

Tori sind elliptische Kurven

Nico Köslich

8. und 15. Juli 2025

Abstract

1 Doppeltperiodische Funktionen

Definition 1.1 Seien $\omega_1, \omega_2 \in \mathbb{C}$ linear unabhängig über $\mathbb{R}$. Also $\frac{\omega_1}{\omega_2} \notin \mathbb{R}$. Dann nennen wir

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \{n_1\omega_1 + n_2\omega_2 \mid n_1, n_2 \in \mathbb{Z}\}$$

ein **Gitter**.

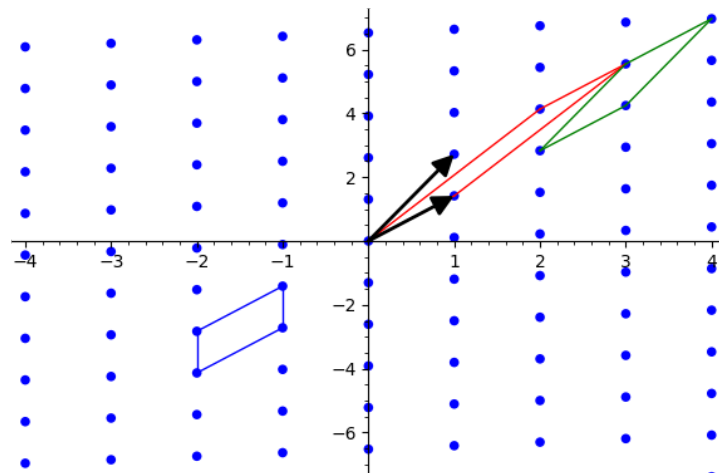
Wie kann man nun so ein Gitter handlich beschreiben? Anschaulich gesprochen sieht man sich jetzt eine Kachel genauer an, diese Idee bringt uns zu folgender Definition:

Definition 1.2 Als **Fundamentalparallelogramm** bezeichnet man die folgende Menge:

$$F = \{a_1\omega_1 + a_2\omega_2 \mid 0 < a_i < 1, i = 1, 2\}$$

Wenn man sich das Gitter in der komplexen Zahlenebene vorstellt, liefert diese Menge genau eine Kachel, welche natürlich von den ω_i 's abhängt.

Natürlich ist ein Fundamentalparallelogramm nicht eindeutig. Es hängt von der Basiswahl ab. Siehe unten, die schwarzen Pfeile sind die Basis zu dem blauen Fundamentalparallelogramm. Das grüne und das rote Viereck sind ebenfalls Fundamentalparallelogramme.



Das Gitter wird erzeugt von $\omega_1 = 1 + \sqrt{2}i$ und $\omega_2 = 1 + ei$. Gitter interessieren uns insbesondere deshalb, weil uns $\mathbb{C}/\Lambda$ einen Torus liefert.

Definition 1.3 Eine **doppelt periodische Funktion** ist eine meromorphe Funktion

$$f : \mathbb{C} \rightarrow \mathbb{C} \cup \infty$$

so dass $f(z + \omega) = f(z)$, für alle $z \in \mathbb{C}$ und alle $\omega \in \Lambda$. Für die Menge der doppeltperiodischen Funktionen schreiben wir $\mathbb{C}(\Lambda)$.

Für die folgenden Eigenschaften erinnern wir uns an die folgenden funktionentheoretischen Grundlagen:

- Bemerkung 1.4**
1. Eine meromorphe Funktion ist eine komplexe Funktion welche auf $\mathbb{C} \setminus D$ mit D diskreter Punktmenge holomorph ist. D besteht aus den Polstellen von f .
 2. Die Laurent-Entwicklung einer meromorphen Funktion ist die Potenzreihenentwicklung in einem kreisförmigen Gebiet um die Polstellen.

3. das Residuum einer Polstelle ist der -1. Term der Laurent-Reihe

Satz 1.5 Sei $f \in \mathbb{C}(\Lambda)$ holomorph, also ohne Polstellen, dann ist f konstant.

