# Vortrag 5 – Elliptische Kurven

Christoph Sünderhauf, zum Seminar „Einführung in die Theorie elliptischer Kurven“ bei Prof. Dr. K. Wingberg und K. Hübner im Wintersemester 2012/2013 an der Universität Heidelberg.

Literatur:
Joseph H. Silverman. *The Arithmetic of Elliptic Curves.* Springer, 1986.
Robin Hartshorne. *Algebraic Geometry.* Springer, 1977.

**Definition 1 (elliptische Kurve)** *Eine elliptische Kurve (über einem Körper $K$) ist ein Paar $(E, O)$, wobei $E$ eine glatte algebraische Kurve des Geschlechts 1 (über $K$) und $O \in E$ ($O \in E(K)$) ein ausgezeichneter Punkt ist.*

## Verbindung zu Weierstraß-Kurven

**Satz 1** *Sei $E$ eine elliptische Kurve über dem Körper $K$.*

*a) Es existieren Funktionen $x, y \in K(E)$, sodass*

$$\varphi : E \to \mathbb{P}^2 \quad \varphi(P) = [x(P), y(P), 1]$$

*mit $\varphi(O) = [0, 1, 0]$ ein Isomorphismus zu einer Weierstraß-Kurve $C \subset \mathbb{P}^2$*

$$C : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

*ist.*

*b) Je zwei Weierstraß-Kurven zu $E$ aus a) gehen mit einem Koordinatenwechsel*

$$X = u^2X' + r$$

$$Y = u^3Y' + su^2X' + t$$

*($u \neq 0, r, s, t \in K$ geeignet) ineinander über.*

*c) Jede glatte Weierstraß-Kurve ist eine elliptische Kurve mit $O = [0, 1, 0]$.*

**Beweis** **a)** Aus dem Satz von Riemann-Roch wissen wir für $D \in \mathrm{Div}(E)$

$$\deg D > 2g - 2 = 0 \Rightarrow \dim \mathscr{L}(D) = \deg D - g + 1 = \deg D,$$

also hat $\mathscr{L}(n(O))$ für $n \geq 1$ die Dimension $n$. Wähle $x, y \in K(E)$, sodass $\{1, x\}$ eine Basis von $\mathscr{L}(2(O))$ und $\{1, x, y\}$ eine Basis von $\mathscr{L}(3(O))$ ist. Da $\mathrm{ord}_O\, x = -2$ und $\mathrm{ord}_O\, y = -3$ ist $1, x, y, x^2, xy, y^2, x^3 \in \mathscr{L}(6(O))$. Diese Funktionen sind also linear abhängig und es gibt eine nicht-triviale Linearkombination der Null:

$$C : A_1 + A_2x + A_3y + A_4x^2 + A_5xy + A_6y^2 + A_7x^3 = 0, \quad A_i \in K.$$

Es ist $A_6, A_7 \neq 0$; wäre eines von beiden Null, hätten alle Summanden unterschiedliche (Pol)ordnung in $O$ und durch wiederhohltes Anmultiplizieren des Uniformisierenden $t_O$ bei $O$ wären alle $A_i$=0.

O.B.d.A. sei $A_6 = -A_7$. Wähle ansonsten $x' = -A_6 A_7 x \in K(E)$ und $y' = A_6 A_7^2 y \in K(E)$ anstatt $x$ und $y$. Teilt man nun durch $A_6 = -A_7$, erhält man eine Weierstraß-Gleichung von $C$.

Wie gefordert gilt auch

$$\varphi(O) = [x(O), y(O), 1] = [t_O^3 x(O), t_O^3 y(O), t_O^3] = [0, 1, 0].$$

Nach Konstruktion liegt das Bild von $\varphi$ in $C$. Da $E$ glatt ist, ist die rationale Funktion $\varphi : E \to C$ bereits ein Morphismus von Kurven. Nun zeigen wir, dass $\deg \varphi = 1$ und $C$ glatt ist, denn daraus folgt, dass $\varphi$ ein Isomorphismus ist.

$\deg \varphi = 1$:

$$\deg \varphi = 1 \Leftrightarrow [K(E) : \varphi^* K(C)] = 1 \Leftrightarrow K(E) = \varphi^* K(C) \Leftrightarrow K(E) = K(x, y)$$

Betrachte die Abbildung $\psi : E \to \mathbb{P}^1, P \mapsto [x(P), 1]$. Es gilt

$$[K(E) : K(x)] = \deg \psi = \sum_{P \in \psi^{-1}([1,0])} e_\psi(P) = e_\psi(O) = 2.$$

Analog gilt $[K(E) : K(y)] = 3$. Der Index $[K(E) : K(x, y)]$ muss also 2 und 3 teilen, demnach ist er 1.

