \Lambda_\tau}_{= \frac{1}{N} + \Lambda_\tau, \text{ da } (c,d) \equiv (0,1) \pmod N}\big) \\ &= (c\tau + d)^k f(\tau). \end{aligned}$$

■

Es gibt ebenfalls den umgekehrten Fall, bei dem man zu f eine homogene Funktion F definiert:

Satz 3: *Sei $\Gamma \in \{\Gamma_0(N), \Gamma_1(N), \Gamma(N)\}$. Sei $f\colon \mathcal{H} \to \mathbb{C}$ eine unter Γ invariante Funktion vom Gewicht k. Dann ist durch*

$$F\big(\mathbb{C}/\Lambda_\tau, (\textit{Torsionsdaten})\big) := f(\tau)$$

eine komplexwertige Funktion auf verschönerten elliptischen Kurven gegeben. Diese ist unter Γ homogen vom Grad k.

Beweis: Auch diesen Satz zeigen wir nur für $\Gamma = \Gamma_1(N)$.

- F ist wohldefiniert:
  Seien dazu $\tau, \tau' \in \mathcal{H}$ mit $\tau \neq \tau'$ und $\left(\mathbb{C}/\Lambda_\tau, \frac{1}{N} + \Lambda_\tau\right) = \left(\mathbb{C}/\Lambda_{\tau'}, \frac{1}{N} + \Lambda_{\tau'}\right)$; es gilt also: $\Lambda_\tau = \Lambda_{\tau'}$. Aus Lemma 1 folgt dann:

  $$\exists \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \text{ mit } \left(\begin{smallmatrix} \tau' \\ 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} \tau \\ 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} a\tau+b \\ c\tau+d \end{smallmatrix}\right).$$

  Also ist: $(c, d) = (0, 1)$ und wegen $\det \gamma = 1$ auch $a = 1$. Dieses liefert:

  $$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_1(N).$$

  Außerdem folgt: $\gamma(\tau) = \tau + b = \tau'$. Damit erhält man:

  $$\begin{aligned} F\left(\mathbb{C}/\Lambda_{\tau'}, \tfrac{1}{N} + \Lambda_{\tau'}\right) &= f(\tau') = f(\gamma(\tau)) \\ &= (0\tau + 1)^k f(\tau) = f(\tau) = F\left(\mathbb{C}/\Lambda_\tau, \tfrac{1}{N} + \Lambda_\tau\right). \end{aligned}$$

  Für gleiche verschönerte elliptische Kurven liefert also F denselben Wert, d. h. F ist wohldefiniert.

- F ist homogen vom Grad k:
  Seien $\left(\mathbb{C}/\Lambda_\tau, \frac{1}{N} + \Lambda_\tau\right)$ und $\left(\mathbb{C}/\Lambda_{\tau'}, \frac{1}{N} + \Lambda_{\tau'}\right)$ zwei äquivalente verschönerte elliptische Kurven. Nach Satz 1.II gilt dann: $\Gamma_1(N)\tau = \Gamma_1(N)\tau'$, d. h. es gibt ein $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(N)$ mit $\tau = \gamma\tau'$. Nach Gleichung (1) ist dann $(c\tau' + d)\Lambda_\tau = \Lambda_{\tau'}$. Damit folgt:

  $$\begin{aligned} F\left(\mathbb{C}/\Lambda_\tau, \tfrac{1}{N} + \Lambda_\tau\right) &= f(\tau) = f(\gamma(\tau')) \\ &= (c\tau' + d)^k f(\tau') = (c\tau' + d)^k F\left(\mathbb{C}/\Lambda_{\tau'}, \tfrac{1}{N} + \Lambda_{\tau'}\right). \end{aligned}$$

  Also ist F unter $\Gamma_1(N)$ homogen vom Grad k. ∎

6 Ein Beispiel

Für $N = 1$ ist $\Gamma_0(1) = \Gamma_1(1) = \Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$. Es gibt formal drei Möglichkeiten, verschönerte elliptische Kurven festzulegen, nämlich durch die Wahl der Torsionsdaten zur elliptischen Kurve $E = \mathbb{C}/\Lambda$:

- C: zyklische Untergruppe von E der Ordnung 1, also $C = \{0 + \Lambda\}$,
- Q: Punkt von E der Ordnung 1, also $Q = 0 + \Lambda$,
- (P, Q): Punktepaar, welches die 1-Torsionsuntergruppe $E[1] = \{0 + \Lambda\}$ erzeugt, also $(P, Q) = (0 + \Lambda, 0 + \Lambda)$.