Beweis: f ist holomorph, also insbesondere stetig. Es genügt, f auf dem Fundamentalparallelogramm zu betrachten; dieses ist kompakt. Mit den zwei Aussagen folgt, dass f beschränkt ist. Wendet man nun den Satz von Liouville an, folgt die Aussage. $\square$

Satz 1.6 Sei $f \in \mathbb{C}(\Lambda)$, dann gilt:

a)

$$\sum_{\omega \in \mathbb{C}/\Lambda} \text{Res}_{\omega}(f) = 0$$

b)

$$\sum_{\omega \in \mathbb{C}/\Lambda} \text{Ord}_{\omega}(f) = 0$$

c)

$$\sum_{\omega \in \mathbb{C}/\Lambda} \text{Ord}_{\omega}(f) \omega \in \Lambda.$$

Hierbei bezeichnet $\mathbb{C}/\Lambda$ eine Summe von $\omega \in D$ mit D als Fundamentalparallelogramm von Λ .

Beweis: ad a): Vom Residuensatz erhalten wir:

$$\sum_{\omega \in \mathbb{C}/\Lambda} \text{res}_{\omega} f = \frac{1}{2\pi i} \int_{\partial D} f(z) dz$$

Mit der Periodizität von f folgern wir, dass sich gegenüberliegende Seiten des Fundamentalparallelograms im Integral aufheben.

ad b): Aus der Periodizität von f folgt auch die von f' . Also wenden wir die Aussage a) auf die doppeltperiodische Funktion $\frac{f'(z)}{f(z)}$ an.

$$\text{Res}_{\omega} \left(\frac{f'}{f} \right) = 0.$$

Nachdem gilt $\text{Res}_{\omega} \left(\frac{f'}{f} \right) = \text{Ord}_{\omega}(f)$, folgt die Aussage.

ad c): Wir wenden den Residuumsatz für die Funktion $z \frac{f'(z)}{f(z)}$ an und erhalten:

$$\begin{aligned} \sum_{\omega \in \mathbb{C}/\Lambda} \text{Ord}_{\omega}(f) \omega &= \frac{1}{2\pi i} \int_{\partial D} z \frac{f'(z)}{f(z)} dz \\ &= \frac{1}{2\pi i} \left(\int_a^{a+\omega_1} + \int_{a+\omega_1}^{a+\omega_1+\omega_2} + \int_{a+\omega_1+\omega_2}^{a+\omega_2} + \int_{a+\omega_2}^a \right) z \frac{f'(z)}{f(z)} dz \end{aligned}$$

Jetzt kriegen wir mit einer Substitution von $z \mapsto z + \omega_1$ im 3. und $z \mapsto z + \omega_2$ im 4. Integral:

$$\sum_{\omega \in \mathbb{C}/\Lambda} \text{Ord}_{\omega}(f) \omega = -\frac{\omega_2}{2\pi i} \int_a^{a+\omega_1} \frac{f'(z)}{f(z)} dz + \frac{\omega_1}{2\pi i} \int_a^{a+\omega_2} \frac{f'(z)}{f(z)} dz.$$

Allgemein gilt für meromorphe Funktionen $g(z)$:

$$\frac{1}{2\pi i} \int_a^b \frac{g'(z)}{g(z)} dz$$

ist die Windungszahl um die 0 des Weges

$$[0, 1] \rightarrow \mathbb{C}, t \mapsto g((1-t)a + tb).$$

Startpunkt des Weges ist $g(a)$ und Endpunkt ist $g(b)$. Insbesondere ist, wenn $g(a) = g(b)$, das Integral eine ganze Zahl. Somit impliziert die Periodizität von $\frac{f'}{f}$, dass $\sum \text{ord}_\omega(f)\omega$ die Form $n_1\omega_1 + n_2\omega_2$ mit $n_1, n_2 \in \mathbb{Z}$. Also ist die Aussage gezeigt. $\square$

Definition 1.7 Nun benötigen wir einige Definitionen, um die Hauptaussage dieses Kapitels zu formulieren.

