Punktgruppen auf Elliptischen Kurven

Gerrit Gruben
Freie Universität Berlin
Fachbereich Mathematik und Informatik
Institut für Mathematik

30. Januar 2011

I Das Gruppengesetz

Sei $E \subseteq \mathbb{P}^2$ eine Elliptische Kurven gegeben durch die Weierstrass-Gleichung. Das heisst nach Inhomogenisierung:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

für $a_i \in \bar{K}$ bzw. K (wenn gegeben über K) und ausgezeichnetem Punkt $O := [0, 1, 0]$ bei Unendlich.

Wenn $L \subseteq \mathbb{P}^2$ eine Gerade, kläre hier das Verhalten, wie die Gerade geschnitten wird (entweder ist L tangential oder schneidet drei verschiedene Punkte von E).

Definition 1 (Verknüpfungsgesetz).
Seien $P, Q \in E$ und L die Gerade, welche P und Q verbindet bzw. bei $P = Q$ tangential an P liegt und R ein dritter Schnittpunkt. Betrachte die Gerade L', welche R und O verbindet, der dritte Schnittpunkt von L' mit E (außer R und 0) sei $P \oplus Q$.

Satz 1 (Eigenschaften von $\oplus$).
(a) Sei eine Gerade $L \subseteq \mathbb{P}^2$ gegeben, die E an den Punkten P, Q, R schneidet, dann gilt

$$(P \oplus Q) \oplus R = O.$$

(b) $P \oplus O = P$ für alle $P \in E$.

(c) $P \oplus Q = Q \oplus P$ für alle $P, Q \in E$.

(d) Sei $P \in E$. Dann gibt es einen Punkt auf E ($\ominus P$, so dass

$$P \oplus (\ominus P) = O.$$

(e) Sei $P, Q, R \in E$. Dann

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$$

(f) Wenn E/K, dann ist die Menge der K-rationalen Punkte auf E:

$$E(K) := \left\{(x, y) \in K^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\right\}$$

eine Untergruppe von E.

BEWEIS
(a) Es wurde $P \oplus Q$ als dritter Schnittpunkt von L' außer R und O definiert. Daher ist O der dritte Schnittpunkt der Geraden, welche $P \oplus Q$ und R verbindet. Die Gerade durch O und O schneidet sonst nur O.

(b) Es wird jeweils die selbe Gerade betrachtet und man erhält wieder P.

(c) Es werden die selben Geraden auf beiden Seiten der Gleichung betrachtet.

(d) Betrachten wir die Gerade, welche P und O verbindet, so ist der dritte Schnittpunkt mit E das gesuchte Element $\ominus$.

(e) Wiederholung vom letzten Mal: Wir haben einen Isomorphismus κ:

$$\kappa : E \to \mathrm{Pic}^0(E), P \mapsto [(P)] - (O)$$

Wobei $\mathrm{Pic}^0(E)$ die Gruppe $Div^0(E)$ (Divisoren mit Grad 0) ausgeteilt nach den Hauptdivisoren ist (solche, wo man ein $f \in \bar{K}(E)$ findet, sodass (f) gerade dieser Divisor ist). Für $P, Q \in E$ folgt die Assoziativität aus der Gleichung

$$\kappa(P \oplus Q) = \kappa(P) + \kappa(Q).$$

Sei $L \subseteq \mathbb{P}^2$ die Verbindungsgerade durch P und Q gegeben durch die Gleichung:

$$L : \underbrace{\alpha x + \beta y + \gamma z}_{=:F(x,y,z)} = 0.$$

es bezeichnet R den dritten Schnittpunkt von L mit E. $L' \subseteq \mathbb{P}^2$ sei dann die Verbindungsgerade von R und O. $Z \subseteq \mathbb{P}^2$ sei die Linie gegeben durch $z = 0$. Es schneidet Z E bei O mit der Multiplizität 3 (per Konstruktion!). Damit gilt für die Divisoren:

$$\mathrm{div}(F/Z) = \mathrm{div}(F) - \mathrm{div}(Z) = (P) + (Q) + (R) - 3(O)$$

und

$$\mathrm{div}(F'/Z) = \mathrm{div}(F') - \mathrm{div}(Z) = (R) + (P \oplus Q) + (O) - 3(O) = (R) + (P \oplus Q) - 2(O)$$