$C$ glatt: Angenommen, $C$ sei singulär. Dann existiert nach einem Satz für singuläre Weierstraß-Gleichungen eine rationale Funktion $\psi : C \to \mathbb{P}^1$ mit Grad 1. Dann hat $\psi \circ \varphi : E \to \mathbb{P}^1$ auch den Grad 1, $E$ und $\mathbb{P}^1$ sind glatt, also ist $\psi \circ \varphi$ ein Isomorphismus. Das ist ein Widerspruch dazu, dass $E$ das Geschlecht 1 und $\mathbb{P}^1$ das Geschlecht 0 hat.

**b)** Seien $x, y, x', y'$ die Funktionen für die zwei verschiedenen Weierstraß-Kurven aus a). Da $\{1, x'\}$ eine Basis von $\mathscr{L}(2(O))$ ist und $x \in \mathscr{L}(2(O))$ gibt es $u_1, r \in K : x = u_1 x' + r$. Analog ist $y$ auch eine Linearkombination von 1, $y'$ und $x'$: $\exists u_2, s_2, t \in K : y = u_2 y' + s_2 x' + t$. Da die Koeffizienten von $x^3$ und $y^2$ in der Weierstraß-Gleichung (bis auf Vorzeichen) gleich sind und nicht verschwinden, muss $u_1^3 = u_2^2 \neq 0$ sein. Mittels $u := u_2/u_1$ und $s := s_2/u^2$ erhält man Transformationsformeln der gewünschten Form.

**c)** Zu zeigen ist, dass die glatte Weierstraß-Kurve das Geschlecht 1 hat. Aus einem früheren Satz wissen wir, dass das invariante Differential $\omega$ regulär und nicht-verschwindend ist, also $\operatorname{div} \omega = 0$. Mit dem Satz von Riemann-Roch erhält man nun mit $\operatorname{div} \omega$ als kanonischen Divisor $\deg \operatorname{div} \omega = 2g - 2$. Also ist $g = 1$.

## Gruppengesetz

**Lemma 1** *Sei $C$ eine algebraische Kurve des Geschlechts 1 und $P, Q \in C$. Dann ist*

$$(P) \sim (Q) \Leftrightarrow P = Q.$$

*($\sim$ ist die Äquivalenzrelation für $\operatorname{Pic}(C) = \operatorname{Div}(E)/\sim$: $D_1, D_2 \in \operatorname{Div}(C)$, dann*

$$D_1 \sim D_2 \Leftrightarrow \exists f \in \bar{K}(C) : D_1 - D_2 = \operatorname{div} f)$$

**Beweis** „⇒“: Sei $f \in \bar{K}(C)$ mit $\operatorname{div} f = (P) - (Q)$. Dann folgt mit dem Satz von Riemann-Roch wegen $\deg(Q) > 2g - 2 = 0$, dass $\dim \mathscr{L}((Q)) = \deg(Q) - g + 1 = 1$. Allerdings ist $1, f \in \mathscr{L}((Q))$.

$$\Rightarrow \exists \lambda \in \bar{K} : \lambda \cdot 1 = f \Rightarrow \operatorname{div} f = 0 \Rightarrow (P) = (Q) \Rightarrow P = Q$$

„⇐“: Klar, da $1 \in \bar{K}(C)$ und $\operatorname{div} 1 = 0$.

**Satz 2** *Sei $(E, O)$ eine elliptische Kurve.*

*a) Zu $D \in \operatorname{Div}^0(E)$ existiert genau ein Punkt $P := \sigma(D) \in E$, sodass $D \sim (P) - (O)$. Dies erklärt eine Abbildung $\sigma : \operatorname{Div}^0(E) \to E$.*

*b) Für $D_1, D_2 \in \operatorname{Div}^0(E)$ gilt*

$$\sigma(D_1) = \sigma(D_2) \Leftrightarrow D_1 \sim D_2,$$

*c) $\sigma : \operatorname{Pic}^0(E) \to E, D \to \sigma(D)$ ist wohldefiniert und bijektiv.*

