Das Additionstheorem der $\wp$-Funktion und elliptische Kurven

Vortrag zum Seminar zur Funktionentheorie, 05.11.2007

Cornelia Wirtz

Ziel dieses Vortrages ist es, das Additionstheorem der Weierstraß'schen $\wp$-Funktion zu beweisen. Im Anschluss daran wird kurz auf elliptische Kurven und Beispiele zu Rechnungen mit Hilfe des Additionstheorems sowie Beispiele für elliptische Kurven eingegangen.

§1 Das Additionstheorem und Folgerungen

Ziel des ersten Abschnittes ist es, das Additionstheorem der Weierstraß'schen $\wp$-Funktion zu beweisen. Dazu werden wir eine Funktion konstruieren, mit deren Hilfe ein erster Beweis des Additionstheorems gegeben werden kann.

— *Das Additionstheorem* —

Sei $\Omega = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ ein beliebiges Gitter in $\mathbb{C}$ und $\wp(z) = \wp_\Omega(z) = \wp(z;\omega_1,\omega_2)$ die zugehörige Weierstraß'sche $\wp$-Funktion.

(1.1) Satz (Das Additionstheorem)
Für alle $z, w \in \mathbb{C}$ mit $z, w, z+w, z-w \notin \Omega$ gilt

$$\wp(z+w) + \wp(z) + \wp(w) = \frac{1}{4} \cdot \left(\frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)} \right)^2 . \tag{1}$$

◇

Um diesen Satz zu beweisen, benötigen wir folgendes

(1.2) Lemma
Für $w \in \mathbb{C} \backslash \frac{1}{2}\Omega$ ist

$$f(z) := f(z;w) := \frac{1}{2} \cdot \frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)} \tag{2}$$

eine elliptische Funktion in z mit Parameter w zum Gitter Ω mit Polen erster Ordnung in den Punkten

$$z \in \Omega \text{ und } z \in -w + \Omega \tag{3}$$

und Hauptteilen

$$f(z;w) = -\frac{1}{z} - \wp(w)\cdot z + \mathcal{O}(z^2) \text{ bei } z = 0, \tag{4}$$

$$f(z;w) = \frac{1}{z+w} + c(w) + \mathcal{O}(z+w) \text{ bei } z = -w. \tag{5}$$

Der Koeffizient $c(w)$ wird im Anschluss an den Beweis bestimmt. $\diamond$

Beweis
Die Funktion f ist als Komposition elliptischer Funktionen eine elliptische Funktion zum Gitter Ω und holomorph als Verknüpfung holomorpher Funktionen auf $\mathbb{C}\backslash(\frac{1}{2}\Omega \cup (\pm w + \Omega))$. Da die Weierstraß'sche $\wp$-Funktion Pole in $z \in \Omega$ hat und der Nenner von f für $z \in \pm w + \Omega$ Null wird ($\wp$ ist eine gerade Funktion), ist f in diesen Punkten zunächst nicht definiert. Wir betrachten daher $\lim_{z\to w} f(z;w)$:

$$\begin{aligned}
\lim_{z\to w} f(z;w) &= \frac{1}{2}\cdot \lim_{z\to w} \frac{\wp'(z)-\wp'(w)}{\wp(z)-\wp(w)} \\
&= \frac{1}{2}\cdot \lim_{z\to w} \frac{\wp'(z)-\wp'(w)}{\wp(z)-\wp(w)} \cdot \underbrace{\frac{z-w}{z-w}}_{=1} \\
&= \frac{1}{2}\cdot \lim_{z\to w} \underbrace{\frac{\wp'(z)-\wp'(w)}{z-w}}_{\to \wp''(w)} \cdot \underbrace{\frac{z-w}{\wp(z)-\wp(w)}}_{\to \frac{1}{\wp'(w)}} \\
&= \frac{1}{2}\cdot \wp''(w)\cdot \frac{1}{\wp'(w)} \\
&= \frac{1}{2}\cdot \frac{\wp''(w)}{\wp'(w)}
\end{aligned}$$

Da nach Voraussetzung $w \notin \frac{1}{2}\Omega$, ist $\wp'(w) \neq 0$ nach [K]Lemma 2.3 A (mit [K] wird das Buch *Elliptische Funktionen und Modulformen* von Koecher/Krieg bezeichnet), somit gilt dann $\frac{1}{2}\frac{\wp''(w)}{\wp'(w)} \in \mathbb{C}$, wodurch in den Punkten $z \in w + \Omega$ hebbare Singularitäten vorliegen ($\wp''$ hat keinen Pol in w, da die Laurentreihe von $\wp''$ auf jedem Kompaktum, das keinen Gitterpunkt enthält, gleichmäßig konvergiert).

Betrachte nun $z \in \Omega$. Da f eine elliptische Funktion zum Gitter Ω ist, wird ohne Beschränkung der Allgemeinheit $z = 0$ angenommen. Zeige die erste Aussage über die Hauptteile von f, also dass $f(z;w) = -\frac{1}{z} - \wp(w)\cdot z + \mathcal{O}(z^2)$ bei $z = 0$ gilt. Dazu entwickle $f(z;w)$ in eine Laurent-Reihe um $z = 0$, schreibe also $f(z;w) = \sum_{n=m}^{\infty} c_n z^n$

in einer punktierten Umgebung von 0. Nun hat man

$$\sum_{n=m}^{\infty} c_n z^n = f(z;w) = \frac{1}{2} \cdot \frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)},$$

also

$$\tfrac{1}{2}(\wp'(z) - \wp'(w)) = (\wp(z) - \wp(w)) \sum_{n=m}^{\infty} c_n z^n.$$

Nach dem Konstruktionssatz für die $\wp$-Funktion gilt $\wp(z) = \frac{1}{z^2} + \mathcal{O}(z^2)$, und durch gliedweise Differentiation (möglich, da die Laurent-Reihe lokal gleichmäßig konvergent ist) erhält man $\wp'(z) = -2\frac{1}{z^3} + \mathcal{O}(z)$. Einsetzen in obige Gleichung liefert

$$\tfrac{1}{2}(-2\tfrac{1}{z^3} - \wp'(w) + \mathcal{O}(z)) = (\tfrac{1}{z^2} - \wp(w) + \mathcal{O}(z^2)) \sum_{n=m}^{\infty} c_n z^n,$$

also

$$-\tfrac{1}{z^3} - \tfrac{1}{2}\wp'(w) + \mathcal{O}(z) = c_m z^{m-2} + c_{m+1} z^{m-1} + (c_{m+2} - \wp(w)c_m) z^m + \cdots,$$

woraus man durch Koeffizientenvergleich zunächst direkt $m = -1$ und $c_{-1} = -1$ sowie $c_0 = 0$ erhält. Weiter folgt die Gleichung $0 = c_1 - \wp(w)c_{-1} = c_1 + \wp(w)$, aus der sich $c_1 = -\wp(w)$ ergibt. Dies zeigt $f(z;w) = -\frac{1}{z} - \wp(w) \cdot z + \mathcal{O}(z^2)$ bei $z = 0$. Der Laurent-Reihe entnimmt man nun, dass f in $z \in \Omega$ einen Pol erster Ordnung hat mit $\operatorname{Res}_0 f = -1$.

Betrachte nun $z \in -w + \Omega$. Da f eine elliptische Funktion zum Gitter Ω ist, wird ohne Beschränkung der Allgemeinheit $z = -w$ angenommen. Zeige die zweite Aussage über die Hauptteile von f, also dass $f(z;w) = \frac{1}{z+w} + c(w) + \mathcal{O}(z+w)$ bei $z = -w$ gilt. Dazu betrachte den Nenner von f. Nach [K]2.3(5) hat $\wp(z) - \wp(w)$ zwei einfache Nullstellen in dem Periodenparallelogramm P, da nach Voraussetzung $w \notin \frac{1}{2}\Omega$, also ist $z = -w$ einfache Nullstelle von $\wp(z) - \wp(w)$, da $\wp(-w) = \wp(w)$ ($\wp$ ist eine gerade Funktion). Betrachten wir nun den Zähler von f, so gilt

$$\wp'(z) - \wp'(w) \overset{(z=-w)}{=} \wp'(-w) - \wp'(w) \overset{(\wp' \text{ ungerade})}{=} -\wp'(w) - \wp'(w) = -2\wp'(w) \neq 0.$$

Nach [K]Lemma 2.3 A, folgt nun, dass $f(z;w)$ einen Pol erster Ordnung in $z = -w$ hat, da $\wp(z) - \wp(w)$ eine einfache Nullstelle in $-w$ hat und $\wp'(z) - \wp'(w)$ keine Nullstelle in $z = -w$. Nach obigen Überlegungen hat $f(z;w)$ in jedem Periodenparallelogramm P nur Pole erster Ordnung und $\operatorname{Res}_0 f = -1$. Nach [K]Satz 2.2 B gilt dann

$$0 = \sum_{c \in P} \operatorname{Res}_c f = \operatorname{Res}_{-w} f + \operatorname{Res}_0 f = \operatorname{Res}_{-w} f - 1 \Rightarrow \operatorname{Res}_{-w} f = 1.$$