- a) Die Divisorgruppe von $\mathbb{C}/\Lambda$, bezeichnet als $\text{Div}(\mathbb{C}/\Lambda)$, ist die Gruppe der Linearkombinationen

$$\sum_{\omega \in \mathbb{C}/\Lambda} n_\omega(\omega)$$

mit $n_\omega \in \mathbb{Z}$ und gleich 0 für fast alle ω .

- b) Für $D \in \text{Div}(\mathbb{C}/\Lambda)$ definieren wir den Grad von D mit

$$\deg(D) = \sum n_\omega$$

- c)

$$\text{Div}^0(\mathbb{C}/\Lambda) = \{D \in \text{Div}(\mathbb{C}/\Lambda) : \deg(D) = 0\}$$

- d) Für $f \in \mathbb{C}(\Lambda)^*$ definieren wir den Divisor von f als:

$$\text{div}(f) = \sum_{\omega \in \mathbb{C}/\Lambda} \text{ord}_\omega(f)(\omega).$$

- e) Und zuletzt noch die Summationsabbildung:

$$\text{sum} \left(\sum_{\omega \in \mathbb{C}/\Lambda} n_\omega(\omega) \right) = \sum n_\omega \omega \pmod{\Lambda}$$

Nun können wir die vorherigen Aussagen und Definitionen zusammenführen.

Satz 1.8 Die folgende Sequenz ist exakt.

$$1 \rightarrow \mathbb{C}^* \rightarrow \mathbb{C}(\Lambda)^* \xrightarrow{\text{div}} \text{Div}^0(\mathbb{C}/\Lambda) \xrightarrow{\text{sum}} \mathbb{C}/\Lambda \rightarrow 0$$

Beweis:

Zuerst schauen wir uns den linken Teil an $1 \rightarrow \mathbb{C}^* \rightarrow \mathbb{C}(\Lambda)^*$:

$\mathbb{C}(\Lambda)$ bildet einen Körper, man überzeuge sich, dass die doppeltperiodizität durch Summen, Produkte und Quotientenbildung erhalten bleibt. Die Abbildung von $\mathbb{C}^* \rightarrow \mathbb{C}(\Lambda)^*$ ordnet einfach jedem Wert in $\mathbb{C}^*$ der konstanten doppeltperiodischen Funktion mit entsprechendem Wert zu. Diese Abb. ist ein Isomorphismus von $\mathbb{C}^*$ in den Unterkörper $\mathbb{C}^* \subset \mathbb{C}(\Lambda)^*$ somit ist dieser Teil der Sequenz exakt.

Nun zu $\mathbb{C}(\Lambda)^* \xrightarrow{\text{div}} \text{Div}^0(\mathbb{C}/\Lambda)$:

Sei $z \in \mathbb{C}^*$ und $f(x) = z, \forall x \in \mathbb{C}$ die entsprechende doppeltperiodische Funktion, dann gilt $\text{div}(f) = 0$ Für den weiteren Beweis benötigen wir ein Hilfslemma, welches wir hier nicht beweisen werden. Für die Urbilder in $\text{Div}^0(\mathbb{C}/\Lambda) \setminus \{e\}$ betrachte folgendes Lemma.

Lemma 1.9 Seien $n_1, \dots, n_r \in \mathbb{Z}$ und $z_1, \dots, z_r \in \mathbb{C}$ mit:

$$\sum n_i = 0 \quad \text{und} \quad \sum n_i z_i \in \Lambda.$$

Dann existiert eine doppelperiodische Funktion $f \in \mathbb{C}(\Lambda)$ mit $\text{div}(f) = \sum n_i(z_i)$.

