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

Elliptische Kurven

Vorlesung 11

Wir möchten zeigen, dass sich ein eindimensionaler komplexer Torus $\mathbb{C}/\Gamma$ zu einem Gitter $\Gamma \subseteq \mathbb{C}$ als eine glatte kubische projektive Kurve algebraisch realisieren lässt. Dazu müssen wir meromorphe Funktionen auf $\mathbb{C}/\Gamma$ studieren, die wiederum von meromorphen Funktionen auf $\mathbb{C}$ herrühren, die das Gitter berücksichtigen.

Elliptische Funktionen

Definition 11.1. Es sei $\Gamma \subseteq \mathbb{C}$ ein Gitter. Eine meromorphe Funktion

$$f\colon \mathbb{C} \longrightarrow \mathbb{C}$$

heißt *elliptisch* bezüglich Γ oder Γ- *doppeltperiodisch* , wenn

$$f(z) = f(z+v)$$

für alle $v \in \Gamma$ gilt.

Es genügt natürlich zu zeigen, dass

$$f(z) = f(z+v_1) = f(z+v_2)$$

für zwei Erzeuger v_1, v_2 des Gitters (und alle z) gilt. Diese Erzeuger sind die Perioden, die die Bezeichnung doppeltperiodisch rechtfertigen. Diese Eigenschaft hängt wesentlich von dem gegebenen Gitter ab, es stellt sich aber bald heraus, dass die doppeltperiodischen Funktionen strukturelle Eigenschaften erfüllen, die für alle Gitter gleich sind. Eine doppeltperiodische Funktion ist auf einem Fundamentalbereich des Gitters, beispielsweise einer Fundamentalmasche, eindeutig bestimmt.

Definition 11.2. Es sei $\Gamma \subseteq \mathbb{C}$ ein Gitter. Die Menge aller elliptischen Funktionen bezüglich Γ mit der natürlichen Addition und Multiplikation nennt man den *Körper der elliptischen Funktionen*.

Es ist einfach zu zeigen (vergleiche Aufgabe 11.1 und Aufgabe 11.2), dass dies in der Tat ein Körper ist. Es ist deutlich schwieriger, die Menge der elliptischen Funktionen explizit zu bestimmen. Zunächst ist keineswegs klar, dass es außer den konstanten Funktionen überhaupt elliptische Funktionen gibt.

Lemma 11.3. *Es sei $\Gamma \subseteq \mathbb{C}$ ein Gitter. Dann ist jede Γ-elliptische Funktion, die holomorph ist, konstant.*

Beweis. Es sei $\mathfrak{M}$ eine Grundmasche des Gitters. Diese ist kompakt und die holomorph Funktion f ist darauf nach Satz Anhang B.12 (Lineare Algebra (Osnabrück 2017-2018)) und Satz 81.11 (Analysis (Osnabrück 2021-2023)) beschränkt. Da f elliptisch ist, ist $f(z) = f(z-v)$ mit $v \in \Gamma$ und $z-v \in \mathfrak{M}$. Daher ist f auf ganz $\mathbb{C}$ beschränkt und daher nach dem Satz von Liouville konstant. □

Wir beweisen drei fundamentale Lemmas über elliptische Funktionen, aus denen später die Charakterisierung aller elliptischen Funktionen (siehe insbesondere Lemma 11.12 und Satz 12.11) und die algebraische Realisierung eines komplexen Torus (siehe Satz 12.14) folgt.

LEMMA 11.4. *Es sei $\Gamma \subseteq \mathbb{C}$ ein Gitter mit der Grundmasche $\mathfrak{M}$ und es sei f eine elliptische Funktion. Es sei $P \in \mathbb{C}$ derart, dass f auf dem Rand von $P+\mathfrak{M}$ polstellenfrei ist. Dann ist die Summe der Residuen von f auf $P+\mathfrak{M}$ gleich* 0.