*d) Die Umkehrabbildung von $\sigma$ ist*

$$\kappa : E \to \operatorname{Pic}^0 \quad \kappa(P) = [(P) - (O)].$$

*([$(P) - (O)$] bezeichnet hier die Äquivalenzklasse von $(P) - (O)$ in $\operatorname{Pic}^0(E)$.)*

*e) $\sigma$ ist ein Gruppenisomorphismus. Das heißt,*

$$E \cong \operatorname{Pic}^0(E)$$

*als Gruppen und die Addition auf $\operatorname{Pic}^0(E)$ ist mit der geometrischen Addition auf $E$ verträglich.*

**Beweis** **a)** Sei $D \in \operatorname{Div}^0(E)$.

Eindeutigkeit: Seien $P, P' \in E$ mit $(P) - (O) \sim D \sim (P') - (O)$. Dann gilt auch $(P) \sim (P')$ und mit dem Lemma $P = P'$.

Existenz: Da $\deg(D + (O)) = 1 > 2g - 2$ ist nach Riemann-Roch $\dim \mathscr{L}(D + (O)) = \deg(D + (O)) - g + 1 = 1$. Sei $f \in \bar{K}(E)$ ein Erzeuger. Nun ist $\operatorname{div}(f) \geq -D - (O)$, der Hauptdivisor hat Grad 0 aber $\deg(-D - (O)) = -1$. Also gibt es $P \in E$ mit $\operatorname{div}(f) = -D - (O) + (P) \Rightarrow D \sim (P) - (O)$.

**b)** Seien $D_1, D_2 \in \operatorname{Div}^0(E)$ und $P_i = \sigma(D_i) \in E, i = 1, 2$. Aus $D_i \sim (P_i) - (O)$ für $i = 1, 2$ folgt $D_1 - D_2 \sim (P_1) - (P_2)$. Also

$$P_1 = P_2 \overset{\text{Lemma}}{\Leftrightarrow} (P_1) \sim (P_2) \Leftrightarrow D_1 \sim D_2.$$

**c)** Aus a) und b) folgt die Wohldefiniertheit und Injektivität. Außerdem ist $\sigma$ surjektiv:

$$\forall P \in E : \sigma((P) - (O)) = P.$$

**d)** klar

**e)** Seien $P, Q \in E$. Wir zeigen $\kappa(P+Q) = \kappa(P) + \kappa(Q)$, also dass $\kappa$ ein Gruppenhomomorphismus ist. Seien

$$f = a_1X + a_2Y + a_3Z \text{ und } f' = a_1'X + a_2'Y + a_3'Z$$

die Geraden durch $P, Q, R \in E$ beziehungsweise durch $R, O$ und $P+Q$. (Entsprechend der Definition der Addition auf $E$.) Für die dehomogenisierten Funktionen gilt unter Einbezug von $\operatorname{ord}_O y = -3$

$$\operatorname{div} f/Z = (P) + (Q) + (R) - 3(O) \text{ und } \operatorname{div} f'/Z = (R) + (P+Q) - 2(O).$$

Also ist $\operatorname{div} f/f' = \operatorname{div} f/Z - \operatorname{div} f'/Z = (P) + (Q) - (P+Q) - (O)$.

$$\Rightarrow ((P) - (O)) + ((Q) - (O)) - ((P+Q) - (O)) \sim 0$$

Daraus folgt $\kappa(P) + \kappa(Q) - \kappa(P+Q) = 0$.

**Korollar 1** *Sei $E$ eine elliptische Kurve, $D = \sum_{P \in E} n_P(P) \in \operatorname{Div}(E)$. Dann:*

$$D \textit{ Hauptdivisor} \Leftrightarrow \deg D = \sum_{p \in E} n_P = 0 \textit{ und } \underbrace{\sum_{P \in E} [n_P]P = O}_{\textit{Add. in } E}$$

**Beweis** In beiden Fällen gilt $\deg D = \sum_{P \in E} n_P = 0$, also ist

$$D = \sum_{P \in E} n_P(P) = \sum_{P \in E} n_p((P) - (O)).$$

Weil $\sigma$ ein Gruppenhomomorphismus ist und $\sigma((P) - (O)) = P$ folgt daraus

$$\sigma(D) = \sum_{P \in E} [n_P]P. \qquad (*)$$

Also

$$D \text{ Hauptdivisor } \Leftrightarrow \sigma(D) = O \Leftrightarrow \sum_{P \in E} [n_P]P = O.$$