Zur Exaktheit an $\text{Div}^0(\mathbb{C}/\Lambda) \rightarrow \mathbb{C}/\Lambda$ nach 1.6 c) und dem obigen Lemma. Die Exaktheit an $\mathbb{C}/\Lambda$ folgt aus der Eigenschaft $\text{sum}(\omega - 0) = \omega$ $\square$

1.1 $\wp$ - Funktion

Definition 1.10 Sei $\Lambda \subset \mathbb{C}$ ein Gitter. Die Weierstrass $\wp$ -Funktion relativ zu Λ ist durch die folgende Reihe gegeben:

$$\wp(z, \Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda, \omega \neq 0} \left(\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right)$$

Des Weiteren benötigen wir noch die Eisenstein-Reihe, Washington führt diese allgemein zum Gewicht k ein und zeigt die Konvergenz für Gewichte größer als 2. Da wir nur gerade Gewichte benötigen, werden wir die Definition von Silverman benutzen mit der Eisensteinreihe zum Gewicht $2k$ und die Konvergenz für k größer als 1 zeigen.

Definition 1.11 Die Eisensteinreihe zum Gewicht $2k$ für gewähltes Gitter Λ definieren wir so:

$$G_{2k}(\Lambda) = \sum_{\omega \in \Lambda, \omega \neq 0} \omega^{-2k}.$$

Im folgenden Satz werden wir nun Aussagen über das Konvergenzverhalten dieser Reihen treffen.

Satz 1.12 Sei $\Lambda \subset \mathbb{C}$ ein Gitter. Dann gilt Folgendes:

- a) Die Eisensteinreihe $G_{2k}(\Lambda)$ ist absolut konvergent für $k > 1$.
- b) Die Weierstrass $\wp$ -Funktion konvergiert absolut und gleichmäßig auf jeder kompakten Teilmenge von $\mathbb{C} \setminus \Lambda$. $\wp(z)$ ist eine meromorphe Funktion mit doppelter Polstelle an jedem Gitterpunkt und Residuum 0.
- c) Die Weierstrass $\wp$ -Funktion ist eine gerade Funktion.

Beweisskizze:

ad a): Nachdem Λ diskret in $\mathbb{C}$ ist, existiert eine konstante $c > 0$, so dass für alle $N \geq 1$ die Punkte in einem Schlauch erfüllen:

$$\#\{\omega \in \Lambda : N \leq |\omega| < N + 1\} < cN.$$

Damit können wir nun abschätzen:

$$\sum_{0 \neq \omega \in \Lambda} \frac{1}{|\omega|^{2k}} \leq \sum_{N=1}^{\infty} \frac{\#\{\omega \in \Lambda : N \leq |\omega| < N + 1\}}{N^{2k}} < \sum_{N=1}^{\infty} \frac{c}{N^{2k-1}} < \infty.$$

ad b): Dies ist Aussage a) + Siehe die Reihenentwicklung für Polstellen und Residuum.

ad c): Zu zeigen: $\wp(z) = \wp(-z)$, was klar ist.

△

Nun kommen wir zu einem erstaunlichen Resultat, so ist nämlich jede doppeltperiodische Funktion $f \in \mathbb{C}(\Lambda)$ eine rationale Kombination, bestehend aus $\wp$ und $\wp'$.

Satz 1.13 Sei $\Lambda \subset \mathbb{C}$ ein Gitter, dann gilt:

$$\mathbb{C}(\Lambda) = \mathbb{C}(\wp, \wp')$$

Beweis:

Bemerkung 1.14 Die Ableitung der $\wp$ -Funktion ist eine ungerade Funktion, nämlich explizit $\wp'(z) = -2 \sum_{\omega \in \Lambda} \frac{1}{(z-\omega)^3}$.

