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

Elliptische Kurven

Vorlesung 9

Wir fragen uns, für welche Gitter Γ_1, Γ_2 die komplexen Tori $\mathbb{C}/\Gamma_1$ und $\mathbb{C}/\Gamma_2$ isomorph (als komplexe Lie-Gruppen) sind.

Die spezielle lineare Gruppe über $\mathbb{Z}$

Wir betrachten die spezielle lineare Gruppe in der Dimension 2 über $\mathbb{Z}$, also

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in \mathbb{Z},\, ad-bc=1 \right\}.$$

Wir setzen

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

und

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Diese haben die Wirkungsweise

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}$$

und

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix}.$$

Lemma 9.1. *In* $\mathrm{SL}_2(\mathbb{Z})$ *mit*

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

und

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

gelten die Beziehungen

$$S^2 = -\mathrm{Id}$$

und

$$(ST)^3 = -\mathrm{Id}\,.$$

Beweis. Siehe Aufgabe 9.1. □

Satz 9.2. *Die spezielle lineare Gruppe* $\mathrm{SL}_2(\mathbb{Z})$ *wird von den beiden Matrizen* $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ *und* $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ *erzeugt.*

Beweis. Wir beweisen die Aussage, dass jede spezielle lineare Matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ über $\mathbb{Z}$ in der von den beiden Matrizen erzeugten Untergruppe liegt, durch Induktion über $|c|$. Wenn dieser Betrag gleich 0 ist, so ist $a = d = \pm 1$ und durch Multiplikation mit S^2 (siehe Lemma 9.1) können wir annehmen, dass die Diagonalelemente gleich 1 sind. Dann ist die Matrix eine Potenz von T (mit einem eventuell negativen Exponenten). Sei die Aussage nun für alle speziellen linearen Matrizen mit $|c| < n$ bewiesen und sei eine spezielle lineare Matrix mit $|c| = n$ gegeben. Wegen der Präsenz von S können wir annehmen, dass auch a einen Betrag von zumindest n besitzt. Durch Multiplikation mit T oder mit T^{-1} von links kann man dann die erste Spalte $\begin{pmatrix} a \\ c \end{pmatrix}$ durch $\begin{pmatrix} a \pm c \\ c \end{pmatrix}$ ersetzen und erhält, wenn man dies hinreichend oft ausführt, eine erste Spalte $\begin{pmatrix} a' \\ c \end{pmatrix}$ mit $|a'| < n$, worauf wir nach Multiplikation mit S die Induktionsvoraussetzung anwenden können. □

Streckungsäquivalenz und Modulsubstitution

Zu je zwei Gittern $\Gamma_1, \Gamma_2 \subset \mathbb{C}$ sind die Quotienten $\mathbb{C}/\Gamma_1$ und $\mathbb{C}/\Gamma_2$ als topologische Gruppen isomorph, es handelt sich ja um den topologischen Torus $S^1 \times S^1$. Auch als reelle Lie-Gruppen sind sie stets diffeomorph. Als komplexe Mannigfaltigkeiten bzw. als komplexe Liegruppen sind aber $\mathbb{C}/\Gamma_1$ und $\mathbb{C}/\Gamma_2$ in aller Regel verschieden. Dies bedeutet, dass die eine topologische Gruppe $S^1 \times S^1$ unterschiedliche komplexe Strukturen besitzt.

Definition 9.3. Zwei Gitter $\Gamma_1, \Gamma_2 \subset \mathbb{C}$ heißen *streckungsäquivalent*, wenn es eine komplexe Zahl $s \in \mathbb{C}$ mit $\Gamma_2 = s\Gamma_1$ gibt.

Dabei ist natürlich $s \neq 0$, die Streckungsäquivalenz ist eine Äquivalenzrelation. Wenn das eine Gitter Γ_1 durch die reelle Basis u_1, u_2 und das andere Gitter Γ_2 durch v_1, v_2 gegeben ist, so kann man durch Multiplikation mit

$$s = \frac{v_1}{u_1}$$

ein zu Γ_1 streckungsäquivalentes Gitter

$$s\Gamma_1 = \langle v_1, \frac{v_1 u_2}{u_1} \rangle$$

finden, das mit Γ_2 im ersten Erzeuger übereinstimmt. Damit sind die Streckungsmöglichkeiten aufgebraucht. Allerdings kann man aus

$$\frac{v_1 u_2}{u_1} \neq v_2$$

nicht schließen, dass Γ_1 und Γ_2 nicht zueinander streckungsäquivalent sind, da es ja um die Gleichheit von Gittern und nicht um die Gleichheit von

Gitterbasen geht, d.h. man kann noch mit einer Matrix aus $\mathrm{SL}_2(\mathbb{Z})$ multiplizieren.