Beweis. Es sei $\Gamma = \langle v_1, v_2 \rangle$. Es sei γ ein Weg, der den Rand von $P+\mathfrak{M}$ einfach gegen den Uhrzeigersinn durchläuft. Dann ist nach einem Satz (Funktionentheorie) die Summe der Residuen gleich $\frac{1}{2\pi \mathrm{i}} \int_\gamma f(z)dz$. Der Weg γ besteht aus den vier linearen Teilwegen von P nach $P+v_1$, von $P+v_1$ nach $P+v_1+v_2$, von $P+v_1+v_2$ nach $P+v_2$ und von $P+v_2$ nach P. Da f elliptisch ist, ist insbesondere $f(P+tv_1) = f(P+tv_1+v_2)$ und $f(P+v_1+sv_2) = f(P+sv_2)$. D.h. die Integranden auf den gegenüberliegenden Teilwegen stimmen überein. Da sie unterschiedlich orientiert durchlaufen werden, ist das Gesamtergebnis gleich 0. □

LEMMA 11.5. *Es sei $\Gamma \subseteq \mathbb{C}$ ein Gitter mit der Grundmasche $\mathfrak{M}$ und es sei $f \neq 0$ eine elliptische Funktion. Es sei $P \in \mathbb{C}$ derart, dass f auf dem Rand von $P+\mathfrak{M}$ weder eine Nullstelle noch einen Pol besitzt. Dann ist die Summe der Ordnungen von f auf $P+\mathfrak{M}$ gleich* 0.

Beweis. Dies folgt aus Lemma 11.4 angewendet auf die elliptische Funktion $\frac{f'}{f}$ unter Verwendung von einem Satz (Funktionentheorie). □

LEMMA 11.6. *Es sei $\Gamma \subseteq \mathbb{C}$ ein Gitter mit der Grundmasche $\mathfrak{M}$ und es sei $f \neq 0$ eine elliptische Funktion. Es sei $P \in \mathbb{C}$ derart, dass f auf dem Rand von $P+\mathfrak{M}$ weder eine Nullstelle noch einen Pol besitzt. Dann ist*

$$\sum_{w \in P+\mathfrak{M}} \operatorname{ord}_w(f) \cdot w \in \Gamma$$

Beweis. Es sei $\Gamma = \langle v_1, v_2 \rangle$. Es sei γ die einfach gegen den Uhrzeigersinn durchlaufene Umrandung von $P+\mathfrak{M}$ mit den linearen Teilwegen wie im Beweis zu Lemma 11.4. Wir betrachten die Funktion $\frac{zf'(z)}{f(z)}$ auf $P+\mathfrak{M}$. Nach einem Satz der Funktionentheorie und dem Residuensatz ist

$$\sum_{w \in P+\mathfrak{M}} \operatorname{ord}_w(f) \cdot w$$

$$\begin{aligned} &= \sum_{w\in P+\mathfrak{M}} \mathrm{Res}_w\left(\frac{zf'(z)}{f(z)}\right) \\ &= \frac{1}{2\pi\mathrm{i}}\int_\gamma \frac{zf'(z)}{f(z)}dz \\ &= \frac{1}{2\pi\mathrm{i}}\Big(\int_P^{P+v_1}\frac{zf'(z)}{f(z)}dz+\int_{P+v_1}^{P+v_1+v_2}\frac{zf'(z)}{f(z)}dz+\int_{P+v_1+v_2}^{P+v_2}\frac{zf'(z)}{f(z)}dz+\int_{P+v_2}^{P}\frac{zf'(z)}{f(z)}dz\Big). \end{aligned}$$

Wir verarbeiten das zweite und das vierte Integral, indem wir auf das zweite Integral die lineare Substitution $z\mapsto z+v_1$ anwenden. Dabei erhalten wir unter Verwendung der Periodizität und der Umkehrung des Weges

$$\begin{aligned} \int_{P+v_1}^{P+v_1+v_2}\frac{zf'(z)}{f(z)}dz+\int_{P+v_2}^{P}\frac{zf'(z)}{f(z)}dz &= \int_P^{P+v_2}\frac{(z+v_1)f'(z+v_1)}{f(z+v_1)}dz+\int_{P+v_2}^{P}\frac{zf'(z)}{f(z)}dz \\ &= \int_P^{P+v_2}\frac{(z+v_1)f'(z)}{f(z)}dz-\int_P^{P+v_2}\frac{zf'(z)}{f(z)}dz \\ &= v_1\int_P^{P+v_2}\frac{f'(z)}{f(z)}dz. \end{aligned}$$

Entsprechend ergibt das erste und das dritte Integral $-v_2\int_P^{P+v_1}\frac{f'(z)}{f(z)}dz$. Nach einem weiteren Satz aus der Funktionentheorie ist $\frac{1}{2\pi\mathrm{i}}\int_P^{P+v_1}\frac{f'(z)}{f(z)}dz$ ganzzahlig. Daher ist $\sum_{w\in P+\mathfrak{M}}\mathrm{ord}_w(f)\cdot w$ eine ganzzahlige Kombination von v_1 und v_2, gehört also zum Gitter. □

Die Weierstraßfunktion

Wir setzen $\Gamma' = \Gamma\setminus\{0\}$.

