Einführung in die Theorie der elliptischen Kurven
6. Vortrag: Isogenien

von YICHUAN SHEN

20. Juli 2015

1 Isogenien

Definition. Seien E_1, E_2 elliptische Kurven. Eine *Isogenie* von E_1 nach E_2 ist ein Morphismus $\phi : E_1 \to E_2$, so dass $\phi(O) = O$ gilt. Zwei elliptische Kurven E_1, E_2 heißen *isogen*, wenn es eine nichtkonstante Isogenie von E_1 nach E_2 existiert. Wir sehen später, dass dies eine Äquivalenzrelation ist.

Da ein Morphismus zwischen Kurven stets konstant oder surjektiv ist, gilt für eine Isogenie $\phi : E_1 \to E_2$ entweder:

$$\phi(E_1) = \{O\} \quad \text{oder} \quad \phi(E_1) = E_2$$

Elliptische Kurven sind abelsche Gruppen, daher wird die Menge aller Isogenien $\mathrm{Hom}(E_1, E_2)$ von E_1 nach E_2 mit der komponentenweise Addition zu einer abelschen Gruppe. Ist $E = E_1 = E_2$, so wird $\mathrm{End}(E) = \mathrm{Hom}(E, E)$ zu einem Ring mit der komponentenweisen Addition und der Komposition als Multiplikation. (Wir werden das Distributivgesetz später zeigen.) $\mathrm{End}(E)$ heißt *Endomorphismenring* von E. Die Einheitengruppe $\mathrm{Aut}(E)$ von $\mathrm{End}(E)$ heißt *Automorphismengruppe* von E.

Satz 1. Seien E, E_1, E_2 elliptische Kurven.

(i) Sei $m \in \mathbb{Z},\ m \neq 0$. Die m-Multiplikation $[m] : E \to E$ ist nichtkonstant.

(ii) $\mathrm{Hom}(E_1, E_2)$ ist torsionsfreier $\mathbb{Z}$-Modul.

(iii) $\mathrm{End}(E)$ ist ein (nicht notwendig kommutativer) Ring der Charakteristik 0 und ist nullteilerfrei.

Beweis. (i) Wir werden dies nur für $\mathrm{char}(\overline{K}) \neq 2$ zeigen. Wir zeigen zunächst $[2] \neq [0]$. Ist $P = (x, y) \in E$ der Ordnung 2, so folgt aus der

Duplikationsformel[1]:

$$f(x) := 4x^3 + b_2x^2 + 2b_4x + b_6 = 0$$

Es gibt nur endlich viele solche Punkte P. Da $[m] \circ [n] = [mn]$, müssen wir die Aussage nur noch für den Fall m ungerade zeigen.

Verifiziere durch Polynomdivision, dass:

$$f \nmid g := x^4 - b_4x^2 - 2b_6x - b_8$$

Somit gibt es ein $x_0 \in \overline{K}$, so dass $f(x_0) = 0$, aber $g(x_0) \neq 0$. Wähle nun ein $y_0 \in \overline{K}$ mit $P_0 = (x_0, y_0) \in E$. Die Duplikationsformel liefert $[2]P_0 = O$. Somit hat E ein nichttrivialer Punkt der Ordnung 2. Für ungerade m gilt:

$$[m]P_0 = P_0 \neq O$$

(ii) Sei $\phi \in \mathrm{Hom}(E_1, E_2)$ und $m \in \mathbb{Z}$ mit $[m] \circ \phi = [0]$. Die Gradformel gibt uns $\deg([m]) \deg(\phi) = 0$. Somit ist nach (i) entweder $m = 0$ oder $\phi = [0]$.

(iii) Nach (ii) hat $\mathrm{End}(E)$ Charakteristik 0. Seien $\phi, \psi \in \mathrm{End}(E)$ mit $\phi \circ \psi = [0]$. Dann ist $\deg(\phi) \deg(\psi) = 0$ und somit $\phi = [0]$ oder $\psi = [0]$. □

Theorem 2. Isogenien sind Gruppenhomomorphismen.