Nach Subtraktion der ersten von der zweiten Gleichung erhält man

$$(P \oplus Q) - (P) - (Q) + (O) = \mathrm{div}(f'/f)$$

da $\mathrm{div}(f'/f)$ ein Hauptdivisor ist, ist der Ausdruck in $\mathrm{Pic}^0(E)$ identisch 0. Damit ist aber

$$\kappa(P \oplus Q) - \kappa(P) - \kappa(Q) = 0$$

(f) Wenn P, Q Koordinaten in K haben, dann wird selbiges auch für $P \oplus Q$ gelten, wie man aus den Formeln ablesen kann. ∎

Notation: Es wird ab sofort statt $\oplus$ und $\ominus$ die üblichen Symbole $+$ und $-$ verwendet. Und es sei für $m \in \mathbb{Z}$:

$$[m] : E \to E, P \mapsto m \cdot P = \begin{cases} \underbrace{P + \ldots + P}_{m \text{ mal}}, & m > 0 \\ O, & m = 0 \\ [-m][-P], & m < 0 \end{cases}$$

Im folgendem wird eine explizite Formel zur Berechnungen der Gruppenoperation bestimmt. Setze

$$F(x, y) := y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$$

und sei $P_0 = (x_0, y_0) \in E$. Es ist die Verbindungslinie zwischen P_0 und O gegeben durch:

$$L : x - x_0 = 0$$

wobei der dritte Schnittpunkt $-P_0 = (x_0', y_0')$ ist. Es ist $x_0' = x_0$ evident und die quadratische Gleichung (in y)

$$F(x_0, y) = y^2 + [a_1x + a_3]y - x^3 - a_2x^2 - a_4x - a_6$$

hat zwei Lösungen y_0 und y_0'. Also lässt sich das Polynom in der Form

$$F(x_0, y) = c(y - y_0)(y - y_0')$$

schreiben. Wegen $[y^2]F(x_0, y) = 1$ ist $c = 1$ und $[y]F(x_0, y) = a_1x + a_3 = -y_0 - y_0'$ ergibt

$$y_0' = -y_0 - a_1x - a_3$$

zusammengefasst ist damit

$$-P_0 = (x_0, -y_0 - a_1x - a_3).$$

Nun zur Addition: $P_i = (x_i, y_i) \in E$ für $i = 1, 2$. Wenn $x_1 = x_2$ und $y_1 + y_2 + a_1x_1 + a_3 = 0 \Rightarrow P_1 = -P_2 \Rightarrow P_1 + P_2 = O$. Wenn $x_1 = x_2$ und $y_1 + y_2 + a_1x_1 + a_3 = 0 \Rightarrow P_1 = -P_2$, also $P_1 + P_2 = O$. Die Gerade durch P_1, P_2 hat die Form

$$L : y = \lambda x + \nu$$

Wenn $x_1 \neq x_2$, dann ist

$$\lambda = \frac{\Delta y}{\Delta x} = \frac{y_2 - y_1}{x_2 - x_1}$$

und es gilt für die Abszisse

$$y_1 = \frac{\Delta y}{\Delta x}x_1 + \nu \Leftrightarrow \nu = y_1 - \frac{\Delta y}{\Delta x}x_1 = \frac{y_1\Delta x - \Delta y x_1}{\Delta x} = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}$$

Ist $x_1 = x_2$ muss die Tangente durch $P = (x_1, y_1)$ beschrieben werden. Die Darstellung von L ist

$$\frac{\partial F}{\partial x}(x_1, y_1)(x - x_1) + \frac{\partial F}{\partial y}(x_1, y_1)(y - y_1) = 0.$$

Dazu rechnet man aus:

$$\begin{aligned}\frac{\partial F}{\partial x}(x_1, y_1) &= a_1y_1 - 3x_1^2 - 2a_2x_1 - a_4\\ \frac{\partial F}{\partial y}(x_1, y_1) &= 2y_1 + a_1x_1 + a_3\end{aligned}$$

Und man erhält

$$L : (a_1y_1 - 3x_1^2 - 2a_2x_1 - a_4)(x - x_1) + (2y_1 + a_1x_1 + a_3)(y - y_1) = 0$$

wo man

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}$$

abliest. Und es gilt

$$\begin{aligned}\nu &= \frac{a_1y_1x_1 - 3x_1^3 - 2a_2x_1^2 - a_4 + 2y_1^2 + a_1x_1y_1 + a_3y_1}{2y_1 + a_1x_1 + a_3}\\ &= \frac{-3x_1^3 - 2a_2x_1^2 - a_4x_1 - a_3y_2 + 2x_1^3 + 2a_2x_1^2 + 2a_4x_1 + 2a_6}{2y_1 + a_1x_1 + a_3}\\ &= \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}\end{aligned}$$

Setze $p(x) := \lambda x + \nu$, dann gilt

$$F(x, \lambda x + \nu) = p(x)^2 + [a_1x + a_3]p(x) - x^3 - a_2x^2 - a_4x - a_6.$$

Dieses Polynom hat Nullstellen x_1, x_2, x_3 wobei $P_3 := (x_3, y_3)$ der dritte Punkt von $L \cap E$ ist. Es gilt $P_1 + P_2 + P_3 = O$, also $P_1 + P_2 = -P_3$.

