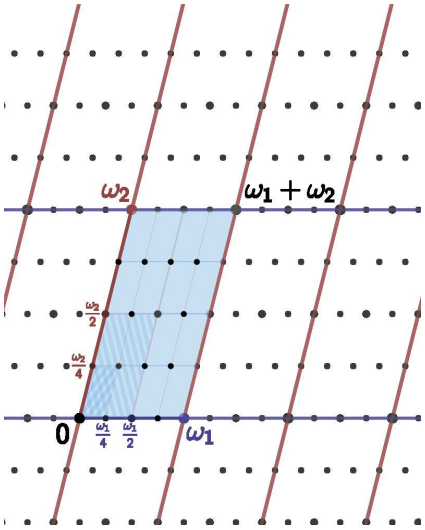
Prof. Dr. H. Brenner **Osnabrück WS 2021/2023**

Elliptische Kurven

Vorlesung 10

Isogenien

Es seien zwei Gitter $\Gamma_1 \subseteq \Gamma_2 \subseteq \mathbb{C}$ gegeben, das eine Gitter sei also in dem anderen Gitter enthalten, d.h. Γ_1 ist ein Untergitter von Γ_2. Beispielsweise ist $\langle 2, 3\mathrm{i}\rangle$ ein Untergitter des Standardgitters $\langle 1, \mathrm{i}\rangle$. Wenn man ein Gitter Γ mit einer positiven natürlichen Zahl n streckt, so erhält man die Untergitterbeziehung $n\Gamma \subseteq \Gamma$. Hierbei sind Γ und $n\Gamma$ zueinander streckungsäquivalent, es kann also durchaus sein, dass ein streckungsäquivalentes Gitter als Untergitter von sich selbst auftritt.



LEMMA 10.1. *Es sei $\Gamma_1 \subseteq \Gamma$ ein Untergitter eines Gitters Γ in $\mathbb{C}$. Dann gibt es $n \in \mathbb{N}_+$ derart, dass $n\Gamma \subseteq \Gamma_1 \subseteq \Gamma$ gilt.*

Beweis. Es sei $\Gamma = \mathbb{Z}u + \mathbb{Z}v$ und $\Gamma_1 = \mathbb{Z}w + \mathbb{Z}z$. Dann gibt es $p, q, r, s \in \mathbb{Z}$ mit $w = pu + qv$ und $z = ru + sv$. Da die Gitter nach Definition volldimensional sind, ist

$$\det \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \pm n \neq 0.$$

Somit gibt es eine weitere Matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ mit

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix}.$$

Mit diesem n gilt die Behauptung. □

LEMMA 10.2. *Zu Gittern $\Gamma_1 \subseteq \Gamma_2 \subseteq \mathbb{C}$ gibt es einen kanonischen surjektiven Gruppenhomomorphismus*

$$\mathbb{C}/\Gamma_1 \longrightarrow \mathbb{C}/\Gamma_2,$$

dessen Kern gleich Γ_2/Γ_1 und insbesondere endlich ist.

Beweis. Unter dem Gruppenhomomorphismus

$$\pi_2 \colon \mathbb{C} \longrightarrow \mathbb{C}/\Gamma_2$$

wird insbesondere auch das Untergitter $\Gamma_1 \subseteq \mathbb{C}$ auf 0 abgebildet, d.h. Γ_1 gehört zum Kern von π_2. Somit gibt es nach dem Homomorphiesatz einen induzierten Gruppenhomomorphismus

$$\mathbb{C}/\Gamma_1 \longrightarrow \mathbb{C}/\Gamma_2.$$

Dieser ist surjektiv, und sein Kern ist isomorph zu Γ_2/Γ_1. Dies ist eine endliche Gruppe. □

LEMMA 10.3. *Zu Gittern $\Gamma_1 \subseteq \Gamma_2 \subseteq \mathbb{C}$ ist der kanonische Gruppenhomomorphismus*

$$\mathbb{C}/\Gamma_1 \longrightarrow \mathbb{C}/\Gamma_2$$

eine Überlagerung, deren Fasern gleich Γ_2/Γ_1 sind. Die Gruppe der Decktransformationen ist isomorph zu Γ_2/Γ_1.

