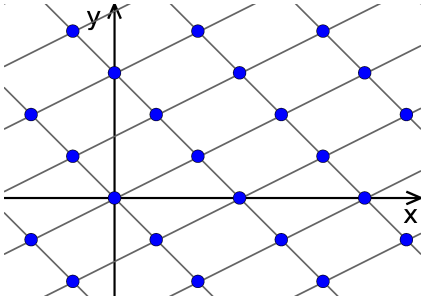
**Prof. Dr. H. Brenner** **Osnabrück WS 2021/2023**

# Elliptische Kurven

## Vorlesung 8

In den nächsten Vorlesungen nähern wir uns den elliptischen Kurven von einem wesentlich verschiedenen Blickwinkel an. Wir betrachten Gitter in $\mathbb{C}$ und die zugehörigen Restklassengruppen. Es ergibt sich schnell, dass diese komplexe eindimensionale Mannigfaltigkeiten mit einer Gruppenstruktur sind. Dass diese aber auch algebraisch realisierbar als elliptische Kurven über $\mathbb{C}$ sind, wird sich erst später zeigen.

### Gitter




DEFINITION 8.1. Es seien $v_1, \ldots, v_n$ linear unabhängige Vektoren im $\mathbb{R}^n$. Dann heißt die Untergruppe $\mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_n$ ein *Gitter* im $\mathbb{R}^n$.

Manchmal spricht man auch von einem vollständigen Gitter, da die Erzeuger eine Basis des Raumes bilden. Als Gruppen sind sie isomorph zu $\mathbb{Z}^n$, hier interessieren aber auch Eigenschafen der Einbettung in $\mathbb{R}^n$. Ein Gitter heißt *rational*, wenn die erzeugenden Vektoren zu $\mathbb{Q}^n$ gehören.

SATZ 8.2. *Zu einem Gitter $\Gamma = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_n \subseteq \mathbb{R}^n$ ist die topologische Restklassengruppe $\mathbb{R}^n/\Gamma$ isomorph zum $n$-dimensionalen Torus $S^1 \times \cdots \times S^1$ (mit $n$ Faktoren).*

*Beweis.* Nach Aufgabe 8.1 können wir davon ausgehen, dass $\Gamma$ das Standardgitter $\mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n$ ist. Für dieses gilt

$$\mathbb{R}^n/(\mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n) = (\mathbb{R}/\mathbb{Z}e_1) \times \cdots \times (\mathbb{R}/\mathbb{Z}e_n) = S^1 \times \cdots \times S^1.$$

□

Topologisch und gruppentheoretisch sind alle vollständigen Gitter zueinander äquivalent. Ein Gitter ist durch seine Basis festgelegt, aber nicht umgekehrt. Man kann aber einfach charakterisieren, ob zwei Basiselemente das gleiche Gitter erzeugen.

LEMMA 8.3. *Es seien $v_1, \ldots, v_n$ und $w_1, \ldots, w_n$ Basen im $\mathbb{R}^n$. Dann stimmen die zugehörigen Gitter $\Gamma = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_n$ und $\Delta = \mathbb{Z}w_1 \oplus \cdots \oplus \mathbb{Z}w_n$ genau dann überein, wenn ihre Übergangsmatrix ganzzahlig mit Determinante $\pm 1$ ist.*

*Beweis.* Es seien $M$ und $N$ die (reellen) Übergangsmatrizen zwischen den beiden Basen, dabei gilt

$$M \circ N = E_n$$

und

$$\det M \cdot \det N = 1$$

nach dem Determinantenmultiplikationsatz. Seien die Gitter gleich. Dann folgt aus $v_j \in \Delta$, dass in

$$v_j = \sum_{i=1}^{n} c_{ij} w_i$$

die Koeffizienten $c_{ij}$ ganzzahlig sind und damit sind die Übergangsmatrizen ganzzahlig. Ihre Determinanten sind somit auch ganzzahlig und aus der Determinantenbedingung folgt, dass die Determinanten 1 oder $-1$ sein müssen, da dies die einzigen Einheiten in $\mathbb{Z}$ sind.

Wenn beide Übergangsmatrizen ganzzahlig sind, so gilt

$$\Gamma \subseteq \Delta \subseteq \Gamma$$

und damit Gleichheit. □

Im Folgenden beschränken wir uns auf den folgenden Spezialfall.

DEFINITION 8.4. Unter einem *Gitter* in den komplexen Zahlen $\mathbb{C}$ versteht man ein vollständiges Gitter $\Gamma = \mathbb{Z}v_1 \oplus \mathbb{Z}v_2 \subset \mathbb{C}$.

