DAS ADDITIONSGESETZ ([1], S. 29–35)

Im vorangegangenen Vortrag haben wir gezeigt, wie die Weierstrass- $\wp$ -Funktion zu einer bijektiven Parametrisierung φ_L der elliptischen Kurve

$$(1) \quad y^2 = 4x^3 - g_2(L)x - g_3(L)$$

durch den Torus $\mathbb{C}/L$ führt. Die Gruppenstruktur auf $\mathbb{C}/L$ kann mittels der Parametrisierung φ_L auf die elliptische Kurve (1) übertragen werden. In Ihrem Vortrag sollen Sie das resultierende Additionsgesetz untersuchen. Bemerkenswerterweise besitzt dieses eine einfache geometrische Interpretation, wie wir in diesem Vortrag sehen werden.

Beweisen Sie zunächst folgenden Hilfssatz.

Hilfssatz 1. *Es sei f eine elliptische Funktion zu dem Gitter $L = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ mit Periodenparallelogramm*

$$\Pi = \{a\omega_1 + b\omega_2 \mid 0 \leq a, b < 1\}.$$

Dann gilt für jedes $\alpha \in \mathbb{C}$

$$\sum_{z \in \Pi + \alpha} \text{ord}_z(f)z \in L.$$

Leiten Sie folgenden Satz her.

Satz 2. *Das additive Inverse des Punktes $P = (x, y)$ auf der elliptischen Kurve (1) ist der Punkt $-P = (x, -y)$.*

Erinnern Sie daran, dass ein Körper K *algebraisch abgeschlossen* genannt wird, wenn jedes nicht-konstante Polynom mit Koeffizienten in K eine Nullstelle in K hat. Erinnern Sie auch daran, dass ein Polynom *homogen* genannt wird, wenn jeder Term von gleichem Grad ist. Hierbei ist der Term x^2y^3z beispielsweise vom Grad 6. Es sei nun $F(x, y, z)$ ein homogenes Polynom. Unter einem *Punkt auf der Kurve F* verstehen wir dann eine (projektive) Lösung $(x, y, z) \in \mathbb{P}_K^2$ der Gleichung $F(x, y, z) = 0$. Desweiteren nennen wir den Punkt $(x, y, z) \in \mathbb{P}_K^2$ einen *Schnittpunkt* der Kurven F und G , wenn das Tripel (x, y, z) die beiden Gleichungen

$$F(x, y, z) = 0,$$

$$G(x, y, z) = 0$$

erfüllt.

Sie können in Ihrem Vortrag den folgenden klassischen Satz ohne Beweis verwenden.

Satz (Satz von Bézout). *Es sei K ein algebraisch abgeschlossener Körper und $F(x, y, z)$ und $G(x, y, z)$ homogene Polynome vom Grad m , bzw. n , mit Koeffizienten aus K . Wir nehmen an, dass F und G keinen echten gemeinsamen Teiler in $K[x, y, z]$ haben. Dann haben die Kurven F und G in $\mathbb{P}_K^2$ genau mn Schnittpunkte, wenn man die Schnittpunkte entsprechend ihrer Multiplizität zählt.*

Zeigen Sie:

Satz 3. *Es seien P_1, P_2, P_3 Punkte auf einer elliptischen Kurve E mit $P_1 + P_2 = P_3$. Dann ist $-P_3$ der dritte Schnittpunkt der Geraden $\overline{P_1P_2}$ mit E . Falls $P_1 = P_2$ gilt, so verstehen wir unter $\overline{P_1P_2}$ die Tangente zu E an P_1 .*

Leiten Sie nun aus dieser geometrischen Beschreibung des Additionsgesetzes einer elliptischen Kurve E folgende explizite Formeln her, welche die Koordinaten von $P_1 + P_2$ durch die Koordinaten von P_1 und P_2 ausdrücken.

Satz 4. *Es sei $f(x) = ax^3 + bx^2 + cx + d \in \mathbb{C}[x]$ mit voneinander verschiedenen Nullstellen. Es seien $P_1 = (x_1, y_1)$ und $P_2 = (x_2, y_2)$ zwei Punkte auf der elliptischen Kurve $y^2 = f(x)$. Wir nehmen an, dass weder P_1 noch P_2 der Punkt im Unendlichen ist. Dann sind die Koordinaten (x_3, y_3) des Punktes $P_3 = P_1 + P_2$ wie folgt gegeben:*

$$(2) \quad x_3 = \begin{cases} -x_1 - x_2 - \frac{b}{a} + \frac{1}{a} \left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 & \text{falls } P_1 \neq P_2, \\ -2x_1 - \frac{b}{a} + \frac{1}{a} \left(\frac{f'(x_1)}{2y_1} \right)^2 & \text{falls } P_1 = P_2, \end{cases}$$

und

$$(3) \quad y_3 = \begin{cases} -y_1 + \frac{(y_2 - y_1)(x_1 - x_3)}{(x_2 - x_1)} & \text{falls } P_1 \neq P_2, \\ -y_1 + \frac{f'(x_1)(x_1 - x_3)}{2y_1} & \text{falls } P_1 = P_2. \end{cases}$$

Wir hätten auch das Additionsgesetz auf einer elliptischen Kurve E direkt durch die Formeln (2) und (3) definieren können und nachrechnen können, dass dann die Punkte auf E eine kommutative Gruppe bilden. Auf diese Weise kann gezeigt werden, dass die Formeln (2) und (3) auf der Menge der Punkte auf einer elliptischen Kurve E über einem beliebigen Körper K mit Charakteristik $\text{char}(K) \neq 2$ eine abelsche Gruppenstruktur definieren.

LITERATUR

- [1] N. Koblitz, Introduction to Elliptic Curves and Modular Forms, Springer, Berlin, 1993.