Nun hat man für die Laurent-Reihe um $z = -w$

$$f(z;w) = \frac{1}{z+w} + c(w) + \mathcal{O}(z+w).$$

□

Wir werden nun den Faktor $c(w)$ bestimmen und einen ersten Beweis des Additionstheorems formulieren:

Beweis
Wir betrachten nun die Funktion

$$g(z) := (f(z;w))^2 - \wp(z+w) - \wp(z) - \wp(w),\ w \in \mathbb{C}\backslash\tfrac{1}{2}\Omega.$$

Die Funktion g ist als Komposition elliptischer Funktionen eine elliptische Funktion zum Gitter Ω. Da $f(z;w)$ nach (1.2) nur einfache Pole in $z \in \Omega$ und $z \in -w+\Omega$ hat, also $(f(z;w))^2$ nur Pole zweiter Ordnung in $z \in \Omega$ und $z \in -w+\Omega$ und $\wp(z+w)$ Pole zweiter Ordnung in $z \in -w+\Omega$ hat, sowie $\wp(z)$ Pole zweiter Ordnung in $z \in \Omega$, kann g höchstens in $z \in \Omega$ und $z \in -w+\Omega$ Pole haben. Betrachte daher $z \in \Omega$. Da g eine elliptische Funktion zum Gitter Ω ist, genügt es, z bei 0 zu betrachten. Mit Hilfe der Laurententwicklung um 0 gilt

$$\begin{aligned}
g(z) =&\ (f(z;w))^2 - \wp(z+w) - \wp(z) - \wp(w)\\
=&\ \left(-\frac{1}{z} - \wp(w)\cdot z + \mathcal{O}(z^2)\right)^2 - \wp(z+w) - \left(\frac{1}{z^2} + \mathcal{O}(z^2)\right) - \wp(w)\\
=&\ \frac{1}{z^2} + \wp(w) - \mathcal{O}(z) + \wp(w) + \wp(w)^2\cdot z^2 - \wp(w)\cdot\mathcal{O}(z^3)\\
&\ -\mathcal{O}(z) - \wp(w)\mathcal{O}(z^3) + \mathcal{O}(z^4) - \wp(z+w) - \wp(w) - \frac{1}{z^2} - \mathcal{O}(z^2)\\
=&\ \underbrace{\mathcal{O}(z)}_{\substack{\to 0 \text{ für } z\to 0}} + \underbrace{\wp(w) - \wp(z+w)}_{\substack{\to 0 \text{ für } z\to 0}}\\
&\to 0 \quad \text{für} \quad z \to 0.
\end{aligned}$$

Damit ist g in $z = 0$ holomorph fortsetzbar mit $g(0) = 0$.

Betrachte nun $z \in -w+\Omega$. Da g eine elliptische Funktion zum Gitter Ω ist, genügt

es, z bei $-w$ zu betrachten. Mit Hilfe der Laurententwicklung um $-w$ gilt

$$\begin{aligned}
g(z) &= (f(z;w))^2 - \wp(z+w) - \wp(z) - \wp(w) \\
&= \left(-\frac{1}{z+w} + c(w) + \mathcal{O}(z+w)\right)^2 - \left(\frac{1}{(z+w)^2} + \mathcal{O}((z+w)^2)\right) \\
&\quad -\wp(z) - \wp(w) \\
&= \frac{1}{(z+w)^2} + \frac{2c(w)}{z+w} + \mathcal{O}(1) + (c(w))^2 + \mathcal{O}(z+w) + \mathcal{O}((z+w)^2) - \frac{1}{(z+w)^2} \\
&\quad +\mathcal{O}((z+w)^2) - \wp(z) - \wp(w) \\
&= \underbrace{\mathcal{O}(1) + (c(w))^2 + \mathcal{O}(z+w) + \mathcal{O}((z+w)^2) + \mathcal{O}((z+w)^2) - \wp(z) - \wp(w)}_{=\mathcal{O}(1)} \\
&\quad +\frac{2c(w)}{z+w} \\
&= \frac{2c(w)}{z+w} + \mathcal{O}(1).
\end{aligned}$$

Da nach obiger Rechnung g keinen Pol in $z \in \Omega$ hat und somit höchstens in den Stellen $z \in -w + \Omega$ Pole erster Ordnung haben kann, folgt mit [K]Satz 2.2 B, dass $0 = \sum_{c \in P} \operatorname{Res}_c f = \operatorname{Res}_{-w} f$ gilt, also $\frac{2c(w)}{z+w} = 0$ und damit $c(w) = 0$. Demnach besitzt g in $z = -w$ eine hebbare Singularität. Insgesamt folgt damit, dass g auf dem Periodenparallelogramm P holomorph und somit nach [K]Satz 2.2 A konstant ist. Weil g in 0 holomorph mit $g(0) = 0$ fortgesetzt werden kann (siehe oben), folgt $g \equiv 0$ auf $w \in \mathbb{C} \backslash \frac{1}{2}\Omega$, das heißt

$$\wp(z+w) + \wp(z) + \wp(w) = \frac{1}{4} \cdot \left(\frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)}\right)^2 \quad \text{für alle} \quad w \in \mathbb{C} \backslash \frac{1}{2}\Omega. \tag{6}$$

Betrachte nun die bisher ausgeschlossenen Fälle $w = \frac{\omega}{2}, \omega \in \Omega$. Die Funktionen auf der rechten und linken Seite sind in $\frac{\omega}{2}$ definiert und stetig auf ihrem Definitionsbereich, $z, w \in \mathbb{C}$ mit $z, w, z+w, z-w \notin \Omega$. Die Gleichheit der Funktionen gilt also auch in $\frac{\omega}{2}$ aufgrund der Stetigkeit. □

— *Folgerungen aus dem Additionstheorem* —

Mit Hilfe des Additionstheorems beweisen wir nun folgendes

(1.3) Korollar
Für $z \in \mathbb{C}\backslash\frac{1}{2}\Omega$ gilt

$$\wp(2z) = -2\wp(z) + \frac{1}{4} \cdot \left(\frac{\wp''(z)}{\wp'(z)}\right)^2. \tag{7}$$

◇

Beweis
Da nach Voraussetzung $z \in \mathbb{C}\backslash\frac{1}{2}\Omega$, folgt mit dem Additionstheorem und der Eigenschaft, dass $\wp$ stetig ist

$$\begin{aligned}
\wp(2z) &= \wp(z+z) \\
&= \lim_{w\to z} \wp(z+w) \\
&= -\wp(z) - \lim_{w\to z} \wp(w) + \lim_{w\to z} \frac{1}{4} \left(\frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)}\right)^2 \\
&= -\wp(z) - \lim_{w\to z} \wp(w) + \lim_{w\to z} \frac{1}{4} \left(\underbrace{\frac{\wp'(w) - \wp'(z)}{w - z}}_{\to \wp''(z)} \underbrace{\frac{w - z}{\wp(w) - \wp(z)}}_{\to \wp'(z)}\right)^2 \\
&= -2\wp(z) + \frac{1}{4} \cdot \left(\frac{\wp''(z)}{\wp'(z)}\right)^2.
\end{aligned}$$

□

Analog kann man mit $\wp(nz)$ für $n = 3, 4, ...$ verfahren, indem man das Additionstheorem verwendet. Man kann alle $\wp(nz)$ als gerade elliptische Funktion rational durch $\wp(z)$ ausdrücken. Dazu folgendes

(1.4) Beispiel
Man kann $\wp(2z)$ rational durch $\wp(z)$ ausdrücken, denn für $z \in \mathbb{C}\backslash\frac{1}{2}\Omega$ gilt

$$\wp(2z) = -2\wp(z) + \frac{1}{16} \cdot \frac{144(\wp(z))^4 - 24(\wp(z))^2 \cdot g_2 + (g_2)^2}{4(\wp(z))^3 - g_2\wp(z) - g_3},$$

und für die anderen Fälle $z \in \Omega$ beziehungsweise $2z \in \Omega$ gilt $\wp(2z) = \wp(z+z) = \wp(z)$ beziehungsweise $\wp(2z) = \infty$. ◇

Beweis
Mit Hilfe von (1.3) und [K]3.3(1) sowie [K]Korollar 3.3 A folgt

$$\begin{aligned}\wp(2z) &= -2\wp(z) + \frac{1}{4}\cdot\left(\frac{\wp''(z)}{\wp'(z)}\right)^2 \\ &= -2\wp(z) + \frac{1}{4}\cdot\frac{\left(\frac{12(\wp(z))^2-g_2}{2}\right)^2}{4(\wp(z))^3 - g_2\wp(z) - g_3} \\ &= -2\wp(z) + \frac{1}{16}\cdot\frac{144(\wp(z))^4 - 24(\wp(z))^2\cdot g_2 + g_2^2}{4(\wp(z))^3 - g_2\wp(z) - g_3}.\end{aligned}$$