KOROLLAR 8.5. *Zwei reell linear unabhängige Paare $(u_1, u_2)$ und $(v_1, v_2)$ vom komplexen Zahlen definieren genau dann das gleiche Gitter, wenn es eine invertierbare Matrix*

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

*mit*

$$\begin{pmatrix} u_1 \\ u_2 \end{pmatrix} = M \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$$

*gibt.*

*Beweis.* Dies ist ein Spezialfall von Lemma 8.3. □

Beispielsweise stimmen die durch $1, \mathrm{i}$ bzw. $1, 2+\mathrm{i}$ erzeugten Gitter überein, es besteht die Beziehung

$$\begin{pmatrix} 1 \\ 2+\mathrm{i} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ \mathrm{i} \end{pmatrix}$$

bzw. umgekehrt

$$\begin{pmatrix} 1 \\ \mathrm{i} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 2+\mathrm{i} \end{pmatrix}.$$

## Komplexe Tori

Satz 8.6. *Zu einem Gitter $\Gamma \subseteq \mathbb{C}$ ist die kanonische Abbildung $\pi\colon \mathbb{C} \to \mathbb{C}/\Gamma$ eine Überlagerung und der Quotientenraum $\mathbb{C}/\Gamma$ ist in natürlicher Weise eine eindimensionale kompakte komplexe Mannigfaltigkeit.*

*Beweis.* Zu jedem Punkt $P \in \mathbb{C}/\Gamma$ und einem Urbild $Q \in \mathbb{C}$ gibt es eine offene Ballumgebung $Q \in U(Q,\epsilon)$, auf der die Einschränkung einen Homöomorphismus

$$\pi\colon U(Q,\epsilon) \longrightarrow V$$

mit einer offenen Umgebung $V$ von $P$ induziert. Man wähle einfach $\epsilon$ kleiner als den minimalen Abstand im Gitter. Damit ist die Abbildung $\pi\colon \mathbb{C} \to \mathbb{C}/\Gamma$ eine Überlagerung mit der Faser $\Gamma$ und man erhält auf $V$ eine komplexe Karte. Zu zwei solchen offenen Mengen $V_1$ und $V_2$ (zu Punkten $P_1, P_2 \in \mathbb{C}/\Gamma$) seien $B_1, B_2 \subseteq \mathbb{C}$ offene Bälle derart, dass die Einschränkungen $\pi_1\colon B_1 \to V_1$ und $\pi_2\colon B_2 \to V_2$ Homöomorphismen sind. Es sei $W = V_1 \cap V_2$ und sei $U_1 \subseteq B_1$ das Urbild von $W$ unter $\pi_1$ und $U_2 \subseteq B_2$ das Urbild von $W$ unter $\pi_2$. Da das Urbild von $W$ unter $\pi$ die disjunkte Vereinigung von zu $W$ homöomorphen Teilmengen ist, die durch eine Translation mit einem Element aus $\Gamma$ ineinander übergehen, ist

$$U_1 = v + U_2$$

mit einem $v \in \Gamma$. Die Abbildung

$$U_1 \longrightarrow U_2,\ z \longmapsto v+z,$$

beschreibt dann den Kartenwechsel, was zeigt, dass durch diese Karten eine wohldefinierte komplexe Struktur vorliegt.

Die Kompaktheit folgt aus Satz 8.2 oder daraus, dass eine Gittermasche ganz in einer beschränkten und abgeschlossenen, also kompakten Teilmenge von $\mathbb{C}$ liegt und dass Bilder kompakter Mengen unter stetigen Abbildungen kompakt sind. □

Definition 8.7. Eine komplexe Mannigfaltigkeit $M$, die zugleich eine Gruppe ist, für die die Gruppenverknüpfung

$$\circ\colon M \times M \longrightarrow M,\ (x,y) \longmapsto x \circ y,$$

und die Inversenbildung

$$M \longrightarrow M,\, x \longmapsto x^{-1},$$

holomorph sind, heißt *komplexe Lie-Gruppe*.