Beweis. Es liegt das kommutative Diagramm

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\pi_1} & \mathbb{C}/\Gamma_1 \\ & \pi_2 \searrow & \downarrow \pi \\ & & \mathbb{C}/\Gamma_2\,, \end{array}$$

wobei π_1 und π_2 nach Satz 8.6 Überlagerungen sind. Zu einer offenen Umgebung $P \in U \subseteq \mathbb{C}/\Gamma_2$, für die es in $\mathbb{C}$ die disjunkten und zu U homöomorphen offenen Umgebungen $g+\tilde{U}$, $g \in \Gamma_2$, gibt, ist das Urbild $\pi^{-1}(U)$ in $\mathbb{C}/\Gamma_1$ die disjunkte Vereinigung der offenen Mengen $\pi_1(g+\tilde{U})$, $[g] \in \Gamma_2/\Gamma_1$, wobei

$$\pi_1(g+\tilde{U}) \longrightarrow U$$

Homöomorphismen sind. Daher liegt eine Überlagerung vor.

Ein Element $[g] \in \Gamma_2/\Gamma_1$ definiert einen stetigen Gruppenhomomorphismus

$$g \colon \mathbb{C}/\Gamma_1 \longrightarrow \mathbb{C}/\Gamma_1,\ z \longmapsto z+g,$$

derart, dass das Diagramm

$$\begin{array}{ccc} \mathbb{C}/\Gamma_1 & \xrightarrow{g} & \mathbb{C}/\Gamma_1 \\ & \pi \searrow & \downarrow \pi \\ & & \mathbb{C}/\Gamma_2 \end{array}$$

kommutiert. Dabei definiert g genau dann die Identität auf $\mathbb{C}/\Gamma_1$, wenn $g \in \Gamma_1$ ist, also wenn $[g] = [0]$ in Γ_2/Γ_1 ist. Die Addition in Γ_2/Γ_1 entspricht dabei der Hintereinanderschaltung von Abbildungen. □

LEMMA 10.4. *Zu Gittern $\Gamma_1 \subseteq \Gamma_2 \subset \mathbb{C}$ ist der kanonische Gruppenhomomorphismus*

$$\mathbb{C}/\Gamma_1 \longrightarrow \mathbb{C}/\Gamma_2$$

ein Homomorphismus von komplexen Lie-Gruppen.

Beweis. Dies folgt aus Lemma 10.2 und aus Lemma 10.3, da die holomorphen Strukturen auf $\mathbb{C}/\Gamma_1$ bzw. $\mathbb{C}/\Gamma_2$ beide von $\mathbb{C}$ geerbt sind (siehe Satz 8.6). □

DEFINITION 10.5. Zu komplexen Tori E_1 und E_2 nennt man einen holomorphen Gruppenhomomorphismus $\varphi\colon E_1 \to E_2$ eine *Isogenie*

Nach Lemma 10.4 ist also zu einem Untergitter $\Gamma_1 \subseteq \Gamma_2$ die induzierte Abbildung $\mathbb{C}/\Gamma_1 \to \mathbb{C}/\Gamma_2$ eine Isogenie.

LEMMA 10.6. *Es sei $\Gamma = \langle u, v\rangle \subseteq \mathbb{C}$ ein Gitter und $n \in \mathbb{N}_+$. Dann führt die Multiplikation mit n zu einem kommutativen Diagramm*

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{n} & \mathbb{C} \\ \downarrow & & \downarrow \\ \mathbb{C}/\Gamma & \xrightarrow{[n]} & \mathbb{C}/\Gamma\ . \end{array}$$

von Gruppenhomomorphismen. Die Abbildung $[n]$ ist eine surjektive Isogenie und der Kern von $[n]$ wird durch die n^2 Elemente

$$\left\{ i\frac{u}{n} + j\frac{v}{n} \mid i, j = 0, 1, \ldots, n-1 \right\}$$

repräsentiert.