□

Mit Hilfe des Additionstheorems folgt weiterhin folgendes

(1.5) Korollar
Für alle $z, w \in \mathbb{C}$ mit $z, w, z+w, z-w \notin \Omega$ gilt

$$\wp(z+w) - \wp(z-w) = -\frac{\wp'(z)\wp'(w)}{(\wp(z)-\wp(w))^2}. \tag{8}$$

◇

Beweis
Mit Hilfe des Additionstheorems folgt

$$\wp(z+w) = -\wp(z) - \wp(w) + \frac{1}{4}\cdot\left(\frac{\wp'(z)-\wp'(w)}{\wp(z)-\wp(w)}\right)^2$$

und

$$\begin{aligned}\wp(z-w) &= -\wp(z) - \wp(-w) + \frac{1}{4}\cdot\left(\frac{\wp'(z)-\wp'(-w)}{\wp(z)-\wp(-w)}\right)^2 \\ &= -\wp(z) - \wp(w) + \frac{1}{4}\cdot\left(\frac{\wp'(z)+\wp'(w)}{\wp(z)-\wp(w)}\right)^2,\end{aligned}$$

da $\wp$ gerade und $\wp'$ ungerade. Betrachtet man nun die Differenz $\wp(z+w) - \wp(z-w)$,

so gilt

$$\begin{aligned}
\wp(z+w)-\wp(z-w) &= -\wp(z)-\wp(w)+\frac{1}{4}\cdot\left(\frac{\wp'(z)-\wp'(w)}{\wp(z)-\wp(w)}\right)^2 \\
&\quad -\left(-\wp(z)-\wp(w)+\frac{1}{4}\cdot\left(\frac{\wp'(z)+\wp'(w)}{\wp(z)-\wp(w)}\right)^2\right) \\
&= \frac{1}{4}\cdot\left(\left(\frac{\wp'(z)-\wp'(w)}{\wp(z)-\wp(w)}\right)^2-\left(\frac{\wp'(z)+\wp'(w)}{\wp(z)-\wp(w)}\right)^2\right) \\
&= \frac{1}{4}\cdot\frac{(\wp'(z)^2-2\wp'(z)\wp'(w)+(\wp'(w))^2}{(\wp(z)-\wp(w))^2} \\
&\quad -\frac{1}{4}\cdot\frac{(\wp'(z))^2+2\wp'(z)\wp'(w)+(\wp'(w))^2}{(\wp(z)-\wp(w))^2} \\
&= \frac{1}{4}\cdot\frac{-2\wp'(z)\wp'(w)-2\wp'(z)\wp'(w)}{(\wp(z)-\wp(w))^2} \\
&= -\frac{\wp'(z)\wp'(w)}{(\wp(z)-\wp(w))^2}.
\end{aligned}$$

□

Auch ergibt sich aus dem Additionstheorem folgendes

(1.6) Korollar
Für alle $z \in \mathbb{C}$ mit $z, z+\frac{\omega_1}{2} \notin \Omega$ gilt

$$\wp(z+\tfrac{\omega_1}{2}) = \frac{e_1\wp(z)+(e_1)^2+e_2e_3}{\wp(z)-e_1}. \tag{9}$$

◇

Beweis
Nach [K]Lemma 2.3 A gilt für $w = \frac{\omega_1}{2}$, dass $\wp'(w) = \wp'(\frac{\omega_1}{2}) = 0$. Damit folgt für $\wp(z+\frac{\omega_1}{2}) = \wp(z+w)$ mit dem Additionstheorem sowie [K]Satz 2.3 und $\wp'(w) = 0$

sowie $\wp(w) = e_1$

$$\begin{aligned}
\wp(z+w) &= -\wp(z) - \wp(w) + \frac{1}{4} \cdot \frac{\left(\wp'(z) - \wp'(w)\right)^2}{\left(\wp(z) - \wp(w)\right)^2} \\
&= -\wp(z) - e_1 + \frac{1}{4} \frac{\left(\wp'(z)\right)^2}{\left(\wp(z) - e_1\right)^2} \\
&= -\wp(z) - e_1 + \frac{1}{4} \frac{4\left(\wp(z) - e_1\right)\left(\wp(z) - e_2\right)\left(\wp(z) - e_3\right)}{\left(\wp(z) - e_1\right)^2} \\
&= -\wp(z) - e_1 + \frac{\left(\wp(z) - e_1\right)\left(\wp(z) - e_2\right)\left(\wp(z) - e_3\right)}{\left(\wp(z) - e_1\right)^2} \\
&= -\wp(z) - e_1 + \frac{\left(\wp(z) - e_2\right)\left(\wp(z) - e_3\right)}{\wp(z) - e_1} \\
&= \frac{\left(-\wp(z) - e_1\right)\left(\wp(z) - e_1\right) + \left(\wp(z) - e_2\right)\left(\wp(z) - e_3\right)}{\wp(z) - e_1} \\
&= \frac{-(\wp(z))^2 + e_1^2 + (\wp(z))^2 - \wp(z)e_3 - \wp(z)e_2 + e_2e_3}{\wp(z) - e_1} \\
&= \frac{e_1^2 - \wp(z)e_3 - \wp(z)e_2 + e_2e_3}{\wp(z) - e_1} \\
&= \frac{(e_1)^2 + \wp(z)\left(-e_3 - e_2\right) + e_2e_3}{\wp(z) - e_1} \\
&= \frac{e_1\wp(z) + (e_1)^2 + e_2e_3}{\wp(z) - e_1},
\end{aligned}$$

wobei die letzte Gleichheit nach [K]Korollar 3.4 A gegeben ist. □

Durch zyklische Vertauschung von e_1, e_2, e_3 erhält man analoge Formeln.

(1.7) Bemerkung

a) (1.2) entnimmt man die Formel $\frac{1}{2}\frac{d}{dz}\frac{\wp'(z)-\wp'(w)}{\wp(z)-\wp(w)} = \wp(z) - \wp(z+w)$ für $z, w \in \mathbb{C}$ mit $z, w, z+w, z-w \notin \Omega$.

Beweis

Nach (1.2) gilt

$$f(z;w) = \frac{1}{2}\frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)} = -\frac{1}{z} - \wp(w)z + \mathcal{O}(z^2) \text{ bei } z = 0.$$

Da f und $\wp$ stetig differenzierbar sind , erhält man durch Differenzieren auf beiden Seiten

$$\frac{d}{dz}f(z;w) = \frac{1}{2}\frac{d}{dz}\frac{\wp'(z)-\wp'(w)}{\wp(z)-\wp(w)} = \frac{1}{z^2} - \wp(w) + \mathcal{O}(z).$$

Damit folgt dann mit Hilfe der Laurententwicklung um 0

$$\begin{aligned}\frac{d}{dz}f(z;w) - \wp(z) + \wp(z+w) &= \frac{1}{2}\frac{d}{dz}\frac{\wp'(z)-\wp'(w)}{\wp(z)-\wp(w)} - \wp(z) + \wp(z+w)\\ &= \frac{1}{z^2} - \wp(w) + \mathcal{O}(z) - \frac{1}{z^2} - \mathcal{O}(z^2)\\ &\quad +\wp(z+w)\\ &= \underbrace{\mathcal{O}(z)}_{\to 0 \text{ für } z\to 0} \underbrace{-\wp(w) + \underbrace{\wp(z+w)}_{\to \wp(w) \text{ für } z\to 0}}_{\to 0 \text{ für } z\to 0}\\ &\to 0 \quad \text{für} \quad z \to 0.\end{aligned}$$

Nach (1.2) gilt weiterhin

$$f(z;w) = \frac{1}{2}\frac{\wp'(z)-\wp'(w)}{\wp(z)-\wp(w)} = \frac{1}{z+w} + \mathcal{O}(z+w) \text{ bei } z = -w.$$

Da f und $\wp$ stetig differenzierbar sind, erhält man durch Differenzieren auf beiden Seiten

$$\frac{d}{dz}f(z;w) = \frac{1}{2}\frac{d}{dz}\frac{\wp'(z)-\wp'(w)}{\wp(z)-\wp(w)} = -\frac{1}{(z+w)^2} + c + \mathcal{O}(z+w),$$

für ein $c \in \mathbb{C}$. Mit Hilfe der Laurententwicklung um $-w$ gilt dann

$$\begin{aligned}\frac{d}{dz}f(z;w) - \wp(z) + \wp(z+w) &= \frac{1}{2}\frac{d}{dz}\frac{\wp'(z)-\wp'(w)}{\wp(z)-\wp(w)} - \wp(z) + \wp(z+w)\\ &= -\frac{1}{(z+w)^2} + c + \mathcal{O}(z+w) - \wp(z)\\ &\quad +\frac{1}{(z+w)^2} + \mathcal{O}(z+w)\\ &= c \underbrace{-\wp(z)}_{\to -\wp(-w)=c' \text{ für } z\to -w} +\mathcal{O}(z+w).\end{aligned}$$