Sei $f \in \mathbb{C}(\Lambda)$, dann können wir f aufteilen und als Summe einer geraden und einer ungeraden Funktion schreiben:

$$f(z) = \frac{f(z) + f(-z)}{2} + \frac{f(z) - f(-z)}{2}.$$

Also reicht es, die Aussage für Funktionen, die entweder gerade oder ungerade sind, zu zeigen. Des Weiteren ist für f ungerade $f\wp'$ gerade. Also sind wir auf den Fall beschränkt, dass f eine gerade Funktion ist. Die Annahme, dass f eine gerade Funktion ist, impliziert:

$$\text{Ord}_\omega(f) = \text{Ord}_{-\omega}(f), \text{ für alle } \omega \in \mathbb{C}$$

Nun behaupten wir, dass falls $2\omega \in \Lambda$, dann ist $\text{Ord}_\omega(f)$ gerade. Um dies zu beweisen, leiten wir $f(z) = f(-z)$ mehrfach ab. Damit erhalten wir:

$$f^{(i)}(z) = (-1)^i f^{(i)}(-z).$$

Falls $2\omega \in \Lambda$, dann hat $f^{(i)}(z)$ den gleichen Wert bei ω und $-\omega$. Also:

$$f^{(i)}(\omega) = f^{(i)}(-\omega) = (-1)^i f^{(i)}(\omega).$$

Also ist $f^{(i)}(\omega) = 0$ für ungerade i , somit ist also $\text{Ord}_\omega(f)$ gerade. Sei D ein Fundamentalparallelogramm von Λ , und sei H eine Halbebene von D . Insbesondere ist H also ein Fundamentalbereich von $(\mathbb{C}/\Lambda)/\{1, -1\}$. Das bisherige liefert den Divisor von f :

$$\sum_{\omega \in H} n_\omega((\omega) + (-\omega))$$

für bestimmte $n_\omega \in \mathbb{Z}$. Für $2\omega \in \Lambda$ wissen wir, dass die Ordnung gerade ist. Betrachte nun also die Funktion:

$$g(z) = \prod_{\omega \in H \setminus \{0\}} (\wp(z) - \wp(\omega))^{n_\omega}.$$

Der Divisor von $\wp(z) - \wp(\omega)$ ist $\omega + (-\omega) - 2(0)$. Also haben f und g die gleichen Pol- und Nullstellen, außer evtl. in der 0. Somit ist $\frac{f}{g}$ eine holomorphe doppeltperiodische Funktion und damit konstant. Es existiert nun also ein $c \in \mathbb{C}$, mit $f = cg \in \mathbb{C}(\wp, \wp')$. $\square$

Wie kommen wir nun zu elliptischen Kurven? Dies ist eine gute Frage, dafür betrachten wir nun die Laurententwicklung von $\wp$ um die Null.

Satz 1.15 a) Die Laurent-Reihe von $\wp(z)$ um $z=0$, ist gegeben durch:

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1)G_{2k+2}z^{2k}$$

b) Für alle $z \in \mathbb{C} \setminus \Lambda$, erfüllt die $\wp$ -Funktion und ihre Ableitung

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6$$

Beweis: ad a)

Für alle $|z| < |\omega|$ gilt:

$$\begin{aligned}
\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} &= \frac{1}{\omega^2} \left(\frac{1}{(1-\frac{z}{\omega})^2} - 1 \right) \\
&= \frac{1}{\omega^2} \left(\sum_{i=0}^{\infty} \left(\sum_{j=0}^i \frac{z^j}{\omega^j} \frac{z^{i-j}}{\omega^{i-j}} \right) - 1 \right) \\
&= \frac{1}{\omega^2} \left(\sum_{i=0}^{\infty} \left(\sum_{j=0}^i \frac{z^i}{\omega^i} \right) - 1 \right) \\
&= \frac{1}{\omega^2} \left(\sum_{i=0}^{\infty} (i+1) \left(\frac{z^i}{\omega^i} \right) - 1 \right) \\
&= \sum_{i=1}^{\infty} (i+1) \frac{z^i}{\omega^{i+2}}
\end{aligned}$$

Für den 2. Schritt erinnere man sich an die geometrische Reihe. Nun setzen wir dieses Resultat in die $\wp$ -Funktion ein.