DEFINITION 9.4. Unter der *oberen Halbebene* in $\mathbb{C}$ versteht man

$$\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}\ (z) > 0\}.$$

LEMMA 9.5. *Jedes Gitter in $\mathbb{C}$ ist streckungsäquivalent zu einem Gitter der Form $\mathbb{Z} + \mathbb{Z}u$ mit $u \in \mathbb{H}$.*

Beweis. Sei $\Gamma = \mathbb{Z}u_1 + \mathbb{Z}u_2$. Da u_1, u_2 eine reelle Basis sind, ist insbesondere $u_1 \neq 0$. Mit $s := u_1^{-1}$ erhält man das streckungsäquivalente Gitter

$$s\Gamma = \langle su_1, su_2\rangle = \langle u_1^{-1}u_1, u_1^{-1}u_2\rangle = \langle 1, u_1^{-1}u_2\rangle.$$

Sei $v = u_1^{-1}u_2$. Diese Zahl ist nicht reell, da andernfalls eine reelle lineare Abhängigkeit zwischen u_1 und u_2 vorliegen würde. Also besitzt v einen imaginären Anteil. Wenn dieser in der unteren Halbebene liegt, so ersetzen wir v durch $-v$ und erhalten eine Basis mit den verlangten Eigenschaften. □

Es bleibt noch zu fragen, wann zwei Gitter, die beide durch eine Basis der Form $(1, u)$ bzw. $(1, v)$ mit $u, v \in \mathbb{H}$ gegeben sind, übereinstimmen.

LEMMA 9.6. *Zwei Gitter der Form $\Gamma_1 = \mathbb{Z}\tau_1 + \mathbb{Z}$ und $\Gamma_2 = \mathbb{Z}\tau_2 + \mathbb{Z}$ mit $\tau_1, \tau_2 \in \mathbb{H}$ sind genau dann streckungsäquivalent, wenn es ein $M \in \mathrm{SL}_2(\mathbb{Z})$ mit*

$$\tau_2 = \frac{a\tau_1 + b}{c\tau_1 + d}$$

gibt.

Beweis. Die Streckungsbedingung zusammen mit der Basisbeschreibung aus Korollar 8.5 führt auf die Bedingung

$$\begin{pmatrix}\tau_2\\1\end{pmatrix} = s\begin{pmatrix}a & b\\c & d\end{pmatrix}\begin{pmatrix}\tau_1\\1\end{pmatrix} = s\begin{pmatrix}a\tau_1 + b\\c\tau_1 + d\end{pmatrix}$$

mit $s \in \mathbb{C}^\times$ und $\begin{pmatrix}a & b\\c & d\end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$. Daher muss

$$s = \frac{1}{c\tau_1 + d}$$

sein und die Bedingung wird zu

$$\tau_2 = \frac{a\tau_1 + b}{c\tau_1 + d}.$$

Es ist

$$\frac{a\tau_1 + b}{c\tau_1 + d} = \frac{(a\tau_1 + b)(c\overline{\tau_1} + d)}{(c\tau_1 + d)(c\overline{\tau_1} + d)}.$$

Der Nenner ist reell und positiv, der Zähler ist

$$\begin{aligned}(a\tau_1 + b)(c\overline{\tau_1} + d) &= ac\tau_1\overline{\tau_1} + bd + ad\tau_1 + bc\overline{\tau_1}\\ &= ac\tau_1\overline{\tau_1} + bd + (bc \pm 1)\tau_1 + bc\overline{\tau_1}\end{aligned}$$

$$= \quad ac\tau_1\overline{\tau_1} + bd + bc(\tau_1 + \overline{\tau_1}) \pm \tau_1.$$

Hierbei sind die drei Summanden links reell. Somit gehört $\frac{a\tau_1+b}{c\tau_1+d}$ genau dann zu $\mathbb{H}$, wenn das Vorzeichen vor τ_1 positiv ist, und dies ist genau dann der Fall, wenn die Matrix die Determinante 1 besitzt. □

Aufgrund von Lemma 9.6 ist es naheliegend, die folgende Wirkungsweise der Gruppe der speziellen ganzzahligen 2×2-Matrizen auf der oberen Halbebene zu betrachten.

Definition 9.7. Die Gruppenoperation der Gruppe $\mathrm{SL}_2(\mathbb{Z})$ auf der oberen Halbebene $\mathbb{H}$ durch

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau := \frac{a\tau + b}{c\tau + d}$$

heißt *Modulsubstitution*.