Lemma 11.7. *Es sei $\Gamma\subseteq\mathbb{C}$ ein Gitter und sei $s>2$ eine reelle Zahl. Dann ist die Familie*

$$v^{-s},\ v\in\Gamma'$$

summierbar.

Beweis. Die Familie ist genau dann summierbar, wenn die Familie $|v|^{-s}$ summierbar ist. Die Aussage kann man auf das Standardgitter zurückführen. Wir betrachten zu $n\in\mathbb{N}_+$ die endlichen Teilfamilien (Quadrat mit Seitenlänge $2n$)

$$\sum_{\max(|a|,|b|)=n}|a+b\mathrm{i}|^{-s}\ .$$

Diese besteht aus

$$2(2n+1)+2(2n-1)\ =\ 8n$$

Summanden und diese sind $\leq n^{-s}$. Die Summe a_n dieser Teilfamilie ist also

$$\leq\ 8n\cdot n^{-s}\ =\ 8n^{1-s},$$

wobei der Exponent <-1 ist. Die Summe $\sum_{n\in\mathbb{N}_+}a_n$ existiert also und daher ist nach dem großen Umordnungssatz die Ausgangsfamilie summierbar. □

LEMMA 11.8. *Es sei $\Gamma \subseteq \mathbb{C}$ ein Gitter. Dann ist die meromorphe Funktion*

$$f(z) = \sum_{v\in\Gamma}(z-v)^{-3}$$

elliptisch und besitzt genau in den Gitterpunkten einen Pol der Ordnung -3.

Beweis. Die Konvergenz für $z \notin \Gamma$ folgt aus Lemma 11.7 durch eine geeignete Abschätzung. Daraus folgt auch die Holomorphie auf $\mathbb{C} \setminus \Gamma$. In $z_0 \in \Gamma$ ist $\sum_{v\in\Gamma,\, v\neq z_0}(z-v)^{-3}$ konvergent und die Polordnung ist durch den fehlenden Term $(z-z_0)^{-3}$ festgelegt. Die Funktion $\sum_{v\in\Gamma}(z-v)^{-3}$ ist elliptisch, da sich die Summe nicht ändert, wenn man z durch $z-v_0$ mit einem $v_0 \in \Gamma$ ersetzt. □

DEFINITION 11.9. Es sei $\Gamma \subseteq \mathbb{C}$ ein Gitter. Man nennt die meromorphe Funktion

$$\wp\colon \mathbb{C}\setminus\Gamma \longrightarrow \mathbb{C},\, z \longmapsto \frac{1}{z^2} + \sum_{v\in\Gamma'}\left(\frac{1}{(z-v)^2} - \frac{1}{v^2}\right),$$

die *Weierstraßsche $\wp$- Funktion* zum Gitter Γ.

Wir werden gleich begründen, dass diese Funktion auf $\mathbb{C}\setminus\Gamma$ holomorph und in Γ meromorph ist.

LEMMA 11.10. *Es sei $\Gamma \subseteq \mathbb{C}$ ein Gitter. Dann ist die Weierstraßsche $\wp$-Funktion $\wp$ elliptisch. Sie besitzt genau in den Gitterpunkten einen Pol der Ordnung -2. Ihre Ableitung ist $\wp'(z) = -2\sum_{v\in\Gamma}(z-v)^{-3}$.*

Beweis. Die Ableitung der Summanden $\frac{1}{(z-v)^2} - \frac{1}{v^2}$ für $v \in \Gamma'$ ist $-2\frac{1}{(z-v)^3}$. Ferner ist $-2\frac{1}{z^3}$ die Ableitung des allerersten Summanden. Die summandenweise genommene Ableitung ist also bis auf den Faktor -2 die Funktion $\sum_{v\in\Gamma}(z-v)^{-3}$, die nach Lemma 11.8 elliptisch ist. Damit ist $\wp(z)$ meromorph mit der angegebenen Poleigenschaft. Ferner ist die Funktion gerade, da ihre Ableitung ungerade ist. Zum Nachweis, dass $\wp(z)$ selbst elliptisch ist, sei v_0 ein Erzeuger des Gitters, und insbesondere $v_0/2 \notin \Gamma$. Dann ist

