Prof. Dr. Irene Bouw
Christian Steck
Sommersemester 2014

Übungsblatt 7

Elliptische Kurven

Die Besprechung erfolgt am Mittwoch, dem 2.7.2014,
um 12:00 Uhr in He18 - E60.

Aufgabe 1 (1+4)

Für $\tau \in \mathbb{C}\backslash\mathbb{R}$ bezeichnen wir mit Λ_τ das Gitter $\mathbb{Z} \cdot 1 \oplus \mathbb{Z} \cdot \tau$. Sind Λ und Λ' Gitter in $\mathbb{C}$, so nennen wir diese *homothetisch*, falls es ein $\alpha \in \mathbb{C}^\times$ mit $\Lambda = \alpha\Lambda'$ gibt. Zeigen Sie die folgenden Aussagen.

(a) Jedes Gitter $\Lambda \subset \mathbb{C}$ ist homothetisch zu einem Gitter Λ_τ mit $\tau \in \mathbb{H}$.

(b) Zwei Gitter Λ_τ und $\Lambda_{\tau'}$ mit $\tau, \tau' \in \mathbb{H}$ sind genau dann homothetisch, wenn es ein Element $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ mit $\gamma \circ \tau = \tau'$ gibt.

Bemerkung: Hier bezeichnet $\circ$ die Wirkung von $\mathrm{SL}_2(\mathbb{Z})$ auf $\mathbb{H}$, die gegeben ist durch

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \circ z := \frac{az+b}{cz+d}.$$

Aufgabe 2 (2+1+2)

Für ein Gitter $\Lambda \subset \mathbb{C}$ wurden in der Vorlesung $g_2(\Lambda)$ und $g_3(\Lambda)$ definiert. Ferner sind

$$\Delta(\Lambda) := g_2(\Lambda)^3 - 27g_3(\Lambda)^2 \quad \text{und} \quad j(\Lambda) := 1728\frac{g_2(\Lambda)^3}{\Delta(\Lambda)}.$$

Zeigen Sie nun für $\alpha \in \mathbb{C}^\times$ die folgenden Aussagen.

(a) Es gilt $g_2(\alpha\Lambda) = \alpha^{-4}g_2(\Lambda)$ und $g_3(\alpha\Lambda) = \alpha^{-6}g_3(\Lambda)$.

(b) Es gilt $j(\alpha\Lambda) = j(\Lambda)$, d.h. homothetische Gitter besitzen die selbe j-Invariante.

Die $\wp$-Funktion zum Gitter Λ erfüllt die Gleichung $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$, entspricht also der elliptischen Kurve $E_\Lambda : y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$.

(c) Zeigen Sie $j(E_\Lambda) = j(\Lambda)$.

Aufgabe 3 (2+3)

Sei $\Lambda \subset \mathbb{C}$ ein nicht entartetes Gitter und $\wp$ die zugehörige Weierstrass-$\wp$-Funktion. Zeigen Sie die Gleichungen

(a) $\wp''(z) = 6\wp(z)^2 - \frac{1}{2}g_2(\Lambda)$,

(b) $\wp(2z) = \frac{1}{4}\left(\frac{\wp''(z)}{\wp'(z)}\right)^2 - 2\wp(z)$.

Aus der Vorlesung ist bekannt, dass $\wp$ und $\wp'$ die elliptische Kurve $E_\Lambda : y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ beschreiben. Entspricht $\wp(z)$ der x-Koordinate von $P \in E$, so entspricht $\wp(2z)$ der x-Koordinate von $2P \in E$. Die Formel in Aufgabenteil (b) beschreibt also die Duplikationsformel auf der elliptischen Kurve in der Beschreibung durch die $\wp$-Funktion. Machen Sie sich den Zusammenhang zu der bereits bekannten Duplikationsformel klar.