Satz 8.8. *Zu einem Gitter $\Gamma \subset \mathbb{C}$ ist der Quotientenraum $\mathbb{C}/\Gamma$ in natürlicher Weise eine eindimensionale kompakte kommutative komplexe Lie-Gruppe.*

*Beweis.* Da $\Gamma \subset \mathbb{C}$ eine Untergruppe ist, ist die Restklassengruppe $\mathbb{C}/\Gamma$ eine kommutative Gruppe. Nach Satz 8.6 ist $\mathbb{C}/\Gamma$ auch eine kompakte komplexe Mannigfaltigkeit. Es ist also noch zu zeigen, dass die Gruppenaddition auf $\mathbb{C}/\Gamma$ und das Negative holomorphe Abbildungen sind. Dies ergibt sich aber im Wesentlichen aus den kommutativen Diagrammen

$$\begin{array}{ccc} \mathbb{C} \times \mathbb{C} & \stackrel{+}{\longrightarrow} & \mathbb{C} \\ \pi \times \pi \downarrow & & \downarrow \pi \\ \mathbb{C}/\Gamma \times \mathbb{C}/\Gamma & \stackrel{+}{\longrightarrow} & \mathbb{C}/\Gamma \end{array}$$

und

$$\begin{array}{ccc} \mathbb{C} & \stackrel{-}{\longrightarrow} & \mathbb{C} \\ \pi \downarrow & & \downarrow \pi \\ \mathbb{C}/\Gamma & \stackrel{-}{\longrightarrow} & \mathbb{C}/\Gamma\,. \end{array}$$

□

Definition 8.9. Unter einem *komplexen Torus* versteht man den Quotientenraum $\mathbb{C}/\Gamma$ zu einem Gitter $\Gamma \subseteq \mathbb{C}$.

Statt von einem (eindimensionalen) komplexen Torus spricht man auch von einer komplex-elliptischen Kurve, dies vor allem aber dann, wenn man den Torus als glatte kubische Kurve in der projektiven Ebene realisiert hat, siehe Satz 12.14.

Bemerkung 8.10. Ein komplexer Torus (eine elliptische Kurve über $\mathbb{C}$) ist durch eine Vielzahl an Strukturen ausgezeichnet, die sich teilweise gegenseitig bedingen. Nach Satz 8.6 handelt es sich um eine eindimensionale komplexe Mannigfaltigkeit, also eine riemannsche Fläche. Damit ist sie insbesondere eine zweidimensionale reelle Mannigfaltigkeit. Ihre topologische Gestalt ist schon in Satz 8.2 beschrieben worden, es handelt sich um einen Torus, ein Produkt der 1-Sphäre $S^1$ mit sich selbst, also $S^1 \times S^1$. Insbesondere ist ein komplexer Torus kompakt. Ferner ist ein komplexer Torus nach Satz 8.8 eine komplexe Lie-Gruppe, es gibt eine Addition auf ihr, die sie zu einer kommutativen Gruppe macht, bei der die Addition und die Negation holomorph sind. Die Abbildung

$$\mathbb{C} \longrightarrow \mathbb{C}/\Gamma$$

ist holomorph und ein Gruppenhomomorphismus, genauer ein Homomomorphismus von komplexen eindimensionalen Lie-Gruppen. Als topologische

Gruppe bzw. als reelle Lie-Gruppe handelt es sich einfach um das Produkt der Kreisgruppe mit sich selbst. Die reelle Mannigfaltigkeitsstruktur und die Struktur als reelle Lie-Gruppe ist also für jeden komplexen Torus gleich. Dagegen hängen die Eigenschaften eines komplexen Torus als komplexe Mannigfaltigkeit bzw. als komplexe Lie-Gruppe wesentlich vom Gitter ab. Es gibt eine Vielzahl von unterschiedlichen komplexen Tori. Man kann auch so sagen, dass es auf der einen reellen Mannigfaltigkeit $S^1 \times S^1$ eine Vielzahl an komplexen Strukturen gibt.

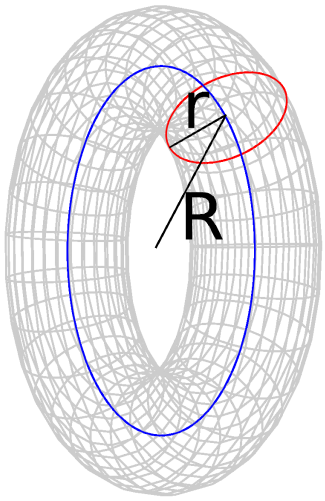
## Liftungen

SATZ 8.11. *Zu einem Gitter $\Gamma \subseteq \mathbb{C}$ ist die Quotientenabbildung*

$$\pi \colon \mathbb{C} \longrightarrow \mathbb{C}/\Gamma$$

*die universelle Überlagerung des komplexen Torus $\mathbb{C}/\Gamma$.*

*Beweis.* Dass eine Überlagerung vorliegt, wurde schon in Satz 8.6 mitbewiesen. Da $\mathbb{C} = \mathbb{R}^2$ einfach zusammenhängend ist, handelt es sich um die universelle Überlagerung. □




Die beiden bunten Kreise zeigen die Erzeuger der Fundamentalgruppe.