$$\frac{\partial(\wp(z+v_0)-\wp(z))}{\partial z} = -2\left(\sum_{v\in\Gamma}(z+v_0-v)^{-3} - \sum_{v\in\Gamma}(z-v)^{-3}\right) = 0$$

und $\wp(z+v_0)-\wp(z)$ ist konstant. Für $z = -\frac{v_0}{2}$ ist der Wert dieser Funktion gleich

$$\wp(-\frac{v_0}{2}+v_0) - \wp(-\frac{v_0}{2}) = \wp(\frac{v_0}{2}) - \wp(-\frac{v_0}{2}) = \wp(\frac{v_0}{2}) - \wp(\frac{v_0}{2}) = 0.$$

□

LEMMA 11.11. *Es sei $\Gamma \subseteq \mathbb{C}$ ein Gitter. Dann nimmt die Weierstraßsche $\wp$-Funktion zu Γ jeden Wert auf der halboffenen Grundmasche (mit Vielfachheit gezählt) zweifach an.*

Beweis. Es sei $w \in \mathbb{C}$, wir betrachten die Funktion $\wp(z) - w$, es geht um die Nullstellen dieser Funktion. Da es auf einer verschobenenen kompakten Masche

$$\mathfrak{N} = P + \mathfrak{M}$$

nur endlich viele Nullstellen gibt, kann man P so wählen, dass es auf den Rand weder eine Nullstelle noch einen Pol gibt. Es gibt dann in $\mathfrak{N}$ nach Lemma 11.10 genau eine Polstelle mit der Ordnung -2. Nach Lemma 11.5 muss es zwei Nullstellen mit Ordnung 1 oder eine Nullstelle mit der Ordnung 2 geben. □

LEMMA 11.12. *Es sei $\Gamma \subseteq \mathbb{C}$ ein Gitter. Dann wird der Körper der elliptischen Funktionen von $\wp$ und $\wp'$ erzeugt, d.h. jede elliptische Funktion kann man als eine rationale Funktion in $\wp$ und $\wp'$ schreiben.*

Beweis. Jede elliptische Funktion kann man als eine Summe einer geraden und einer ungeraden elliptischen Funktion schreiben, siehe Aufgabe 11.4. Eine ungerade elliptische Funktion kann man mit $\wp'$ multiplizieren und erhält eine gerade elliptische Funktion. Es genügt also zu zeigen, dass jede gerade elliptische Funktion eine rationale Funktion in $\wp$ ist.

Sei f eine gerade elliptische Funktion. Die Ordnung von f in einem Punkt w stimmt mit der Ordnung von f in $-w$ überein. Wenn dabei $w = -w \bmod \Gamma$ ist, also $2w \in \Gamma$, so ist die Ordnung in einem solchen Punkt gerade. Es sei $\Gamma = \langle u, v \rangle$, $\mathfrak{M} = \{ru + sv \mid 0 \leq r, s < 1\}$ die zugehörige Fundamentalmasche und $\mathfrak{N} = \left\{ru + sv \mid 0 \leq r < 1, 0 \leq s < \frac{1}{2}\right\}$. Es seien $w_1, \ldots, w_n$ die Punkte $\neq 0$ in $\mathfrak{N}$, in denen eine Pol- oder eine Nullstelle vorliegt. Aus diesen Ordnungen basteln wir die elliptische Funktion

$$g(z) = \prod_i (\wp(z) - \wp(w_i))^{r_i},$$

wobei r_i die Ordnungen sind. Diese Funktion besitzt überall außer eventuell im Nullpunkt die gleichen Ordnungen wie f. Aus Lemma 11.5 folgt dann, dass auch im Nullpunkt die Ordnungen gleich sind. Daher ist $\frac{f}{g}$ holomorph und somit nach Lemma 11.3 konstant. Daher ist $f \in \mathbb{C}(\wp)$, da g nach Konstruktion dazugehört. □

Abbildungsverzeichnis

Erläuterung: Die in diesem Text verwendeten Bilder stammen aus Commons (also von http://commons.wikimedia.org) und haben eine Lizenz, die die Verwendung hier erlaubt. Die Bilder werden mit ihren Dateinamen auf Commons angeführt zusammen mit ihrem Autor bzw. Hochlader und der Lizenz. 7

Lizenzerklärung: Diese Seite wurde von Holger Brenner alias Bocardodarapti auf der deutschsprachigen Wikiversity erstellt und unter die Lizenz CC-by-sa 3.0 gestellt. 7