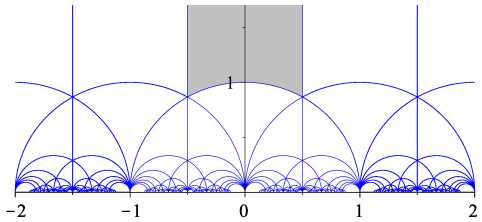
Dass das Ergebnis einer solchen Substitution (man spricht auch von einer speziellen Möbiustransformation) wieder in der oberen Halbebene liegt wurde in Lemma 9.6 mitbewiesen. Die spezielle lineare Gruppe $\mathrm{SL}_2(\mathbb{Z})$ nennt man in diesem Zusammenhang auch *Modulgruppe*. Da die negative Einheitsmatrix $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ als Modulsubstitution trivial operiert, betrachtet man zumeist die Restklassengruppe $\mathrm{SL}_2(\mathbb{Z})/\pm\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ als die Modulgruppe.

Bemerkung 9.8. Die Wirkungsweise der beiden Matrizen $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ und $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, die nach Satz 9.2 die Gruppe der speziellen ganzzahligen Matrizen erzeugen, bei der Modulsubstitution ist

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \tau = -\tau^{-1}$$

und

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \tau = \tau + 1.$$



Der Fundamentalbereich der Gruppenoperation durch Modulsubstitution ist grau. Im Bild ist nicht erkennbar, inwiefern die Randpunkte dazu gehören oder nicht.

LEMMA 9.9. *Es sei*

$$\begin{aligned} D &= \left\{ z \in \mathbb{C} \mid |z| > 1 \text{ und } |\mathrm{Re}\,(z)| < \frac{1}{2} \right\} \\ &\cup \left\{ z \in \mathbb{C} \mid |z| \geq 1 \text{ und } \mathrm{Re}\,(z) = -\frac{1}{2} \right\} \\ &\cup \left\{ z \in \mathbb{C} \mid |z| = 1 \text{ und } -\frac{1}{2} < \mathrm{Re}\,(z) \leq 0 \right\}. \end{aligned}$$

Dann ist D ein Fundamentalbereich für die Modulsubstitution auf der oberen Halbebene.

Beweis. Zu $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ und $\tau = r + s\mathrm{i}$ ist

$$\begin{aligned} g\tau &= \frac{a\tau + b}{c\tau + d} \\ &= \frac{(a\tau + b)(\overline{c\tau + d})}{(c\tau + d)(\overline{c\tau + d})} \\ &= \frac{(a(r + s\mathrm{i}) + b)(c(r - s\mathrm{i}) + d)}{|c\tau + d|^2} \\ &= \frac{(ar + b + as\mathrm{i})(cr + d - cs\mathrm{i}))}{|c\tau + d|^2} \\ &= \frac{(ar + b)(cr + d) + acs^2 + (da - bc)s\mathrm{i}}{|c\tau + d|^2} \\ &= \frac{(ar + b)(cr + d) + acs^2 + s\mathrm{i}}{|c\tau + d|^2}. \end{aligned}$$

Dies bedeutet, dass zwischen den Imaginärteilen die Beziehung

$$\mathrm{Im}\,(g\tau) = \frac{\mathrm{Im}\,(\tau)}{|c\tau + d|^2}$$

besteht. Für $\tau \in H$ folgt daraus ferner, dass die Menge Im $(g\tau)$, $g \in \mathrm{SL}_2(\mathbb{Z})$, ein Maximum besitzt. Sei g entsprechend gewählt. Wir wählen ferner $n \in \mathbb{Z}$ derart, dass der Realteil von

$$\tau' = T^n g\tau$$

zwischen $-\frac{1}{2}$ und $\frac{1}{2}$ liegt, was nach Bemerkung 9.8 möglich ist. Der Betrag von τ' ist ≥ 1, andernfalls würde sich durch $S\tau' = -\frac{1}{\tau'}$ ein Widerspruch zur Wahl von $g\tau$ ergeben. Somit gelangt man in den Abschluss von D. Sei $\tau \in \overline{D}$. Wenn der Realteil von τ gleich $\frac{1}{2}$ ist, so kann man durch Anwendung von T^{-1} erreichen, dass $T^{-1}\tau \in D$ ist. Die Elemente auf dem rechten Kreisteilbogen kann man durch eine Anwendung von S auf den linken Kreisteilbogen schicken. Daher wird jedes Element von H durch ein Element aus D repräsentiert.