Damit ist gezeigt, dass $\frac{1}{2}\frac{d}{dz}\frac{\wp'(z)-\wp'(w)}{\wp(z)-\wp(w)} - \wp(z) + \wp(z+w)$ eine elliptische Funktion (als Komposition elliptischer Funktionen) ohne Pole ist (nach (1.2) hat $f(z;w)$ nur Pole in $z \in \Omega$ und $z \in -w+\Omega$ und $\wp(z)$ nur Pole in $z \in \Omega$, also kann $\frac{d}{dz}f(z;w) - \wp(z) + \wp(z+w)$ nur Pole in $z \in \Omega$ oder $z \in -w+\Omega$ haben, welche jedoch nach obiger Rechnung nicht vorhanden sind), und somit nach [K]Satz 2.2 A konstant. Die obige Rechnung zeigt

$$\frac{1}{2}\frac{d}{dz}\frac{\wp'(z)-\wp'(w)}{\wp(z)-\wp(w)} - \wp(z) + \wp(z+w) \equiv 0.$$

Daraus folgt die Behauptung. □

b) Mit (1.2) kann man elliptische Funktionen konstruieren, die an zwei vorgegebenen Punkten eines Periodenparallelogramms je einen Pol erster Ordnung haben.

c) Nach dem Additionstheorem und der Differentialgleichung ist $\wp'(z)\cdot\wp'(w)$ ein Polynom in $\wp(z)$, $\wp(w)$ und $\wp(z+w)$. Man erhält ein *algebraisches Additionstheorem* für $\wp$, das heißt es existiert ein Polynom $0 \neq P \in \mathbb{C}[X,Y,Z]$ mit

$$P(\wp(z),\wp(w),\wp(z+w)) = 0 \text{ für alle } z,w \in \mathbb{C}$$

mit $z, w, z+w, z-w \notin \Omega$. Explizit erhält man

$$\begin{aligned} P(X,Y,Z) = {} & (4(X+Y+Z)(X-Y)^2 - (4X^3 - g_2X - g_3) - (4Y^3 - g_2Y - g_3))^2 \\ & -4(4X^3 - g_2X - g_3)(4Y^3 - g_2Y - g_3). \end{aligned}$$

Beweis
Nach dem Additionstheorem und [K]3.3 (die zweite Differentialgleichung) gilt

$$\begin{aligned} & \wp(z+w) + \wp(z) + \wp(w) = \frac{1}{4}\left(\frac{\wp'(z)-\wp'(w)}{\wp(z)-\wp(w)}\right)^2 \\ \Leftrightarrow\ & 4(\wp(z+w)+\wp(z)+\wp(w))\,(\wp(z)-\wp(w))^2 \\ & = (\wp'(z))^2 - 2\wp'(z)\wp'(w) + (\wp'(w))^2 \\ \Leftrightarrow\ & 4(\wp(z+w)+\wp(z)+\wp(w))\,(\wp(z)-\wp(w))^2 \\ & = 4(\wp(z))^3 - g_2\wp(z) - g_3 - 2\wp'(z)\wp'(w) + 4(\wp(w))^3 - g_2\wp(w) - g_3 \\ \Leftrightarrow\ & 4(\wp(z+w)+\wp(z)+\wp(w))\,(\wp(z)-\wp(w))^2 - 4(\wp(z))^3 + g_2\wp(z) + g_3 \\ & -4(\wp(w))^3 + g_2\wp(w) + g_3 \\ & = -2\wp'(z)\wp'(w). \end{aligned}$$

Quadriert man nun die Gleichung auf beiden Seiten, so wird die rechte Seite zu

$$4(\wp'(z))^2(\wp'(w))^2 = 4(4(\wp(z))^3 - g_2\wp(z) - g_3)(4(\wp(w))^3 - g_2\wp(w) - g_3).$$

Setzt man nun $X = \wp(z), Y = \wp(w)$ und $Z = \wp(z+w)$, so erhält man für die Gleichung

$$\begin{aligned}&(4(X+Y+Z)(X-Y)^2 - 4X^3 + g_2X + g_3 - 4Y^3 + g_2Y + g_3)^2\\ &= 4(4X^3 - g_2X - g_3)(4Y^3 - g_2Y - g_3).\end{aligned}$$

Damit folgt für das Polynom P

$$\begin{aligned}P(X,Y,Z) = (4(X+Y+Z)(X-Y)^2 - 4X^3 + g_2X + g_3 - 4Y^3 + g_2Y + g_3)^2\\ -4(4X^3 - g_2X - g_3)(4Y^3 - g_2Y - g_3).\end{aligned}$$

Daraus folgt die Behauptung. □

Weierstraß hat in seinen Vorlesungen die folgende Umkehrung bewiesen

(1.8) Satz
Erfüllt eine meromorphe Funktion f auf $\mathbb{C}$ ein algebraisches Additionstheorem, dann ist f entweder

a) eine rationale Funktion oder

b) eine rationale Funktion in $e^{2\pi i\alpha z}$ mit geeignetem $0 \neq \alpha \in \mathbb{C}$ oder

c) eine elliptische Funktion zu einem geeigneten Gitter. ◇

Einen Beweis findet man zum Beispiel bei W. F. Osgood oder H. Hancock.

§ 2 Elliptische Kurven

In diesem Unterabschnitt geht es um elliptische Kurven und deren Eigenschaften.

— *Bijektion auf die elliptische Kurve* —

(2.1) Definition
Die Teilmenge

$$\mathbb{E} := \mathbb{E}(\Omega) := \left\{(X, Y) \in \mathbb{C} \times \mathbb{C}; \quad Y^2 = 4X^3 - g_2X - g_3\right\} \tag{10}$$

von $\mathbb{C} \times \mathbb{C}$ heißt die (affine) *elliptische Kurve* zu Ω. ◇

Wir haben bereits die Faktorgruppe

$$\mathbb{C}/\Omega = \{z + \Omega; \quad z \in \mathbb{C}\} \tag{11}$$

kennen gelernt. Die Weierstraß'sche $\wp$-Funktion erlaubt eine Parametrisierung der elliptischen Kurve (10) durch die Faktorgruppe (11).

(2.2) Lemma
Die Abbildung

$$\Phi : (\mathbb{C}/\Omega)\setminus\{\Omega\} \to \mathbb{E}(\Omega), \quad \Phi(z + \Omega) := (\wp(z), \wp'(z)), \tag{12}$$

ist eine Bijektion. ◇

Beweis
Die zweite Differentialgleichung nach [K]3.3 ($(\wp'(z))^2 = 4(\wp(z))^3 - g_2\wp(z) - g_3$) zeigt zunächst, dass das Bild von Φ in $\mathbb{E}$ enthalten ist, denn mit $X = \wp(z)$ und $Y = \wp'(z)$ folgt für ein beliebiges, aber festes $z \in \mathbb{C}$, dass $(X, Y) \in \mathbb{E}$, da $Y^2 = (\wp'(z))^2 = 4(\wp(z))^3 - g_2\wp(z) - g_3 = 4X^3 - g_2X - g_3$. Somit gilt $\Phi(z + \Omega) \subseteq \mathbb{E}(\Omega)$. Da jedem Wert aus $(\mathbb{C}/\Omega)\setminus\{\Omega\}$ genau ein Wert aus $\mathbb{E}(\Omega)$ zugeordnet wird und jeder Restklassenvertreter denselben Funktionswert hat ($\wp(z + \omega) = \wp(z)$ für alle $\omega \in \Omega$), ist die Abbildung wohldefiniert.

Um die Surjektivität der Abbildung zu beweisen, wähle man zu $(X, Y) \in \mathbb{E}$ nach [K]Lemma 2.3 B ein $z \in \mathbb{C}$ mit $\wp(z) = X$. Dann gilt

$$Y^2 = 4X^3 - g_2X - g_3 = 4(\wp(z))^3 - g_2\wp(z) - g_3 = (\wp'(z))^2,$$

wodurch $Y = \pm\wp'(z)$, also $Y = \wp'(z)$ oder $Y = -\wp'(z) = \wp'(-z)$, folgt, da $\wp'$ eine ungerade Funktion ist. Ersetzt man nun gegebenenfalls z durch $-z$, so folgt neben $\wp(z) = X$ ($= \wp(-z)$, da $\wp$ eine gerade Funktion ist) auch $\wp'(z) = Y$. Damit liegt (X, Y) im Bild von Φ und die Surjektivität ist gezeigt.