Schreibe wieder $F(x, \lambda x+\nu) = c(x-x_1)(x-x_2)(x-x_3)$, dann ist $[x^3]F(x, p(x)) = -1 \Rightarrow c = -1$ und $[x^2]F(x, p(x)) = x_1 + x_2 + x_3 = \lambda^2 + a_1\lambda - a_2$, also haben wir

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$$

woraus $y_3 = \lambda x_3 + \nu$ folgt. Es ist also $P_3 = (x_3, \lambda x_3 + \nu)$ und

$$P_1 + P_2 = -P_3 = (x_3, -(\lambda x_3 + \nu) - a_1 x_3 - a_3).$$

Zusammenfassend:

Satz 2 (Rechenformeln).
Sei E eine Elliptische Kurve gegeben in der Weiterstrassform:

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

(a) (Invertierungsformel) Sei $P_0 = (x_0, y_0) \in E$. Dann

$$-P_0 = (x_0, -y_0, a_1 x_0 - a_3).$$

(b) (Additionsformel) Sei $P_1 + P_2 = P_3$ mit $P_i = (x_i, y_i) \in E$ für $i = 1, 2, 3$. Wenn $x_1 = x_2$ und $y_1 + y_2 + a_1 x_2 + a_3 = 0$, dann

$$P_1 + P_2 = 0.$$

Sonst sei

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_2}, & x_1 \neq x_2 \\ \dfrac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3}, & x_1 = x_2 \end{cases}.$$

und

$$\nu = \begin{cases} \dfrac{y_1 x_2 - y_2 x_1}{x_2 - x_1}, & x_1 \neq x_2 \\ \dfrac{-x_1^3 + a_4 x_1 + 2a_6 - a_3 y_1}{2y_1 + a_1 x_1 + a_3}, & x_1 = x_2 \end{cases}.$$

Dann gilt

$$\begin{aligned} x_3 &= \lambda^2 + a_1 \lambda - a_2 - x_1 - x_2 \\ y_3 &= -(\lambda + a_1) x_3 - \nu - a_3 \end{aligned}$$

(c) Für $P_1 \neq \pm P_2$ lässt sich die x Koordinate so ausrechnen

$$x(P_1 + P_2) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 + a_1 \left(\frac{y_2 - y_2}{x_2 - x_2}\right) - a_2 - x_1 - x_2.$$

(d) Die Verdopplungsformel $P = (x, y) \in E$:

$$x([2]P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6}$$

wobei $b_2 = a_1^2 + 4a_4, b_4 = 2a_4 + a_1a_3, b_6 = a_3^2 + 4a_6$ und $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$.

BEWEIS
(a) und (b) haben wir schon.

(c) Wegen $P_1 \neq \pm P_2$ ist $\lambda = \Delta y/\Delta x$. Einsetzen liefert dann genau die Formel.

(d) ∎

Wenn $\operatorname{char} K \neq 2$, dann kann über die Substitution

$$y \mapsto \frac{1}{2}(y - a_1x - a_3)$$

die Gleichung in die Form

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

gebracht werden (b_i definiert wie bei der Verdopplungsformel).

Kann man sogar $\operatorname{char} K \neq 2, 3$ voraussetzen, dann kann man ausgehend von dieser Gleichung mit der Substitution

$$(x, y) \mapsto \left(\frac{x - 3b_2}{36}, \frac{y}{108}\right)$$

die Gleichung in die Form

$$E : y^2 = x^3 - 27c_4x - 54c_6$$

bringen, wobei

$$\begin{aligned} c_4 &= b_2^2 - 24b_4 \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6 \end{aligned}$$

gilt. Wenn man nun $y^2 = x^3 + ax + b$ annimmt, so vereinfachen sich die arithmetischen Formeln oben.

Satzverzeichnis

Literatur

[1] Silverman, Joseph H.: *Graduate Texts in Mathematics*. Bd. 106: *The Arithmetic of Elliptic Curves*. Springer-Verlag, 1986