mit $\Omega = \mathbb{Z}i\lambda + \mathbb{Z}\lambda$. Das Gitter Ω erfüllt genau dann $g_2(\Omega) = 0$ bzw. $j(\Omega) = 0$, wenn es ein $0 \neq \lambda \in \mathbb{C}$ gibt mit

$$\Omega = \mathbb{Z}\tfrac{1}{2}(1 + i\sqrt{3})\lambda + \mathbb{Z}\lambda.$$

4) Genau dann gilt $j(\Omega) \in \mathbb{R}$ (vgl. 3.5), wenn es ein $0 \neq \lambda \in \mathbb{C}$ gibt, so dass $\lambda\Omega$ konjugationsstabil ist. Es gilt $j(\tau) \in \mathbb{R}$, falls $2\mathrm{Re}\,(\tau) \in \mathbb{Z}$.
5) e_1, e_2, e_3 sind genau dann alle reell, wenn $g_2(\Omega)$ und $g_3(\Omega)$ reell sind und $\Delta(\Omega) > 0$ gilt.
6) Ω ist genau dann ein Gitter, bei dem die Nullstellen von $\wp_\Omega(z)$ in $\frac{1}{2}\Omega$ enthalten sind, wenn $\Omega = \mathbb{Z}i\lambda + \mathbb{Z}\lambda$ für ein $0 \neq \lambda \in \mathbb{C}$ gilt.
7) Wie in Korollar 4.4E betrachte man die Funktion

$$\lambda : \mathbb{H} \to \mathbb{C}\ ,\ \lambda(\tau) := \frac{\wp(1/2; \mathbb{Z}\tau + \mathbb{Z}) - \wp((\tau+1)/2; \mathbb{Z}\tau + \mathbb{Z})}{\wp(\tau/2; \mathbb{Z}\tau + \mathbb{Z}) - \wp((\tau+1)/2; \mathbb{Z}\tau + \mathbb{Z})}.$$

Dann ist λ holomorph mit $\lambda(\tau) \neq 0, 1$ und erfüllt

$$\lambda\left(\frac{a\tau + b}{c\tau + d}\right) = \lambda(\tau) \quad \text{für alle} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}\,(2; \mathbb{Z}) \ \text{ mit } \ b \equiv c \equiv 0\,(\mathrm{mod}\ 2),$$
$$\lambda(\tau + 1) = 1 - \lambda(\tau), \quad \lambda(-1/\tau) = 1/\lambda(\tau).$$

8) Sei $\lambda : \mathbb{H} \to \mathbb{C}$ wie in Aufgabe 7 definiert. Dann existiert zu $\gamma \in \mathbb{C}$ mit $\gamma \neq 0, 1$ ein $\tau \in \mathbb{H}$ mit $\lambda(\tau) = \gamma$.
9) Man berechne ein Analogon der Hurwitz-Identität für σ_9 und σ_{11}, in der nur σ_3 und σ_5 vorkommen.

§5. Elliptische Kurven und das Additionstheorem der $\wp$-Funktion

Wenn es nicht ausdrücklich anders gesagt wird, ist $\Omega = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ auch in diesem Paragrafen ein beliebiges Gitter in $\mathbb{C}$ und $\wp(z) = \wp_\Omega(z) = \wp(z; \omega_1, \omega_2)$ die zugehörige Weierstrasssche $\wp$-Funktion.

1. Das Additionstheorem. *Für alle $z, w \in \mathbb{C}$ mit $z, w, z \pm w \notin \Omega$ gilt*

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

Man hat dazu zunächst die

Proposition. *Für $w \in \mathbb{C} \setminus \frac{1}{2}\Omega$ ist*

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

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

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

und Hauptteilen

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

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

Der Koeffizient $c(w)$ wird sogleich bestimmt.