Um die Injektivität der Abbildung zu beweisen, seien $z_1, z_2 \in \mathbb{C}\backslash\Omega$ gegeben mit $(\wp(z_1), \wp'(z_1)) = (\wp(z_2), \wp'(z_2))$. Dann gilt

$$\begin{aligned} &\wp(z_1), \wp'(z_1)) = (\wp(z_2), \wp'(z_2)) \\ \Leftrightarrow\ &\wp(z_1) = \wp(z_2) \text{ und } \wp'(z_1) = \wp'(z_2). \end{aligned}$$

Sei nun zuerst $\wp'(z_1) \neq 0$. Nach [K]Lemma 2.3 A folgt, dass $z_1 \neq \frac{\omega}{2}$ für alle $\omega \in \Omega$ mit $\frac{\omega}{2} \notin \Omega$, also insbesondere $\wp(z_1) \neq e_1, e_2, e_3$ ist. Da $0 \neq \wp'(z_1) = \wp'(z_2)$, ist auch $z_2 \neq \frac{\omega}{2}$, also $\wp(z_2) \neq e_1, e_2, e_3$. Nun gilt

$$\begin{aligned} &\wp(z_1) = \wp(z_2) \\ \Leftrightarrow\ &\wp(z_2) - \underbrace{\wp(z_1)}_{=:w} = 0 \\ \Leftrightarrow\ &\wp(z_2) - w = 0, \end{aligned}$$

wobei $\wp(z_2) - w$, als Funktion von z_2 aufgefasst, nach [K]2.3(5) (und obigen Voraussetzungen) zwei einfache Nullstellen im Periodenparallelogramm P hat, das heißt, es existieren genau zwei verschiedene Punkte $u, v \in P$ mit $\wp(u) = \wp(v) = w$. Wir wissen aber, dass z_1 eine Nullstelle von $\wp(z_2) - w$ ist. Wir können daher ohne Einschränkung $u = z_1 \in P$ wählen. Da ebenfalls z_2 eine Lösung der Gleichung ist, gilt entweder $z_2 \equiv z_1 \pmod{\Omega}$, oder $z_2 \equiv v \pmod{\Omega}$. Nun nehmen wir an, dass $z_2 \equiv v \pmod{\Omega}$. Dann gilt nach [K]Lemma 2.3 B, dass $u + v \in \Omega \Leftrightarrow u \in -v + \Omega$, also dass für ein $\omega \in \Omega$ gilt:

$$\wp'(u) = \wp'(-v + \omega) = \wp'(-v) = -\wp'(v) \neq \wp'(v),$$

da $\wp'$ eine ungerade Funktion ist und $\wp'(v) \neq 0$. Dies ist aber ein Widerspruch zu $\wp'(u) = \wp'(z_1) = \wp'(z_2) = \wp'(v + \omega) = \wp'(v)$ für ein $\omega \in \Omega$. Die Annahme war also falsch und es gilt $z_2 \equiv z_1 \pmod{\Omega}$.

Sei nun $\wp'(z_1) = 0$. Nach [K]Lemma 2.3 A folgt, dass $z_1 = \frac{\omega_k}{2}$ mit $\omega_k \in \Omega$, $\frac{\omega_k}{2} \notin \Omega$, $k = 1, 2, 3$. Nach [K]2.3(4) hat $\wp(z_2) - e_k = \wp(z_2) - \wp(z_1)$, als Funktion von z_2 aufgefasst, genau eine (doppelte) Nullstelle in P, also gilt $z_1 \equiv z_2 \pmod{\Omega}$. Damit folgt insgesamt, dass Φ injektiv ist. Aus der Injektivität und Surjektivität folgt nun die Bijektivität von Φ und damit die Behauptung. □

Neben $\mathbb{E} = \mathbb{E}(\Omega)$ betrachten wir den *Abschluss*

$$\overline{\mathbb{E}} := \overline{\mathbb{E}}(\Omega) := \mathbb{E} \cup \{\mathcal{O}\} \text{ mit } \mathcal{O} := (\infty, \infty), \tag{13}$$

und setzen die Abbildung Φ fort zu einer Bijektion

$$\Phi : \mathbb{C}/\Omega \to \overline{\mathbb{E}}(\Omega), \Phi(z+\Omega) := \begin{cases} (\wp(z), \wp'(z)), & \text{für } z \notin \Omega \\ \mathcal{O}, & \text{für } z \in \Omega. \end{cases} \tag{14}$$

Mit Hilfe der bijektiven Abbildung Φ kann man nun die Gruppenstruktur von $\mathbb{C}/\Omega$ auf die Menge $\overline{\mathbb{E}}$ übertragen, denn für $P, Q \in \overline{\mathbb{E}}$ wird eine Addition erklärt durch

$$P + Q := \Phi(\Phi^{-1}(P) + \Phi^{-1}(Q)), \tag{15}$$

wobei die Addition in $\mathbb{C}/\Omega$ durch $(u+\Omega) + (v+\Omega) := (u+v) + \Omega$ gegeben ist. Damit erhalten wir folgenden

(2.3) Satz
Mit der Verknüpfung (15) wird $\overline{\mathbb{E}}(\Omega)$ zu einer abelschen Gruppe mit $\mathcal{O}$ als neutralem Element. Die Abbildung $\Phi : \mathbb{C}/\Omega \to \overline{\mathbb{E}}(\Omega)$ ist ein Isomorphismus der Gruppen. Für $z \in P$ ist das Inverse $-(\wp(z), \wp'(z))$ gegeben durch $(\wp(-z), \wp'(-z)) = (\wp(z), -\wp'(z))$, und für alle $u, v \in \mathbb{C}$ mit $u, v, u+v \notin \Omega$ hat man

$$(\wp(u), \wp'(u)) + (\wp(v), \wp'(v)) = (\wp(u+v), \wp'(u+v)). \tag{16}$$

$\diamond$

Beweis
Wir zeigen zunächst, dass das Inverse von $(\wp(z), \wp'(z))$ durch $(\wp(-z), \wp'(-z))$ gegeben ist. Mit Hilfe der in (15) erklärten Addition und der schon bekannten Additon in $\mathbb{C}/\Omega$ gilt

$$\begin{aligned} (\wp(z), \wp'(z)) + (\wp(-z), \wp'(-z)) &= \Phi(\Phi^{-1}((\wp(z), \wp'(z))) + \Phi^{-1}((\wp(-z), \wp'(-z)))) \\ &= \Phi(z + \Omega + (-z + \Omega)) \\ &= \Phi(\Omega) \\ &= \mathcal{O}. \end{aligned}$$

Um die Gültigkeit der Gleichung (16) zu zeigen, seien $(\wp(u), \wp'(u)), (\wp(v), \wp'(v)) \in \mathbb{E}$. Dann gilt mit der in (15) erklärten Addition und der schon bekannten Additon in $\mathbb{C}/\Omega$

$$\begin{aligned} (\wp(u), \wp'(u)) + (\wp(v), \wp'(v)) &= \Phi(\Phi^{-1}((\wp(u), \wp'(u))) + \Phi^{-1}((\wp(v), \wp'(v)))) \\ &= \Phi(u + \Omega + (v + \Omega)) \\ &= \Phi((u+v) + \Omega) \\ &= (\wp(u+v), \wp'(u+v)). \end{aligned}$$

Damit haben wir außerdem gezeigt, dass

$$\begin{aligned}\Phi((u+\Omega)+(v+\Omega)) &= \Phi((u+v)+\Omega)\\ &= (\wp(u+v),\wp'(u+v))\\ &= (\wp(u),\wp'(u))+(\wp(v),\wp'(v))\\ &= \Phi(u+\Omega)+\Phi(v+\Omega)\end{aligned}$$

gilt. Wir haben also nachgewiesen, dass Φ ein Homomorphismus ist, welcher nach (2.2) bijektiv, also ein Isomorphismus, ist.

Wir wollen nun noch die Eigenschaften einer abelschen Gruppe nachweisen

(AG) Für $A, B, C \in \overline{\mathbb{E}}(\Omega)$ gilt, da Φ und Φ^{-1} Homomorphismen sind,

$$\begin{aligned}(A+B)+C &= \Phi(\Phi^{-1}(\Phi(\Phi^{-1}(A)+\Phi^{-1}(B)))+\Phi^{-1}(C))\\ &= \Phi(\Phi^{-1}(\Phi(\Phi^{-1}(A))+\Phi(\Phi^{-1}(B)))+\Phi^{-1}(C))\\ &= \Phi(\Phi^{-1}(A+B)+\Phi^{-1}(C))\\ &= \Phi((\Phi^{-1}(A)+\Phi^{-1}(B))+\Phi^{-1}(C))\\ &= \Phi(\Phi^{-1}(A)+(\Phi^{-1}(B)+\Phi^{-1}(C)))\\ &= \Phi(\Phi^{-1}(A)+\Phi^{-1}(B+C))\\ &= \Phi(\Phi^{-1}(A)+\Phi^{-1}(\Phi(\Phi^{-1}(B))+\Phi(\Phi^{-1}(C))))\\ &= \Phi(\Phi^{-1}(A)+\Phi^{-1}(\Phi(\Phi^{-1}(B)+\Phi^{-1}(C))))\\ &= A+(B+C).\end{aligned}$$