Diese Möglichkeiten unterscheiden sich offenbar nur unwesentlich, man kann in diesem Fall die drei Typen verschönerter elliptischer Kurven miteinander identifizieren; wir schreiben dann $\left(\mathbb{C}/\Lambda, 0 + \Lambda\right)$ für die verschönerte elliptische Kurve.

Mit der Eisensteinreihe G_k vom Gewicht k, $k > 2$ gerade, läßt sich nun eine komplexe Funktion F auf den verschönerten elliptischen Kurven für $\mathrm{SL}_2(\mathbb{Z})$ konstruieren:

$$F\big(\mathbb{C}/\Lambda, 0+\Lambda\big) := G_k(\Lambda) = \sum_{\omega\in\Lambda}{}' \frac{1}{\omega^k}.$$

Wegen $\mathbb{C}/\Lambda = \mathbb{C}/\Lambda' \iff \Lambda = \Lambda'$ ist F wohldefiniert.

Außerdem ist F unter $\mathrm{SL}_2(\mathbb{Z})$ homogen vom Grad k, denn für die Eisensteinreihe gilt mit $\mu \in \mathbb{C} - \{0\}$:

$$G_k(\mu\Lambda) = \sum_{\omega\in\mu\Lambda}{}' \frac{1}{\omega^k} = \sum_{\omega\in\Lambda}{}' \frac{1}{(\mu\omega)^k} = \frac{1}{\mu^k} G_k(\Lambda).$$

Wie in Definition 5 legen wir eine dehomogenisierte Funktion $f\colon \mathcal{H} \to \mathbb{C}$ fest:

$$f(\tau) := F\big(\mathbb{C}/\Lambda_\tau, 0+\Lambda_\tau\big) = G_k(\Lambda_\tau) = \sum_{(p,q)\in\mathbb{Z}\times\mathbb{Z}}{}' \frac{1}{(p\tau+q)^k}.$$

Man schreibt auch $G_k(\tau)$ für $f(\tau)$ und erhält damit eine Eisensteinreihe auf der oberen Halbebene $\mathcal{H}$.

Für $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ und $(p,q) \in \mathbb{Z}\times\mathbb{Z}$ gilt:

$$p\gamma(\tau) + q = p\tfrac{a\tau+b}{c\tau+d} + q = \tfrac{1}{c\tau+d}\Big((ap+cq)\tau + (bp+dq)\Big) = \tfrac{1}{c\tau+d}(p'\tau+q').$$

Damit folgt:

$$f(\gamma(\tau)) = \sum_{(p,q)}{}' \frac{1}{(p\frac{a\tau+b}{c\tau+d}+q)^k} = (c\tau+d)^k \sum_{(p',q')}{}' \frac{1}{(p'\tau+q')^k} = (c\tau+d)^k f(\tau),$$

also ist f unter $\mathrm{SL}_2(\mathbb{Z})$ invariant vom Gewicht k.

Literatur

Diamond, Fred und Jerry Shurman.
A first course in modular forms.
New York: Springer, 2005.

Freitag, Eberhard und Rolf Busam.
Funktionentheorie 1. 3., neu bearb. und erw. Aufl.
Berlin; Heidelberg; New York: Springer, 2000.