Beweis. Es liegt die Untergitterbeziehung $n\Gamma \subseteq \Gamma$ vor, daher folgen die Aussagen aus Lemma 10.4. □

Der folgende Satz charakterisiert die nichtkonstanten Isogenien.

LEMMA 10.7. *Es seien $\Gamma_1, \Gamma_2 \subseteq \mathbb{C}$ Gitter. Dann sind die folgenden Aussagen äquivalent.*

(1) *Es gibt ein $s \in \mathbb{C}^\times$ mit $s\Gamma_1 \subseteq \Gamma_2$.*
(2) *Es gibt einen surjektiven Homomorphismus von komplexen Lie-Gruppen*

$$\varphi\colon \mathbb{C}/\Gamma_1 \longrightarrow \mathbb{C}/\Gamma_2.$$

(3) *Es gibt einen Homomorphismus von komplexen Lie-Gruppen*

$$\varphi\colon\ \mathbb{C}/\Gamma_1 \longrightarrow \mathbb{C}/\Gamma_2$$

mit einem endlichen Kern.

(4) *Es gibt einen nichtkonstanten Homomorphismus von komplexen Lie-Gruppen*

$$\varphi\colon\ \mathbb{C}/\Gamma_1 \longrightarrow \mathbb{C}/\Gamma_2.$$

Beweis. Von (1) nach (2), (3). Nach Satz 10.8 können wir $s\Gamma_1$ durch Γ_1 ersetzen, da dies den Quotienten mit seiner holomorphen Struktur nicht ändert. Die Aussage (2) und (3) folgen somit aus Lemma 10.2 und Lemma 10.4. Aus (2) bzw. (3) folgt direkt (4). Sei also (4) erfüllt. Wir betrachten den zusammengesetzten holomorphen Gruppenhomomorphismus

$$\mathbb{C} \xrightarrow{\pi_1} \mathbb{C}/\Gamma_1 \xrightarrow{\varphi} \mathbb{C}/\Gamma_2\,.$$

Der Kern dieser Abbildung umfasst Γ_1. Nach Lemma 8.15 besitzt diese Gesamtabbildung eine Faktorisierung

$$\mathbb{C} \xrightarrow{\cdot s} \mathbb{C} \xrightarrow{\pi_2} \mathbb{C}/\Gamma_2$$

mit einer komplexen Zahl s. Somit gilt $s \cdot \Gamma_1 \subseteq \Gamma_2$ und wegen der Nichtkonstanz ist $s \neq 0$. □

Satz 10.8. *Es seien $\Gamma_1, \Gamma_2 \subseteq \mathbb{C}$ Gitter. Dann sind Γ_1 und Γ_2 genau dann zueinander streckungsäquivalent, wenn $\mathbb{C}/\Gamma_1$ und $\mathbb{C}/\Gamma_2$ als komplexe Lie-Gruppen isomorph sind.*

Beweis. Die Hinrichtung wurde in Lemma 9.11 gezeigt. Die Rückrichtung folgt aus Lemma 10.7. □

Satz 10.9. *Es seien E_1 und E_2 komplexe Tori über $\mathbb{C}$ und*

$$\varphi\colon\ E_1 \longrightarrow E_2$$

eine nichtkonstante Isogenie. Dann gibt es eine Isogenie

$$\psi\colon\ E_2 \longrightarrow E_1$$

derart, dass $\psi \circ \varphi$ die n-Multiplikation auf E_1 ist.

Beweis. Dies folgt aus Lemma 10.7 und Lemma 10.1. □

Lemma 10.10. *Es seien $E_1 = \mathbb{C}/\Gamma_1$ und $E_2 = \mathbb{C}/\Gamma_2$ komplexe Tori. Dann entsprechen die Isogenien $\varphi\colon E_1 \to E_2$ den komplexen Zahlen $s \in \mathbb{C}$ mit $s\Gamma_1 \subseteq \Gamma_2$.*

Beweis. Dies folgt aus Lemma 10.7. □

Lemma 10.11. *Es seien E_1, E_2, E_3 komplexe Tori. Dann gelten folgende Aussagen*

(1) *Wenn* $\varphi\colon\ E_1 \to E_2$ *und*

$$\psi\colon\ E_2 \longrightarrow E_3$$

Isogenien sind, so ist auch $\psi \circ \varphi$ *eine Isogenie.*

(2) *Wenn*

$$\varphi, \psi\colon\ E_1 \longrightarrow E_2$$

Isogenien sind, so ist auch ihre Summe $\varphi + \psi$ *eine Isogenie.*

Beweis. (1) Ist klar.