(NE) Das neutrale Element in $\overline{\mathbb{E}}(\Omega)$ ist durch $\mathcal{O}$ gegeben, denn

$$\begin{aligned}A+\mathcal{O} &= \Phi(\Phi^{-1}(A)+\underbrace{\Phi^{-1}(\mathcal{O})}_{=\Omega})\\ &= \Phi(\Phi^{-1}(A))\\ &= A,\end{aligned}$$

und

$$\begin{aligned}\mathcal{O}+A &= \Phi(\underbrace{\Phi^{-1}(\mathcal{O})}_{=\Omega}+\Phi^{-1}(A))\\ &= \Phi(\Phi^{-1}(A))\\ &= A.\end{aligned}$$

(IE) Das inverse Element in $\overline{\mathbb{E}}(\Omega)$ ist durch $-A := \Phi(-\Phi^{-1}(A))$ gegeben, denn

$$\begin{aligned} A + (-A) &= A + \Phi(-\Phi^{-1}(A)) \\ &= \Phi(\Phi^{-1}(A) + \Phi^{-1}(\Phi(-\Phi^{-1}(A)))) \\ &= \Phi(\Phi^{-1}(A) - \Phi^{-1}(A)) \\ &= \Phi(\Omega) \\ &= \mathcal{O}. \end{aligned}$$

(KG) Für $A, B \in \overline{\mathbb{E}}(\Omega)$ gilt

$$\begin{aligned} A + B &= \Phi(\Phi^{-1}(A) + \Phi^{-1}(B)) \\ &= \Phi(\Phi^{-1}(B) + \Phi^{-1}(A)) \\ &= B + A. \end{aligned}$$

□

Damit ist aber noch nicht geklärt, wie man die Summe (15) für $P, Q \in \mathbb{E}$ (man beachte, dass nun der Punkt $\mathcal{O}$ rausgenommen ist) berechnet. Nach dem Additionstheorem kann man wegen (16) zumindest die erste Komponente des Punktes $P + Q$ durch die Komponenten von P und Q ausdrücken. Im nächsten Vortrag werden auf geometrische Weise explizite Formeln für die Komponenten von $P + Q$ hergeleitet. Man erhält dadurch unter anderem einen neuen Beweis des Additionstheorems.

Zum Abschluss dieses Paragraphen formulieren wir noch folgende

(2.4) Bemerkung

a) Die Ausnahmerolle des Punktes $\mathcal{O} = (\infty, \infty)$ entfällt, wenn man die elliptische Kurve projektiv beschreibt: Es bezeichne $\mathbb{P}_2(\mathbb{C})$ den zweidimensionalen projektiven Raum über $\mathbb{C}$. Dann gibt es eine kanonische surjektive Abbildung

$$\pi : (\mathbb{C} \times \mathbb{C} \times \mathbb{C}) \setminus \{0\} \to \mathbb{P}_2(\mathbb{C})$$

mit

$$\pi(X, Y, Z) = \pi(X', Y', Z') \Leftrightarrow (X, Y, Z) = \alpha(X', Y', Z') \text{ für ein } 0 \neq \alpha \in \mathbb{C}.$$

Damit ist die projektive elliptische Kurve zu Ω definiert durch

$$\mathbb{PE} := \mathbb{PE}(\Omega) := \left\{ \pi(X, Y, Z); \quad Y^2 Z = 4X^3 - g_2 X Z^2 - g_3 Z^3 \right\}.$$

Offenbar wird durch $(X, Y) \mapsto \pi(X, Y, 1)$ eine Injektion $\mathbb{E} \to \mathbb{PE}$ definiert und der Punkt $\mathcal{O}$ erscheint als $\pi(0, 1, 0)$. Näheres dazu werden wir in den Vorträgen 4–7 kennen lernen.

b) Fasst man $\mathbb{C}/\Omega$ als Riemannsche Fläche auf und betrachtet man $\overline{\mathbb{E}}$ als Kurve im $\mathbb{P}_2(\mathbb{C})$, so definert (14) eine biholomorphe Abbildung. ◇

§ 3 Beispiele

In diesem Unterabschnitt geht es zum einen um Beispiele von elliptischen Kurven, zum anderen um die Anwendung des Additionstheorems an konkreten Aufgaben.

— *Beispiele* —

(3.1) Beispiele

a) Wir wollen nun den reellen Teil von $\mathbb{E}$ betrachten. Ist Ω konjugationsstabil, das heißt $\Omega = \overline{\Omega}$, dann sind g_2 und g_3 nach [K]Satz 3.5 reell und man kann den reellen Anteil von $\mathbb{E}$ zeichnen. Je nachdem ob $4X^3 - g_2X - g_3$ drei oder eine reelle Nullstelle hat, erhält man zwei verschiedene Arten von Bildern.

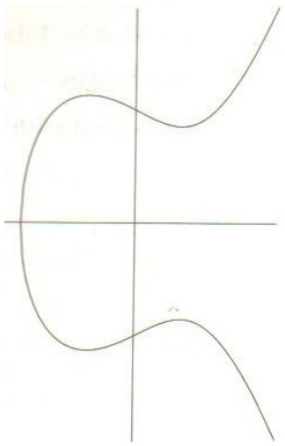
Betrachte zunächst den Fall, dass $4X^3 - g_2X - g_3$ eine reelle Nullstelle hat. Sei $a \in \mathbb{R}$ die reelle Nullstelle von $4X^3 - g_2X - g_3$, dann gilt

$$4X^3 - g_2X - g_3 < 0 \text{ für alle } X < a,$$

da $4X^3 - g_2X - g_3$ für X gegen $-\infty$ gegen $-\infty$ geht (höchster Exponent ist ungerade) und kein weiterer Vorzeichenwechsel stattfinden kann, weil $4X^3 - g_2X - g_3$ als Polynom stetig ist. Weiterhin gilt

$$4X^3 - g_2X - g_3 > 0 \text{ für alle } X > a,$$

da $4X^3 - g_2X - g_3$ für X gegen ∞ gegen ∞ geht (höchster Exponent ist ungerade). Damit wissen wir, dass für $4X^3 - g_2X - g_3 < 0$ die Gleichung $Y^2 = 4X^3 - g_2X - g_3$ keine reelle Lösung für Y hat. Für $4X^3 - g_2X - g_3 \geq 0$ gilt dagegen $Y = \pm\sqrt{4X^3 - g_2X - g_3}$. Es existieren also für alle $X > a$ zwei reelle Werte Y, wodurch sich folgendes Bild ergibt:



Betrachte nun den Fall, dass $4X^3 - g_2X - g_3$ drei reelle Nullstellen hat. Seien $a, b, c \in \mathbb{R}$ mit $a < b < c$ die reellen Nullstellen von $4X^3 - g_2X - g_3$, dann gilt

$$4X^3 - g_2X - g_3 < 0 \text{ für alle } X < a,$$

da $4X^3 - g_2X - g_3$ für X gegen $-\infty$ gegen $-\infty$ geht (höchster Exponent ist ungerade) und kein weiterer Vorzeichenwechsel stattfinden kann, da $4X^3 - g_2X - g_3$ als Polynom stetig ist. Weiterhin gilt

$$4X^3 - g_2X - g_3 > 0 \text{ für alle } a < X < b,$$

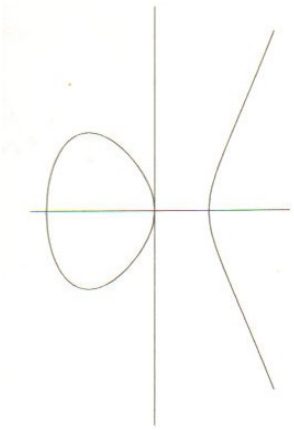
da ein Vorzeichenwechsel von Minus nach Plus stattfinden muss. Es folgt dann, dass

$$4X^3 - g_2X - g_3 < 0 \text{ für alle } b < X < c,$$

da wieder ein Vorzeichenwechsel stattfinden muss, diesmal von Plus nach Minus. Als letztes ergibt sich dann

$$4X^3 - g_2X - g_3 > 0 \text{ für alle } X > c,$$

da $4X^3 - g_2X - g_3$ für X gegen ∞ gegen ∞ geht (höchster Exponent ist ungerade). Daraus folgt insgesamt, dass für $4X^3 - g_2X - g_3 < 0$ die Gleichung $Y^2 = 4X^3 - g_2X - g_3$ keine reelle Lösung für Y hat. Für $4X^3 - g_2X - g_3 \geq 0$ gilt dagegen $Y = \pm\sqrt{4X^3 - g_2X - g_3}$. Es existieren also für alle $a < X < b$ und $X > c$ zwei reelle Werte Y, wodurch sich folgendes Bild ergibt:



b) Als zweites Beispiel betrachten wir eine sogenannte Fermat-Kurve. Wählt man Ω gemäß [K]Korollar 4.4 mit $g_2 = 0, g_3 = (12)^3 = 1728$, also $\wp'^2 = 4\wp^3 - 1728$, dann folgt aus [K]Bemerkung 4.5, dass $\Omega = \frac{(\Gamma(\frac{1}{3}))^3}{4\pi\sqrt{3}}(\mathbb{Z}p + \mathbb{Z})$. In diesem Fall ist die Abbildung

$$f : \mathbb{E}' \Rightarrow \mathbb{F}, (X, Y) \mapsto (U, V), \quad U := \frac{72 + Y}{12X}, V := \frac{72 - Y}{12X}$$

eine Bijektion von

$$\mathbb{E}' := \left\{ (X, Y) \in \mathbb{C} \times \mathbb{C}; \quad Y^2 = 4X^3 - 1728, X \neq 0 \right\}$$

auf die Fermat-Kurve

$$\mathbb{F} := \left\{ (U, V) \in \mathbb{C} \times \mathbb{C}; \quad U^3 + V^3 = 1 \right\}.$$