Beweis. Außer an den Stellen (3) ist f zunächst an den Stellen $z \in w + \Omega$ nicht definiert. Wegen

$$\lim_{z\to w} f(z;w) = \frac{1}{2} \lim_{z\to w} \frac{(\wp'(z) - \wp'(w))/(z-w)}{(\wp(z) - \wp(w))/(z-w)} = \frac{1}{2}\frac{\wp''(w)}{\wp'(w)}$$

und Lemma 2.3A liegen hier aber hebbare Singularitäten vor. Bei $z = 0$ verwendet man $\wp(z) = z^{-2} + \mathcal{O}(z^2)$, also $\wp'(z) = -2z^{-3} + \mathcal{O}(z)$ zum Beweis von (4). Bei $z = -w$ liegt nach 2.3(5) ein einfacher Pol vor, dessen Residuum sich nach Satz 2.2B zu 1 ergibt. □

1. Beweis des Additionstheorems und der Nachweis von

(5') $$c(w) = 0.$$

(Ein 2. Beweis folgt in Abschnitt 5.) Man betrachte die elliptische Funktion

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

Nach der Proposition hat g höchstens in den Punkten (3) Pole. Bei $z = 0$ gilt

$(*)$ $$g(z) = (z^{-2} + 2\wp(w)) - \wp(w) - z^{-2} - \wp(w) + \mathcal{O}(z) = \mathcal{O}(z),$$

und bei $z = -w$ ist

$$g(z) = \frac{1}{(z+w)^2} + \frac{2c(w)}{z+w} - \frac{1}{(z+w)^2} + \mathcal{O}(1) = \frac{2c(w)}{z+w} + \mathcal{O}(1).$$

Danach hätte g höchstens Pole erster Ordnung an den Stellen $-w + \Omega$. Nach Satz 2.2B können solche Pole aber nicht auftreten. Es folgt also $c(w) = 0$ und g ist nach Satz 2.2A konstant. Aus $(*)$ ergibt sich $g = 0$.

Die bisher ausgeschlossenen Fälle $\omega \in \Omega$, $w = \omega/2 \notin \Omega$ folgen nun aus Stetigkeitsgründen. □

Korollar A. *Für $z \in \mathbb{C} \setminus \frac{1}{2}\Omega$ gilt*

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

Beweis. Für $w \to z$ erhält man (6) aus (1). □

Analog kann man mit $\wp(nz)$ für $n = 3, 4, \ldots$ verfahren, indem man das Additionstheorem verwendet. Man beachte, dass sich alle $\wp(nz)$ als gerade elliptische Funktionen rational durch $\wp(z)$ ausdrücken lassen (vgl. **2.4**). Auf diese Frage wird in **6.8** eingegangen.

Korollar B. *Für alle $z, w \in \mathbb{C}$ mit $z, w, z \pm w \notin \Omega$ gilt*

$$\wp(z+w) - \wp(z-w) = -\frac{\wp'(z) \cdot \wp'(w)}{(\wp(z) - \wp(w))^2}. \tag{7}$$

Beweis. Man ersetzt w durch $-w$ in (1) und subtrahiert beide Gleichungen. □

Korollar C. *Für alle $z \in \mathbb{C}$ mit $z, z + \omega_1/2 \notin \Omega$ gilt*

$$\wp\left(z + \omega_1/2\right) = \frac{e_1\wp(z) + e_1^2 + e_2 e_3}{\wp(z) - e_1}.$$

Beweis. Für $w := \omega_1/2$, also $\wp'(w) = 0$, trägt man die Differentialgleichung aus Satz 2.3 in (1) ein und verwendet Korollar 3.4B. □

