Mathematisches Institut
der Universität München
Prof. Dr. O. Forster

WS 2019/20
11. Dez. 2019

Elliptische Funktionen und Elliptische Kurven

Lösung der Aufgabe 27

Aufgabe 27

Sei $\Lambda := \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \subset \mathbb{C}$ ein Gitter ($\omega_1, \omega_2 \in \mathbb{C}$ reell-linear unabhängig).

a) Sei $\Lambda_1 \subset \Lambda$ das Untergitter $\Lambda_1 := 2\mathbb{Z}\omega_1 + 3\mathbb{Z}\omega_2$. Man bestimme eine Basis ω_1', ω_2' von Λ, so dass $\Lambda_1 = \mathbb{Z}\omega_1' + 6\mathbb{Z}\omega_1'$.

b) Sei $\Lambda_2 \subset \Lambda$ das Untergitter $\Lambda_2 := 2\mathbb{Z}\omega_1 + 4\mathbb{Z}\omega_2$. Man zeige: Es gibt keine Basis ω_1', ω_2' von Λ, so dass $\Lambda_2 = \mathbb{Z}\omega_1' + 8\mathbb{Z}\omega_1'$.

Lösungsvorschlag

Wir untersuchen gleich eine etwas allgemeinere Situation:

Sei $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \subset \mathbb{C}$ ein Gitter. O.B.d.A. können wir annehmen, dass die Basis (ω_1, ω_2) positiv orientiert ist. Weiter seien a, b positive ganze Zahlen und $\Lambda_1 \subset \Lambda$ das von $(a\omega_1, b\omega_2)$ aufgespannte Untergitter.

Ist nun (ω_1', ω_2') eine weitere positiv orientierte Basis von Λ, so gibt es eine Matrix $S \in \mathrm{SL}(2, \mathbb{Z})$ mit

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

Es bezeichne $\Lambda_1' = \mathbb{Z}\omega_1' + \mathbb{Z}ab\omega_2'$ das von $(\omega_1', ab\omega_2')$ aufgespannte Untergitter. Genau dann gilt $\Lambda_1 = \Lambda_1'$, wenn eine Matrix $S_2 \in \mathrm{SL}(2, \mathbb{Z})$ existiert, so dass

$$\begin{pmatrix} \omega_1' \\ ab\omega_2' \end{pmatrix} = S_2 \begin{pmatrix} a\omega_1 \\ b\omega_2 \end{pmatrix},$$

d.h.

$$\begin{pmatrix} 1 & 0 \\ 0 & ab \end{pmatrix} S \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = S_2 \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}.$$

Da ω_1, ω_2 reell-linear unabhängig sind, ist dies gleichbedeutend mit

$$\begin{pmatrix} 1 & 0 \\ 0 & ab \end{pmatrix} = S_2 \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} S^{-1}.$$

Wir beweisen nun folgendes Lemma.

---

b.w.

Lemma. *Seien a, b positive ganze Zahlen. Genau dann gibt es Matrizen $S_1, S_2 \in \mathrm{SL}(2,\mathbb{Z})$ mit*

$$\begin{pmatrix} 1 & 0 \\ 0 & ab \end{pmatrix} = S_2 \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} S_1, \qquad (*)$$

wenn a und b teilerfremd sind.

Beweis. a) Sei zunächst vorausgesetzt, dass $\gcd(a,b) = 1$. Dann gibt es $\lambda, \mu \in \mathbb{Z}$ mit

$$\lambda a + \mu b = 1.$$

Es folgt, dass die Matrix

$$S_1 := \begin{pmatrix} \lambda & b \\ -\mu & a \end{pmatrix}$$

die Determinante 1 hat, also in $\mathrm{SL}(2,\mathbb{Z})$ liegt. Man berechnet

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} \lambda & b \\ -\mu & a \end{pmatrix} = \begin{pmatrix} \lambda a & ab \\ -\mu b & ab \end{pmatrix}.$$

Nun multiplizieren wir von links mit $\left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right)$. (Dies entspricht der Subtraktion der zweiten Zeile von der ersten.)

$$\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \lambda a & ab \\ -\mu b & ab \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -\mu b & ab \end{pmatrix}.$$

Jetzt addieren wir das μb-fache der ersten Zeile zur zweiten:

$$\begin{pmatrix} 1 & 0 \\ \mu b & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -\mu b & ab \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & ab \end{pmatrix}.$$

Mit der Definition

$$S_2 := \begin{pmatrix} 1 & 0 \\ \mu b & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ \mu b & 1-\mu b \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ \mu b & \lambda a \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$$

gilt daher

$$S_2 \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} S_1 = \begin{pmatrix} 1 & 0 \\ 0 & ab \end{pmatrix}, \qquad \text{q.e.d.}$$

b) Im Fall, dass $\gcd(a,b) =: d > 1$, ist eine Gleichung $(*)$ unmöglich, denn dann sind alle Koeffizienten der Produkt-Matrix der rechten Seite von $(*)$ durch d teilbar, was im Widerspruch zum Koeffizienten 1 der Matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & ab \end{smallmatrix}\right)$ auf der linken Seite steht.

Anwendung. Für Aufgabe 27a) ist $(a,b) = (2,3)$. Da $2 \cdot 2 - 1 \cdot 3 = 1$, ist mit den Bezeichnungen des Lemmas

$$S_1 = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}, \quad \text{also} \quad S = S_1^{-1} = \begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix}.$$

Mit $\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} := \begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$ gilt daher $2\mathbb{Z}\omega_1 + 3\mathbb{Z}\omega_1 = \mathbb{Z}\omega_1' + 6\mathbb{Z}\omega_2'$.

Teil b) folgt daraus, dass 2 und 4 nicht teilerfremd sind.