Die Umkehrabbildung wird dabei gegeben durch

$$f^{-1} : \mathbb{F} \Rightarrow \mathbb{E}', (U, V) \mapsto (X, Y) \text{ mit } X := \frac{12}{U + V} \text{ und } Y := 72\frac{U - V}{U + V}.$$

Beweis
Es gilt $(U, V) \in \mathbb{F}$ für alle $(X, Y) \in \mathbb{E}$, denn mit $Y^2 = 4X^3 - 1728$ gilt

$$\begin{aligned}
\left(\frac{72 + Y}{12X}\right)^3 + \left(\frac{72 - Y}{12X}\right)^3 &= \frac{(5184 + 144Y + Y^2)(72 + Y)}{1728X^3} \\
&\quad + \frac{(5184 - 144Y + Y^2)(72 - Y)}{1728X^3} \\
&= \frac{746496 + 432Y^2}{1728X^3} \\
&= \frac{746496 + 432(4X^3 - 1728)}{1728X^3} \\
&= 1
\end{aligned}$$

Mit dieser Rechnung und der Tatsache, dass jedem Tupel (X, Y) ein eindeutiges Tupel (U, V) zugeordnet wird, ist die Abbildung wohldefiniert. Wir wollen nun noch zeigen, dass die Abbildung bijektiv ist.

Um die Injektivität zu zeigen, seien $(U, V), (U', V') \in \mathbb{F}$ mit $(U, V) = (U', V')$ gegeben. Für $Y \neq \pm 72$ gilt dann

$$\begin{aligned}
(U, V) = (U', V') &\Leftrightarrow \left(\frac{72+Y}{12X}, \frac{72-Y}{12X}\right) = \left(\frac{72+Y'}{12X'}, \frac{72-Y'}{12X'}\right) \\
&\Leftrightarrow \frac{72+Y}{12X} = \frac{72+Y'}{12X'} \text{ und } \frac{72-Y}{12X} = \frac{72-Y'}{12X'} \\
&\Leftrightarrow (72+Y)X' = (72+Y')X \text{ und } (72-Y)X' = (72-Y')X \\
&\Leftrightarrow \frac{X'}{X} = \frac{72+Y'}{72+Y} \text{ und } \frac{X'}{X} = \frac{72-Y'}{72-Y} \\
&\Rightarrow (72+Y')(72-Y) = (72-Y')(72+Y) \\
&\Leftrightarrow 72^2 + 72Y' - 72Y - YY' = 72^2 - 72Y' + 72Y - YY' \\
&\Leftrightarrow Y = Y'.
\end{aligned}$$

Falls $Y = -72$ ist, gilt

$$(U, V) = (U', V') \Rightarrow 0 = \frac{72+Y'}{12X'} \Leftrightarrow Y' = -72 (= Y)$$

und falls $Y = 72$ ist, gilt

$$(U, V) = (U', V') \Rightarrow 0 = \frac{72-Y'}{12X'} \Leftrightarrow Y' = 72 (= Y)$$

Mit $Y = Y'$ folgt für $Y \neq \pm 72$:

$$(U, V) = (U', V') \Leftrightarrow \frac{72+Y}{12X} = \frac{72+Y}{12X'} \text{ und } \frac{72-Y}{12X} = \frac{72-}{12X'},$$

also

$$(U, V) = (U', V') \Rightarrow \frac{1}{12X} = \frac{1}{12X'} \Leftrightarrow X = X'.$$

Für $Y = Y' = \pm 72$ folgt

$$(U, V) = (U', V') \Leftrightarrow \frac{72+Y}{12X} = \frac{72+Y}{12X'} \text{ und } \frac{72-Y}{12X} = \frac{72-Y}{12X'},$$

also

$$(U, V) = (U', V') \Rightarrow \frac{144}{12X} = \frac{144}{12X'} \Leftrightarrow X = X'.$$

Damit ist die Injektivität der Abbildung gezeigt.

Um die Surjektivität nachzuweisen sei nun $(U,V) \in \mathbb{F}$ beliebig. Wähle $(X,Y) = (\frac{12}{U+V}, 72\frac{U-V}{U+V})$, was möglich ist, da $U+V \neq 0$ gelten muss, da sonst $V = -U$ und damit $U^3+V^3 = 0$ im Widerspruch zu $(U,V) \in \mathbb{F}$ gelten würde, dann gilt

$$\begin{aligned} f(X,Y) = f(\tfrac{12}{U+V}, 72\tfrac{U-V}{U+V}) &= \left(\frac{72+72\frac{U-V}{U+V}}{\frac{144}{U+V}}, \frac{72-72\frac{U-V}{U+V}}{\frac{144}{U+V}} \right) \\ &= \left(\tfrac{72(U+V)+72(U-V)}{144}, \tfrac{72(U+V)-72(U-V)}{144} \right) \\ &= (U,V). \end{aligned}$$

Damit ist die Surjektivität der Abbildung gezeigt. Aus der Injektivität und Surjektivität der Abbildung ergibt sich somit die Bijektivität. Es gilt zudem die Richtigkeit der Umkehrabbildung, denn

$$f(X,Y) = f(\tfrac{12}{U+V}, 72\tfrac{U-V}{U+V}) = (U,V),$$

nach obiger Rechnung. □

(3.2) Beispiel

1) Es gilt

$$\wp'(2z) = \frac{28(\wp(z))^3 - g_2\wp(z) + 2g_3}{2\wp'(z)} - \frac{1}{4}\left(\frac{12(\wp(z))^2 - g_2}{2\wp'(z)} \right)^3 \text{ für alle } z \in \mathbb{C}\backslash\frac{1}{2}\Omega,$$

denn $\wp(2z) = -2\wp(z) + \frac{1}{4}(\frac{\wp''(z)}{\wp'(z)})^2$ (siehe (1.3)) ist als Komposition stetig differenzierbarer Funktion stetig differenzierbar in $z \in \mathbb{C}\backslash\frac{1}{2}\Omega$. Differenziert man nun auf

beiden Seiten der Gleichung nach z, so folgt:

$$
\begin{aligned}
2\wp'(2z) &= -2\wp'(z) + \frac{1}{2}\frac{\wp''(z)}{\wp'(z)} \cdot \frac{\wp'''(z)\wp'(z) - (\wp''(z))^2}{(\wp'(z))^2} \\
\Leftrightarrow \wp'(2z) &= -\wp'(z) + \frac{1}{4}\frac{\wp''(z)\wp'''(z)\wp'(z) - (\wp''(z))^3}{(\wp'(z))^3} \\
\Leftrightarrow \wp'(2z) &= -\wp'(z) + \frac{1}{4}\frac{\wp''(z)\wp'''(z)}{(\wp'(z))^2} - \frac{1}{4}\left(\frac{\wp''(z)}{\wp'(z)}\right)^3 \\
\Leftrightarrow \wp'(2z) &= -\wp'(z) + \frac{3\wp'(z)\wp''(z)\wp(z)}{(\wp'(z))^2} - \frac{1}{4}\left(\frac{\wp''(z)}{\wp'(z)}\right)^3 \\
\Leftrightarrow \wp'(2z) &= \frac{-2(\wp'(z))^2 + 3\wp(z)(12(\wp(z)^2 - g_2))}{2\wp'(z)} - \frac{1}{4}\left(\frac{\wp''(z)}{\wp'(z)}\right)^3 \\
\Leftrightarrow \wp'(2z) &= \frac{-2(\wp'(z))^2 + 36(\wp(z))^3 - 3\wp(z)g_2}{2\wp'(z)} \\
&\quad -\frac{1}{4}\left(\frac{12(\wp(z))^2 - g_2}{2\wp'(z)}\right)^3 \\
\Leftrightarrow \wp'(2z) &= \frac{-2(4(\wp(z))^3 - g_2\wp(z) - g_3) + 36(\wp(z))^3 - 3\wp(z)g_2}{2\wp'(z)} \\
&\quad -\frac{1}{4}\left(\frac{12(\wp(z))^2 - g_2}{2\wp'(z)}\right)^3 \\
\Leftrightarrow \wp'(2z) &= \frac{28(\wp(z))^3 - g_2\wp(z) + 2g_3}{2\wp'(z)} - \frac{1}{4}\left(\frac{12(\wp(z))^2 - g_2}{2\wp'(z)}\right)^3,
\end{aligned}
$$