KOROLLAR 8.12. *Die Fundamentalgruppe eines komplexen Torus ist $\mathbb{Z} \times \mathbb{Z}$.*

*Beweis.* Dies folgt aus Satz 8.11 und Satz 17.4 (Topologie (Osnabrück 2008-2009)). □

LEMMA 8.13. *Es sei* $\Gamma \subseteq \mathbb{C}$ *ein Gitter mit der Quotientenabbildung* $\pi\colon \mathbb{C} \to \mathbb{C}/\Gamma$ *und sei* $\varphi\colon \mathbb{C} \to \mathbb{C}/\Gamma$ *ein stetiger Gruppenhomomorphismus. Dann gibt es einen eindeutig bestimmten stetigen Gruppenhomomorphismus*

$$\tilde{\varphi}\colon \mathbb{C} \longrightarrow \mathbb{C}$$

*mit* $\varphi = \pi \circ \tilde{\varphi}$.

*Beweis.* Da $\pi\colon \mathbb{C} \to \mathbb{C}/\Gamma$ die universelle Überlagerung und $\mathbb{C}$ einfach zusammenhängend ist, gibt es nach Satz 15.3 (Topologie (Osnabrück 2008-2009)) eine eindeutig bestimmte stetige Liftung $\tilde{\varphi}\colon \mathbb{C} \to \mathbb{C}$ mit $\varphi = \pi \circ \tilde{\varphi}$ und $\tilde{\varphi}(0) = 0$. Wir betrachten die stetige Abbildung

$$\Psi\colon \mathbb{R}^2 \times \mathbb{R}^2 \longrightarrow \mathbb{R}^2,\ (P,Q) \longmapsto \tilde{\varphi}(P+Q) - \tilde{\varphi}(P) - \tilde{\varphi}(Q),$$

die für $(0,0)$ den Wert 0 besitzt. Es ist

$$\begin{aligned} \pi(\tilde{\varphi}(P+Q) - \tilde{\varphi}(P) - \tilde{\varphi}(Q)) &= \pi(\tilde{\varphi}(P+Q)) - \pi(\tilde{\varphi}(P)) - \pi(\tilde{\varphi}(Q)) \\ &= \varphi(P+Q) - \varphi(P) - \varphi(Q) \\ &= [0], \end{aligned}$$

da ja $\varphi$ ein Gruppenhomomorphismus ist. Somit ist $\tilde{\varphi}(P+Q) - \tilde{\varphi}(P) - \tilde{\varphi}(Q) \in \Gamma$ für alle $(P,Q)$. Da $\Psi$ stetig und $\Gamma$ diskret ist, ist $\Psi$ konstant gleich 0. Also ist $\tilde{\varphi}$ ein Gruppenhomomorphismus. □

KOROLLAR 8.14. *Es sei* $\Gamma \subseteq \mathbb{C}$ *ein Gitter mit der Quotientenabbildung* $\pi\colon \mathbb{C} \to \mathbb{C}/\Gamma$ *und sei* $\varphi\colon \mathbb{C} \to \mathbb{C}/\Gamma$ *ein stetiger Gruppenhomomorphismus. Dann gibt es eine eindeutig bestimmte* $\mathbb{R}$*-lineare Abbildung*

$$\tilde{\varphi}\colon \mathbb{C} \longrightarrow \mathbb{C}$$

*mit* $\varphi = \pi \circ \tilde{\varphi}$.

*Beweis.* Dies folgt aus Lemma 8.13 und aus Aufgabe 8.18. □

LEMMA 8.15. *Es sei* $\Gamma \subseteq \mathbb{C}$ *ein Gitter mit der Quotientenabbildung* $\pi\colon \mathbb{C} \to \mathbb{C}/\Gamma$ *und sei* $\varphi\colon \mathbb{C} \to \mathbb{C}/\Gamma$ *ein holomorpher Gruppenhomomorphismus. Dann gibt es ein* $s \in \mathbb{C}$ *mit* $\varphi = \pi \circ \mu_s$, *wobei* $\mu_s$ *die Multiplikation mit* $s$ *bezeichnet.*

*Beweis.* Nach Korollar 8.14 ist die eindeutig bestimmte Liftung $\tilde{\varphi}\colon \mathbb{C} \to \mathbb{C}$ zu $\varphi$ mit $\tilde{\varphi}(0) = 0$ bereits $\mathbb{R}$-linear. Als Liftung zu einer holomorphen Abbildung ist sie selbst holomorph, also die Multiplikation mit einer komplexen Zahl $s$. □

# Abbildungsverzeichnis