$$\begin{aligned}
\wp(z) &= \frac{1}{z^2} + \sum_{\omega \in \Lambda, \omega \neq 0} \sum_{i=1}^{\infty} (i+1) \frac{z^i}{\omega^{i+2}} \\
&= \frac{1}{z^2} + \sum_{i=1}^{\infty} G_{2i+2} (2i+1) z^{2i}
\end{aligned}$$

Zum letzten Schritt beachte, dass beim Vertauschen der Summenzeichen sich ω und $-\omega$ bei ungeraden Exponenten aufheben. $\omega^n + (-1)^n \omega = 0$ für n ungerade.

ad b): Siehe [1]Seite 169. Im Prinzip schaut man sich die Laurent-Entwicklung an und sieht dann direkt das Resultat. $\square$

Nun kommen wir zu dem Hauptresultat dieses Kapitels. Hierfür definieren wir uns die Koeffizienten aus 1.15b), als :

$$g_2 = g_2(\Lambda) = 60G_4(\Lambda) \quad \text{und} \quad g_3 = g_3(\Lambda) = 140G_6(\Lambda).$$

Satz 1.16 Sei $\Lambda \subset \mathbb{C}$ ein Gitter.

- a) Das Polynom $f(x) = 4x^3 - g_2x - g_3$ hat drei verschiedene Wurzeln, also ist seine Diskriminante $\Delta(\Lambda) = g_2^3 - 27g_3^2 \neq 0$.
- b) Sei $E(\mathbb{C})$ die Kurve:

$$E : y^2 = 4x^3 - g_2x - g_3$$

, nach a) ist dies eine elliptische Kurve. Dann betrachten wir nun die folgende Abbildung, welche ein Isomorphismus von Gruppen ist.

$$\begin{aligned}
\phi : \mathbb{C}/\Lambda &\rightarrow E(\mathbb{C}) \subset \mathbb{P}^2(\mathbb{C}), \\
z &\mapsto [\wp(z), \wp'(z), 1] \quad , \text{ für } z \not\equiv 0 \pmod{\Lambda}, \\
z &\mapsto [0, 1, 0] \quad , \text{ für } z \equiv 0 \pmod{\Lambda}.
\end{aligned}$$

Beweis: ad a):

Seien $\omega_1, \omega_2 \in \Lambda$ eine Gitterbasis. Sei nun $\omega_3 = \omega_1 + \omega_2$, nachdem $\wp'$ eine ungerade Funktion ist, gilt:

$$\wp' \left(\frac{\omega_i}{2} \right) = -\wp' \left(\frac{-\omega_i}{2} \right) = -\wp' \left(\frac{\omega_i}{2} \right)$$

, also ist $\wp'(\frac{\omega_i}{2}) = 0$. Nach 1.15b) verschwindet $f(x)$ bei $x = \wp(\frac{\omega_i}{2})$. Nun reicht es zu zeigen, dass diese 3 Werte unterschiedlich sind. Die Funktion $\wp(z) - \wp(\omega_i/2)$ ist gerade, also hat sie mindestens eine doppelte Nullstelle bei $z = \omega_i/2$. Nachdem sie eine doppeltperiodische Funktion von Ordnung 2 ist, hat sie nur diese Nullstelle in einem passenden Fundamentalparallelogramm. Also ist $\wp(\omega_i/2) \neq \wp(\omega_j/2)$ für $i \neq j$.

ad b) Für die Surjektivität sei $(x, y) \in E(\mathbb{C})$ ein Punkt auf der elliptischen Kurve. Nachdem $\wp(z) - x$ eine doppelte Polstelle besitzt (Ordnung 2). Impliziert 1.6 a), dass es Nullstellen gibt, somit $\exists z' \in \mathbb{C}$ mit $\wp(z') = x$. Nach 1.15 b) gilt also

$$\wp'(z)^2 = y^2,$$

also $\wp'(z) = \pm y$. Falls $\wp'(z) = y$, sind wir fertig. Sei $\wp'(z) = -y$, dann ist $\wp'(-z) = y$ und $\wp(-z) = x$, also erhalten wir $-z \mapsto (x, y)$.