**Exakte Sequenz** Aus der exakten Sequenz

$$1 \to \bar{K}^* \to \bar{K}(C)^* \xrightarrow{\operatorname{div}} \operatorname{Div}^0(C) \to \operatorname{Pic}^0(C)$$

für algebraische Kurven $C$ folgt nun für elliptische Kurven $E$ die exakte Sequenz

$$1 \to \bar{K}^* \to \bar{K}(E)^* \xrightarrow{\operatorname{div}} \operatorname{Div}^0(E) \xrightarrow{\sigma} E.$$

Aufgrund von (*) kann man $\sigma$ auf $\operatorname{Div}^0(E)$ als Addition der einzelnen Komponenten auffassen: Für $\sum_{P \in E} n_P(P) \in \operatorname{Div}^0(E)$ ist

$$\sigma\left(\sum_{P \in E} n_P(P)\right) = \sum_{P \in E} [n_P]P.$$

## Additionsmorphismus

**Satz 3** *Sei $E$ eine elliptische Kurve. Die Addition*

$$+ : E \times E \to E$$

*und das additive Inverse*

$$- : E \to E$$

*sind Morphismen.*

**Beweis** **„-“:** Für das Inverse von $P = (x, y) \in E$ gilt die Formel

$$-P = (x, -y - a_1 x - a_3)$$

mit den entsprechenden Koeffizienten aus der Weierstraß-Gleichung. Da $E$ glatt ist, ist diese rationale Funktion bereits ein Morphismus.

**„+“:** Zunächst zeigen wir, dass für $Q \in E$ die Translation um $Q$

$$\tau_Q : E \to E,\ P \mapsto P + Q$$

ein Morphismus ist. Da wir eine explizite Formel für die Addition auf Weierstraß-Kurven haben, sehen wir, dass $\tau_Q$ eine rationale Abbildung ist. Außerdem ist $E$ eine glatte Kurve, $\tau_Q$ also ein Morphismus. $\tau_{-Q}$ ist die Inverse, bei $\tau_Q$ handelt es sich demnach um einen Isomorphismus.

Für die allgemeine Addition von $P = (x_1, y_1), Q = (x_2, y_2) \in E$ gelten ebenfalls die Additionsformeln. Allerdings bräuchten wir für dieselbe Folgerung wie für $\tau$, dass $E \times E$ eine glatte Kurve ist.

Anhand der Additionsformel sieht man, dass die rationale Abbildung $+$ zumindest für $P, Q \neq O$ und $x_1 \neq x_2$ definiert ist. $x_1 = x_2$ impliziert $P = \pm Q$. $+$ ist also bei allen Punkten, die nicht die Form $(P, \pm P)$, $(P, O)$ oder $(O, P)$ haben, definiert.

Betrachte die Translationen $\tau_{R_1}$, $\tau_{R_2}$ um $R_1, R_2 \in E$ und die rationale Abbildung

$$\varphi : E \times E \xrightarrow{\tau_{R_1} \times \tau_{R_2}} E \times E \xrightarrow{+} E \xrightarrow{\tau_{-R_1}} E \xrightarrow{\tau_{-R_2}} E$$

$$(P_1, P_2) \mapsto (P_1 + R_1, P_2 + R_2) \mapsto P_1 + R_1 + P_2 + R_2 \mapsto P_1 + P_2 + R_2 \mapsto P_1 + P_2.$$

Nun stimmen $\varphi$ und $+$ überall wo diese beide definiert sind überein. Bei geeigneter Wahl von $R_1, R_2 \in E$ kann man Abbildungen $\varphi_1, \dots \varphi_n : E \times E \to E$ wie oben finden, sodass an jedem Punkt zumindest ein $\varphi_i$ definiert ist. Sind mehrere dieser rationalen Abbildungen an einem Punkt definiert, stimmen sie dort überein. Insgesamt ist damit $+$ also auf ganz $E \times E$ definiert und ist damit ein Morphismus.

## Ausblick auf Jacobi-Varietäten

Zu jeder algebraischen Kurve gibt es eine sogenannte Jacobi-Varietät. Das ist eine spezielle Varietät, die eine Gruppenstruktur besitzt. Im Falle von elliptischen Kurven ist die elliptische Kurve ihre eigene Jacobi-Varietät. Das dadurch auf der elliptischen Kurve erklärte Gruppengesetz ist genau das, welches wir hier auch betrachten.