(2) Folgt direkt aus dem Diagramm

$$E_1 \xrightarrow{\varphi,\psi} E_2 \times E_2 \xrightarrow{+} E_2\,.$$

□

Definition 10.12. Komplexe Tori E_1, E_2 über $\mathbb{C}$ heißen *isogen*, wenn es eine nichtkonstante Isogenie $E_1 \to E_2$ gibt.

Endomorphismenring

Definition 10.13. Es sei $\Gamma \subseteq \mathbb{C}$ ein Gitter und $E = \mathbb{C}/\Gamma$ der zugehörige komplexe Torus. Man nennt

$$\operatorname{End}(E) = \{f : E \to E \mid f \text{ Isogenie}\}$$

mit der Addition und der Hintereinanderschaltung von Isogenien den *Endomorphismenring* von E.

Lemma 10.14. *Zu einem komplexen Torus ist der Endomorphismenring ein Integritätsbereich.*

Beweis. Bei der Korrespondenz aus Lemma 10.10 zwischen Isogenien und Multiplikationen in $\mathbb{C}$ entsprechen sich auch die Hintereinanderschaltungen und die Summen. Dies gilt insbesondere für $\Gamma' = \Gamma$, so dass sich alles innerhalb von $\mathbb{C}$ abspielt. Es liegt also eine Unterring von $\mathbb{C}$ vor. □

Der Standardfall ist, dass der Endomorphismenring gleich $\mathbb{Z}$ ist und einfach nur aus den Multiplikationen mit ganzen Zahlen im Sinne von Lemma 10.6 besteht. Es gibt aber auch Fälle, wo der Endomorphismenring größer ist. Wenn Γ das definierende Gitter ist, so ist die entscheidende Frage, ob es komplexe Zahlen $s \notin \mathbb{Z}$ gibt mit $s\Gamma \subseteq \Gamma$. Wenn das Gitter in der Form $\mathbb{Z}1+\mathbb{Z}u$ gegeben ist, so muss s selbst zu dem Gitter gehören, also $s = n+mu$, und es muss

$$su = nu + mu^2 \in \Gamma$$

gelten, also $mu^2 \in \Gamma$. D.h. u muss eine quadratische Gleichung über $\mathbb{Z}$ erfüllen. Daher besteht ein enger Zusammenhang zwischen elliptischen Kurven über $\mathbb{C}$ mit „großem“ Endomorphismenring und imaginär-quadratischen Zahlbereichen.

Beispiel 10.15. Zum Gitter $\mathbb{Z} + \mathbb{Z}\mathrm{i}$ gibt es neben den Multiplikationen mit einer ganzen Zahl noch die Multiplikation mit i, die das Gitter in sich selbst überführt. Der Endomorphismenring der elliptischen Kurve $\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\mathrm{i})$ ist $\mathbb{Z}[\mathrm{i}]$.

Beispiel 10.16. Zum Gitter $\Gamma = \mathbb{Z} + \mathbb{Z}\frac{-1+\sqrt{3}\mathrm{i}}{2}$ gibt es neben den Multiplikationen mit einer ganzen Zahl noch die Multiplikation mit $\frac{-1+\sqrt{3}\mathrm{i}}{2}$, die das Gitter in sich selbst überführt. Der Endomorphismenring des komplexen Torus $\mathbb{C}/\Gamma$ ist $\mathbb{Z}[\frac{-1+\sqrt{3}\mathrm{i}}{2}]$.

Abbildungsverzeichnis