Sei nun $\wp(z_1) = \wp(z_2)$ und damit $\wp'(z_1) = \wp'(z_2)$, und $z_1 \not\equiv z_2 \pmod{\Lambda}$. Die einzigen Polstellen von $\wp(z)$ sind bei $z \in \Lambda$. Somit ist für z_1 Polstelle von $\wp$ $z_1 \in \Lambda$ und damit auch $z_2 \in \Lambda$, also wäre $z_2 \equiv z_1 \pmod{\Lambda}$. Sei nun z_1 kein Pol von $\wp$, also $z_1 \notin \Lambda$. Die Funktion:

$$h(z) = \wp(z) - \wp(z_1)$$

hat eine doppelte Polstelle bei $z = 0$ und keine anderen Polstellen in $\mathbb{C}/\Lambda$. Nach 1.6 hat h genau zwei Nullstellen. Sei $z_1 = \omega_i/2$ für ein i . Nach a) ist $\wp(\omega_i/2) = 0$, also ist z_1 eine doppelte Nullstelle von $h(z)$, und damit die einzige Wurzel. Somit ist $z_1 = z_2$. Nehme letztendlich an, dass z_1 nicht von der Form $\omega_i/2$. Nachdem $h(-z_1) = h(z_1) = 0$, und $z_1 \not\equiv -z_1 \pmod{\Lambda}$, also sind die zwei Nullstellen von h z_1 und $-z_1 \pmod{\Lambda}$. Demnach ist $z_2 \equiv -z_1 \pmod{\Lambda}$. Aber:

$$y = \wp'(z_2) = \wp'(-z_1) = -\wp'(z_1) = -y.$$

Das bedeutet $y = 0$. Aber $\wp'$ hat nur eine dreifache Polstelle, also drei Nullstellen in $\mathbb{C}/\Lambda$. Diese sind aber von der Form $\omega_i/2$. Somit also auch $z_1 \equiv z_2 \pmod{\Lambda}$. Dies ist aber ein Widerspruch, da wir ja angenommen hatten, dass z nicht von dieser Form ist. Also gilt $z_1 \equiv z_2 \pmod{\Lambda}$, somit ist ϕ injektiv.

Es bleibt noch zu zeigen, dass ϕ ein Gruppenhomomorphismus ist. Sei $\phi(z_i) = P_i = (x_i, y_i)$. Nehme an, dass P_1, P_2 nicht gleich dem Punkt im Unendlichen sind und dass die Gerade durch P_1 und P_2 E in drei Punkten schneidet. Für ein gewähltes z_1 schließt dies endlich viele z_2 aus. Dies hat folgende Gründe. Zum einen ist die Additionsformel eine andere, falls die Punkte identisch sind. Zum anderen müssen wir keine Punkte der Ordnung 2 betrachten. Sei nun $P_3 = P_1 + P_2 = (x_3, y_3)$ der dritte Schnittpunkt der Geraden, dann sagt uns das Gruppengesetz auf E :

$$\begin{aligned} x_3 &= \frac{1}{4} \left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2 \\ &= \frac{1}{4} \left(\frac{\wp'(z_2) - \wp'(z_1)}{\wp(z_2) - \wp(z_1)} \right)^2 - \wp(z_1) - \wp(z_2). \end{aligned}$$

Die Funktion:

$$l(z) = \wp'(z) - a\wp(z) - b$$

hat drei Nullstellen bei $z = z_1, z_2, z_3$. Nachdem sie eine dreifache Polstelle hat, besitzt sie drei Nullstellen in $\mathbb{C}/\Lambda$. Also gilt:

$$\text{div}(l) = z_1 + z_2 + z_3 - 3 \cdot 0.$$

Nach 1.6 gilt $z_1 + z_2 + z_3 \in \Lambda$. Und damit:

$$\wp(z_1 + z_2) = \wp(-z_3) = \wp(z_3) = x_3$$

Somit erhalten wir das gewünschte Ergebnis:

$$\wp(z_1 + z_2) = \frac{1}{4} \left(\frac{\wp'(z_2) - \wp'(z_1)}{\wp(z_2) - \wp(z_1)} \right)^2 - \wp(z_1) - \wp(z_2). \quad (1.1)$$

Dies gilt nun für alle Punkte die wir nicht ausgeschlossen haben.