Es ist noch zeigen, dass dieses Element eindeutig ist. Nach Satz 9.2 genügt es zu zeigen, dass für $\tau \in D$ und $g \neq \pm \mathrm{Id}$ das Element $g\tau \notin D$ liegt. Sei also $\tau = r + s\mathrm{i} \in D$ und

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Wir nehmen an, dass $g\tau \in D$ gehört und müssen zeigen, dass g die Identität oder das Negative der Identität ist. Da die Rollen von τ und $g\tau$ vertauscht werden können, können wir annehmen, dass

$$\mathrm{Im}\ (g\tau) \geq \mathrm{Im}\ (\tau)$$

gilt. Wie oben gezeigt gilt für den Imaginärteil

$$\mathrm{Im}\ (g\tau) = \frac{\mathrm{Im}\ (\tau)}{|c\tau + d|^2} \geq \mathrm{Im}\ (\tau),$$

also ist

$$|c\tau + d|^2 = c^2r^2 + d^2 + 2crd + c^2s^2 \leq 1.$$

Aus $s \geq \frac{\sqrt{3}}{2}$ folgt $|c| \leq 1$. Sei zunächst $c = 0$. Dann ist $d = a = \pm 1$, wobei wir direkt $= 1$ annehmen können, und es liegt eine Scherung vor, die wegen des Realteiles trivial sein muss. Sei also $c = \pm 1$, wobei wir durch Multiplikation mit $-\mathrm{Id}$ annehmen können, dass $c = 1$ ist. Aus $|\tau + d| \leq 1$ und $\tau \in D$ folgt $d = 0$. Die Determinante ergibt $b = -1$. Dann ist $g\tau = \frac{a\tau - 1}{\tau} = a - \tau^{-1}$. Der Imaginärteil dieser Zahl ist $\frac{s}{r^2+s^2} \leq s$, also muss τ ein Punkt der Sphäre und $a = 0$ sein. Von τ und $-\tau^{-1}$ liegt aber genau ein Element auf dem fixierten Kreissegment. □

Korollar 9.10. *Jedes Gitter in $\mathbb{C}$ ist streckungsäquivalent zu einem Gitter der Form $\mathbb{Z} + \mathbb{Z}\tau$ mit einem eindeutig bestimmten $\tau \in D$, wobei D den Fundamentalbereich zur Modulsubstitution bezeichnet.*

Beweis. Dies folgt aus Lemma 9.5, Lemma 9.6 und Lemma 9.9. □

Lemma 9.11. *Es seien $\Gamma_1, \Gamma_2 \subset \mathbb{C}$ streckungsäquivalente Gitter. Dann sind $\mathbb{C}/\Gamma_1$ und $\mathbb{C}/\Gamma_2$ als komplexe Lie-Gruppen isomorph.*

Beweis. Es seien Γ_1 und Γ_2 streckungsäquivalent mit

$$\Gamma_2 = s\Gamma_1$$

mit $s \in \mathbb{C}$. Wie betrachten die Multiplikation mit s als lineare Abbildung

$$s\colon \mathbb{C} \longrightarrow \mathbb{C}.$$

Dieser Gruppenisomorphismus führt Γ_1 in Γ_2 über. Somit ist Γ_1 der Kern des surjektiven Gruppenhomomorphismus

$$\mathbb{C} \xrightarrow{s} \mathbb{C} \xrightarrow{\pi_2} \mathbb{C}/\Gamma_2\,.$$

Nach Korollar 47.3 (Lineare Algebra (Osnabrück 2017-2018)) induziert dies einen Gruppenisomorphismus

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

Dieser ist stetig und auch (wegen der Kompaktheit oder wegen der Symmetrie der Situation) ein Homöomorphismus. Für einen Punkt $Q \in \mathbb{C}$ und eine hinreichend kleine Ballumgebung $Q \in U(Q,\epsilon) = V$, die Γ_1 nur einfach trifft, ist

$$V \longrightarrow \pi_1(V)$$

eine komplexe Karte für $\mathbb{C}/\Gamma_1$. Dann kommutiert das Diagramm

$$\begin{array}{ccc} V & \stackrel{s}{\longrightarrow} & sV \\ \pi_1 \downarrow & & \downarrow \pi_2 \\ \pi_1(V) & \stackrel{\varphi}{\longrightarrow} & \pi_2(sV) \end{array}$$

und sV ist eine komplexe Karte für $\mathbb{C}/\Gamma_2$. Somit ist φ mit den komplexen Strukturen verträglich, also holomorph. $\square$

Abbildungsverzeichnis