Anhang

A Die Abbildung $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$

Die Abbildung $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, $\gamma \mapsto \gamma \bmod N$, ist surjektiv. Dieses geht aus folgendem Lemma hervor:

Lemma 3: *Sei* $N \in \mathbb{N} - \{0\}$, $\gamma \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. *Durch Liften von* γ *erhält man* $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{M}_2(\mathbb{Z})$. *Es gilt:*

I: $\mathrm{ggT}(c, d, N) = 1$,
II: *es gibt* $c' = c + sN$, $d' = d + tN$, $s, t \in \mathbb{Z}$, *mit* $\mathrm{ggT}(c', d') = 1$,
III: *es gibt einen Lift* $\gamma' = \left(\begin{smallmatrix} a+kN & b+\ell N \\ c' & d' \end{smallmatrix}\right)$ *von* γ *mit* $\gamma' \in \mathrm{SL}_2(\mathbb{Z})$.

Bemerkung: Für die Matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{M}_2(\mathbb{Z})$ ist $ad - bc = 1 + qN$ mit $q \in \mathbb{Z}$.

Beweis: Für $N = 1$ ist nichts zu zeigen. Im folgenden sei daher stets $N > 1$.

ad I: Annahme: $\mathrm{ggT}(c, d, N) = n > 1$. Dann ist $c = \tilde{c}n$, $d = \tilde{d}n$ und $N = \tilde{N}n$. Es folgt:

$$1 = ad - bc - qN = (\underbrace{a\tilde{d} - b\tilde{c} - q\tilde{N}}_{\in\mathbb{Z}})n \quad \lightning$$

ad II: Wegen obiger Bemerkung ist $(c, d) \neq (0, 0)$. Falls $c = 0$, ist $\mathrm{ggT}(d, N) = 1$ gemäß I; setze also $c' := N$ und $d' := d$.

Sei nun $c \neq 0$. Sei $m := \mathrm{ggT}(c, d)$, also $\mathrm{ggT}(m, N) = 1$ wegen I. Außerdem gilt $c = c_1 m$ und $d = d_1 m$ mit $\mathrm{ggT}(c_1, d_1) = 1$.

Zerlege $c_1 = \tilde{c}_1 \tilde{m}$ so, daß $\mathrm{ggT}(\tilde{c}_1, m) = 1$ und jeder Primteiler von $\tilde{m}$ auch m teilt. Dann ist $\mathrm{ggT}(c, d + \tilde{c}_1 N) = \mathrm{ggT}(\tilde{c}_1 \tilde{m} m, d_1 m + \tilde{c}_1 N) = 1$, denn:

- Jeder Teiler von $\tilde{c}_1$ teilt $\tilde{c}_1 N$, aber weder d_1 noch m.
- Jeder Primteiler von m (bzw. $\tilde{m}$) teilt $d_1 m$, aber weder $\tilde{c}_1$ noch N. Damit teilt kein Teiler von $\tilde{m}m$ die Summe $d_1 m + \tilde{c}_1 N$.

$c' := c$ und $d' := d + \tilde{c}_1 N$ leisten hier also das Gewünschte.

ad III: Für $\det \gamma' = ad' - bc' + (kd' - \ell c')N$ folgt mit II ($c' = c + sN$, $d' = d + tN$):

$$\begin{aligned} \det \gamma' &= \underbrace{ad - bc}_{=1+qN} + (at - bs)N + (kd' - \ell c')N \\ &= 1 + (\underbrace{q + at - bs}_{=:\tilde{q}})N + (kd' - \ell c')N. \end{aligned}$$

Dieses gilt für beliebige $k, \ell \in \mathbb{Z}$.

Da $\mathrm{ggT}(c', d') = 1$, findet man mit dem Euklidischen Algorithmus ganze Zahlen $\tilde{k}, \tilde{\ell}$, so daß:

$$1 = -\tilde{k}d' + \tilde{\ell}c' \implies \tilde{q} = -\tilde{q}\tilde{k}d' + \tilde{q}\tilde{\ell}c'.$$

Wählt man $k := \tilde{q}\tilde{k}$ und $\ell := \tilde{q}\tilde{\ell}$, so ist $\det \gamma' = 1$, also $\gamma' \in \mathrm{SL}_2(\mathbb{Z})$. ∎