wobei wir bei der dritten Äquivalenz verwendet haben, dass wir nach [K]Korollar 3.3 A wissen, dass $2\wp''(z) = 12(\wp(z))^2 - g_2$, dass also, wenn wir nun die Gleichung auf beiden Seiten nach z differenzieren, gilt

$$2\wp'''(z) = 24\wp'(z)\wp(z) \Leftrightarrow \wp'''(z) = 12\wp'(z)\wp(z).$$

2) Es gilt

$$\wp'(z+w) = -\tfrac{1}{2}\left(\wp'(z) + \wp'(w)\right) + \tfrac{1}{4}\tfrac{(\wp'(z)-\wp'(w))(\wp''(z)-\wp''(w))}{(\wp(z)-\wp(w))^2} - \tfrac{1}{4}\left(\tfrac{\wp'(z)-\wp'(w)}{\wp(z)-\wp(w)}\right)^3$$

für alle $z, w \in \mathbb{C}$ mit $z, w, z+w, z-w \notin \Omega$, denn nach dem Additionstheorem gilt

$$\wp(z+w) = -\wp(z) - \wp(w) + \tfrac{1}{4} \cdot \left(\tfrac{\wp'(z)-\wp'(w)}{\wp(z)-\wp(w)}\right)^2.$$

Differenzieren wir nun beide Seiten einmal nach w und einmal nach z, so erhalten wir folgende zwei Gleichungen:

i) Differentiation nach w ergibt

$$\begin{aligned}\wp'(z+w) &= \frac{1}{2}\frac{\wp'(z)-\wp'(w)}{\wp(z)-\wp(w)}\cdot\frac{-\wp''(w)(\wp(z)-\wp(w))+(\wp'(z)-\wp'(w))\wp'(w)}{(\wp(z)-\wp(w))^2}\\ &\quad -\wp'(w)\\ &= -\wp'(w)-\frac{1}{2}\frac{\wp''(w)(\wp'(z)-\wp'(w))}{(\wp(z)-\wp(w))^2}+\frac{1}{2}\frac{(\wp'(z)-\wp'(w))^2\wp'(w)}{(\wp(z)-\wp(w))^3}.\end{aligned}$$

ii) Differentiation nach z ergibt

$$\begin{aligned}\wp'(z+w) &= \frac{1}{2}\frac{\wp'(z)-\wp'(w)}{\wp(z)-\wp(w)}\cdot\frac{-\wp''(z)(\wp(z)-\wp(w))-(\wp'(z)-\wp'(w))\wp'(z)}{(\wp(z)-\wp(w))^2}\\ &\quad -\wp'(z)\\ &= -\wp'(z)+\frac{1}{2}\frac{\wp''(z)(\wp'(z)-\wp'(w))}{(\wp(z)-\wp(w))^2}-\frac{1}{2}\frac{(\wp'(z)-\wp'(w))^2\wp'(z)}{(\wp(z)-\wp(w))^3}.\end{aligned}$$

Addiert man nun die beiden Gleichungen, so erhält man

$$\begin{aligned}2\wp'(z+w) &= -\wp'(w)-\frac{1}{2}\frac{\wp''(w)(\wp'(z)-\wp'(w))}{(\wp(z)-\wp(w))^2}+\frac{1}{2}\frac{(\wp'(z)-\wp'(w))^2\wp'(w)}{(\wp(z)-\wp(w))^3}\\ &\quad -\wp'(z)+\frac{1}{2}\frac{\wp''(z)(\wp'(z)-\wp'(w))}{(\wp(z)-\wp(w))^2}-\frac{1}{2}\frac{(\wp'(z)-\wp'(w))^2\wp'(z)}{(\wp(z)-\wp(w))^3}\\ &= -\wp'(z)-\wp'(w)+\frac{1}{2}\frac{(\wp'(z)-\wp'(w))^2(\wp'(w)-\wp'(z))}{(\wp(z)-\wp(w))^3}\\ &\quad +\frac{1}{2}\frac{(\wp'(z)-\wp'(w))(\wp''(z)-\wp''(w))}{(\wp(z)-\wp(w))^2}\\ &= -\wp'(z)-\wp'(w)-\frac{1}{2}\left(\frac{\wp'(z)-\wp'(w)}{\wp(z)-\wp(w)}\right)^3\\ &\quad +\frac{1}{2}\frac{(\wp'(z)-\wp'(w))(\wp''(z)-\wp''(w))}{(\wp(z)-\wp(w))^2}.\end{aligned}$$

Indem man nun beide Seiten durch 2 dividiert, folgt die Behauptung.

3) Man kann $\wp(3z)$ rational durch $\wp(z)$ ausdrücken. Dazu sei ohne Einschränkung $z \notin \Omega$, denn sonst gilt $\wp(3z) = \infty$. Zudem sei ohne Einschränkung $2z \notin \Omega$ beziehungsweise $3z \notin \Omega$, da sonst $\wp(3z) = \wp(z+2z) = \wp(z)$ beziehungsweise $\wp(3z) = \infty$. Mit Hilfe des Additionstheorems folgt dann für alle $z \in \mathbb{C}\backslash\frac{1}{6}\Omega$

$$\begin{aligned}\wp(3z) &= -\wp(2z) - \wp(z) + \frac{1}{4}\cdot\left(\frac{\wp'(2z)-\wp'(z)}{\wp(2z)-\wp(z)}\right)^2 \\ &= -\wp(2z) - \wp(z) + \frac{1}{4}\frac{(\wp'(2z))^2 - 2\wp'(2z)\wp'(z) + (\wp'(z))^2}{(\wp(2z)-\wp(z))^2},\end{aligned}$$

wobei $\wp(2z)$ nach (1.4) und $(\wp'(z))^2$ nach [K]3.3, der zweiten Differentialgleichung, rational durch $\wp(z)$ darstellbar ist. Es genügt also, die Ausdrücke $(\wp'(2z))^2$ und $2\wp'(2z)\wp'(z)$ zu betrachten. Für $(\wp'(2z))^2$ gilt nach (3.2)(1)

$$\wp'(2z) = \frac{28(\wp(z))^3 - g_2\wp(z) + 2g_3}{2\wp'(z)} - \frac{1}{4}\left(\frac{12(\wp(z))^2 - g_2}{2\wp'(z)}\right)^3,$$

woraus

$$\begin{aligned}(\wp'(2z))^2 = &-\frac{1}{2}\frac{28(\wp(z))^3 - g_2\wp(z) + 2g_3}{2\wp'(z)}\cdot\left(\frac{12(\wp(z))^2 - g_2}{2\wp'(z)}\right)^3 \\ &\left(\frac{28(\wp(z))^3 - g_2\wp(z) + 2g_3}{2\wp'(z)}\right)^2 + \left(\frac{1}{4}\left(\frac{12(\wp(z))^2 - g_2}{2\wp'(z)}\right)^3\right)^2 \\ = &\frac{(28(\wp(z))^3 - g_2\wp(z) + 2g_3)^2}{4(\wp'(z))^2} + \frac{1}{16}\frac{(12(\wp(z))^2 - g_2)^6}{(2\wp'(z))^6} \\ &-\frac{1}{2}\frac{(28(\wp(z))^3 - g_2\wp(z) + 2g_3)(12(\wp(z))^2 - g_2)^3}{(2\wp'(z))^4},\end{aligned}$$

folgt, wobei $(\wp'(z))^2, (2\wp'(z))^4$ und $(2\wp'(z))^6$ nach [K]3.3, die zweite Differentialgleichung, rational durch $\wp(z)$ darstellbar sind. Insgesamt folgt damit, dass $(\wp'(2z))^2$ rational durch $\wp(z)$ darstellbar ist. Betrachte nun $2\wp'(2z)\wp'(z)$. Nach (3.2)(1) gilt wieder

$$\begin{aligned}2\wp'(2z)\wp'(z) &= 2\wp'(z)\cdot\left(\frac{28(\wp(z))^3 - g_2\wp(z) + 2g_3}{2\wp'(z)} - \frac{1}{4}\left(\frac{12(\wp(z))^2 - g_2}{2\wp'(z)}\right)^3\right) \\ &= \frac{28(\wp(z))^3 - g_2\wp(z) + 2g_3}{2} - \frac{1}{4}\frac{(12(\wp(z))^2 - g_2)^3}{(2\wp'(z))^2},\end{aligned}$$

wobei $(2\wp'(z))^2$ nach [K]3.3, die zweite Differentialgleichung, rational durch $\wp(z)$ darstellbar ist. Es ist also auch $2\wp'(2z)\wp'(z)$ rational durch $\wp(z)$ darstellbar. Damit folgt insgesamt die Behauptung. ◇