Für die y-Koordinate ist es eine ziemlich lange Rechnung die Schritte hierfür werden in [2] S.271. Somit haben wir einen Gruppenhomomorphismus für diesen Fall. Bleiben noch die Fälle $\wp(z_i) = \infty$, $z_1 \equiv -z_2 \pmod{\Lambda}$ und $z_1 = z_2$.

Zum Fall: $z_1 \equiv -z_2 \pmod{\Lambda}$

$$\begin{aligned} z_1 &\equiv -z_2 \pmod{\Lambda} \Leftrightarrow z_1 + z_2 \equiv 0 \pmod{\Lambda} \\ &\rightarrow \wp(z_1 + z_2) = \infty. \end{aligned}$$

Stimmt, da $\wp$ Polstellen bei den Gitterpunkten besitzt.

Fall: $\wp(z_i) = \infty$, sei O.b.d.a. $\wp(z_1) \neq \infty$ und $\wp(z_2) = \infty$.

$$\wp(z_1 + z_2) = \wp(z_1)$$

folgt aus der Periodizität von $\wp$.

Für den letzten Fall betrachte die Verdoppelung eines Punktes: Sei $z_2 \rightarrow z_1$ in (1.1). Und bemerke das gilt $2\wp'' = 12\wp^2 - g_2$. Setze dann ein:

$$\begin{aligned} \wp(2z_1) &= \frac{1}{4} \left(\frac{\wp''(z_1)}{\wp'(z_1)} \right)^2 - 2\wp(z_1) \\ &= \frac{1}{4} \left(\frac{6\wp(z_1)^2 - g_2}{\wp'(z_1)} \right) - 2\wp(z_1) \\ &= \frac{1}{4} \left(\frac{6x_1^2 - g_2}{y_1} \right) - 2x_1 \end{aligned}$$

Damit ist es auch in diesem Fall ein Homomorphismus. □

References

- [1] Joseph H. Silverman (2009) *The Arithmetic of Elliptic Curves*.
- [2] Lawrence C. Washington (2008) *Number Theory and Cryptography*.
- [3] Eberhard Freitag, Ralf Busam (2000) *Funktionentheorie 1*.

Anhang

Residuensatz

Sei $D \subset \mathbb{C}$ einfach zusammenhängendes Gebiet. Sei f eine meromorphe Funktion auf D und auf $D \setminus D_f$ holomorph. Sei I ein reelles Intervall und $\Gamma : I \rightarrow D \setminus D_f$ ein geschlossener Weg. Dann gilt:

$$\frac{1}{2\pi i} \int_{\Gamma} f = \sum_{a \in D_f} \text{ind}_{\Gamma}(a) \text{Res}_a(f).$$

ind ist die Windungszahl von Γ um a .

Satz von Liouville

Sei $f : \mathbb{C} \rightarrow \mathbb{C}$ eine beschränkte holomorphe Funktion und existiert eine reelle Konstante c mit $|f(z)| \leq c$ für alle $z \in \mathbb{C}$. Dann ist f konstant.

gerade und ungerade Funktionen

- gerade Funktion f : $f(z) = f(-z)$
- ungerade Funktion f : $f(-z) = -f(z)$

Exakte Sequenz

Eine exakte Sequenz ist eine Sequenz von Objekten, welche mit Morphismen verbunden sind. Sei $f \in \text{Hom}(A, B)$ und $g \in \text{Hom}(B, C)$

$$0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$$

Diese Sequenz ist exakt, falls gilt $\text{Im}(f) = \text{Ker}(g)$, bzw. $f \circ g = 0$.