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

Bemerkungen. a) Der Proposition entnimmt man direkt die Formel

$$\frac{1}{2}\frac{d}{dz}\frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)} = \wp(z) - \wp(z+w) \quad \text{für} \quad z, w \in \mathbb{C} \quad \text{mit} \quad z, w, z \pm w \notin \Omega,$$

denn die Differenz ist eine elliptische Funktion ohne Pole und daher 0 nach (4).
b) Mit Hilfe der Proposition kann man elliptische Funktionen konstruieren, die an zwei vorgegebenen Punkten eines Periodenparallelogramms je einen Pol 1. Ordnung haben.
c) Das Additionstheorem für die Umkehrfunktion von $\wp$ fand man im Nachlass von C.F. Gauss in einem Spezialfall (*Werke VIII*, 93–95).
d) Nach dem Additionstheorem und der Differentialgleichung ist $\wp'(z) \cdot \wp'(w)$ ein Polynom in $\wp(z)$, $\wp(w)$ und $\wp(z+w)$. Nach Quadrieren erhält man bei Beachtung der Differentialgleichung 3.3(1) ein *algebraisches Additionstheorem* für $\wp$, d. h., es existiert ein Polynom $0 \neq P \in \mathbb{C}[X, Y, Z]$ mit

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

Explizit erhält man

$$\begin{aligned} P(X, Y, Z) = {} & \left[4(X+Y+Z)(X-Y)^2 - X^2 - Y^2\right]^2 \\ & - 4(4X^3 - g_2 X - g_3) \cdot (4Y^2 - g_2 X - g_3). \end{aligned}$$

Weierstrass hat gemäß H.A. Schwarz [1893] in seinen Vorlesungen (allerdings nicht in der in den *Math. Werken V* abgedruckten Version) die folgende Umkehrung bewiesen:

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 bei W.F. Osgood ([1920], 515–516) oder H. Hancock ([1910], Chap. II).

2. Elliptische Kurven. In **1.7** hatten wir bereits die Faktorgruppe

(1) $$\mathbb{C}/\Omega = \{z + \Omega \,;\ z \in \mathbb{C}\}$$

betrachtet. Die Teilmenge

(2) $$\mathbb{E} := \mathbb{E}(\Omega) := \{(X, Y) \in \mathbb{C} \times \mathbb{C} \,;\ Y^2 = 4X^3 - g_2 X - g_3\}$$

von $\mathbb{C} \times \mathbb{C}$ heißt die (affine) *elliptische Kurve* zu Ω. Die Weierstraßsche $\wp$-Funktion erlaubt eine *Parametrisierung* der elliptischen Kurve (2) durch die Faktorgruppe (1):

Lemma. *Die Abbildung*

(3) $$\Phi : (\mathbb{C}/\Omega) \setminus \{\Omega\} \longrightarrow \mathbb{E}(\Omega)\ ,\ \Phi(z + \Omega) := (\wp(z), \wp'(z)),$$

ist eine Bijektion.

Beweis. Die Differentialgleichung 3.3(1) zeigt zunächst, dass das Bild von Φ in $\mathbb{E}$ enthalten ist. Zu $(X, Y) \in \mathbb{E}$ wähle man ein $z \in \mathbb{C}$ mit $\wp(z) = X$ gemäß Lemma 2.3B. Dann gilt

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

Ersetzt man ggf. z durch $-z$, so folgt neben $\wp(z) = X$ auch $\wp'(z) = Y$. Damit liegt (X, Y) im Bild von Φ und Φ ist surjektiv.

Sind nun $z_1, z_2 \in \mathbb{C}\backslash\Omega$ mit $(\wp(z_1), \wp'(z_1)) = (\wp(z_2), \wp'(z_2))$ gegeben, so erhält man

$$z_1 \equiv z_2 \,(\mathrm{mod}\ \Omega), \quad \text{falls} \quad \wp'(z_1) \neq 0,$$

oder

$$z_1, z_2 \equiv \omega_1/2, \omega_2/2, \omega_3/2 \,(\mathrm{mod}\ \Omega), \quad \text{falls} \quad \wp'(z_1) = 0,$$

aus 2.3(5) bzw. 2.3(4). Da aber $\wp(\omega_k/2) = e_k$, $k = 1, 2, 3$, paarweise verschieden sind (vgl. 2.3(6)), folgt auch in diesem Fall $z_1 \equiv z_2 \,(\mathrm{mod}\ \Omega)$. Damit ist Φ injektiv. □

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

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