Beweis. Sei $\phi : E_1 \to E_2$ eine o.B.d.A. nichtkonstante Isogenie. ϕ induziert ein Homomorphismus:

$$\phi_* : \mathrm{Pic}^0(E_1) \to \mathrm{Pic}^0(E_2), \ \Big[\sum n_P(P)\Big] \mapsto \Big[\sum n_P(\phi P)\Big]$$

Nun haben wir Gruppenisomorphismen $E_i \to \mathrm{Pic}^0(E_i), \ P \mapsto [(P) - (O)]$. Da $\phi(O) = O$, erhalten wir das folgende kommutative Diagramm:

$$\begin{array}{ccc} E_1 & \longrightarrow & \mathrm{Pic}^0(E_1) \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\phi_*} \\ E_2 & \longrightarrow & \mathrm{Pic}^0(E_2) \end{array}$$

Somit ist auch ϕ ein Gruppenhomomorphismus. □

[1] Für $P = (x, y) \in E$ gilt:

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

Definition. Sei E eine elliptische Kurve und $Q \in E$. Die *Q-Translationsabbildung* ist definiert als:

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

Die Abbildung τ_Q ist ein Isomorphismus, aber keine Isogenie falls $Q \neq O$.

Theorem 3. Sei $\phi : E_1 \to E_2$ eine nichtkonstante Isogenie.

(i) Für alle $Q \in E_2$ gilt $\#\phi^{-1}(Q) = \deg_{\mathrm{s}}(\phi)$.
Für alle $P \in E_1$ gilt $e_\phi(P) = \deg_{\mathrm{i}}(\phi)$.

(ii) Die folgende Abbildung ist ein Isomorphismus:

$$\theta : \ker(\phi) \to \mathrm{Aut}(\overline{K}(E_1)/\phi^*\overline{K}(E_2)),\ T \mapsto \tau_T^*$$

(iii) Sei ϕ separabel. Dann ist ϕ unverzweigt, d.h. $\#\ker(\phi) = \deg(\phi)$ und die Körpererweiterung $\overline{K}(E_1)/\phi^*\overline{K}(E_2)$ ist galoissch.

Beweis. (i) Wir haben schon gezeigt, dass $\#\phi^{-1}(Q) = \deg_{\mathrm{s}}(\phi)$ für fast alle $Q \in E_2$. Für beliebige $Q, Q' \in E_2$, können wir ein $R \in E_1$ wählen mit $\phi(R) = Q' - Q$. Da ϕ ein Homomorphismus ist, gibt es eine Bijektion:

$$\phi^{-1}(Q) \to \phi^{-1}(Q'),\ P \mapsto P + R$$

Dies zeigt die erste Aussage. Sei nun $P, P' \in E_1$ mit $\phi(P) = \phi(P') = Q$ und setze $R = P' - P$. Dann ist $\phi(R) = O$, also $\phi \circ \tau_R = \phi$. Es folgt aus der Tatsache, dass τ_R ein Isomorphismus ist:

$$e_\phi(P) = e_{\phi\circ\tau_R}(P) = e_\phi(\tau_R(P))e_{\tau_R}(P) = e_\phi(P')$$

Also haben alle Punkte in $\phi^{-1}(Q)$ den gleichen Verzweigungsindex. Es gilt:

$$\begin{aligned}\deg_{\mathrm{s}}(\phi)\deg_{\mathrm{i}}(\phi) = \deg(\phi) &= \sum_{P\in\phi^{-1}(Q)} e_\phi(P) \\ &= \#\phi^{-1}(Q)\cdot e_\phi(P) = \deg_{\mathrm{s}}(\phi)\cdot e_\phi(P)\end{aligned}$$

(ii) Ist $T \in \ker(\phi)$ und $f \in \overline{K}(E_2)$, so gilt:

$$\tau_T^*(\phi^* f) = (\phi \circ \tau_T)^* f = \phi^* f$$

Somit ist θ wohldefiniert. θ ist ein Homomorphismus, da $\tau_S \circ \tau_T = \tau_{S+T}$. Elementare Galoistheorie gibt uns:

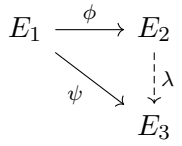
$$\#\,\mathrm{Aut}(\overline{K}(E_1)/\phi^*\overline{K}(E_2)) \leq \deg_{\mathrm{s}}(\phi) \overset{\text{(i)}}{=} \#\ker(\phi)$$

Somit reicht es zu zeigen, dass θ injektiv ist. Wenn τ_T^* ganz $\overline{K}(E_1)$ fixiert, so nimmt jede Funktion auf E_1 bei T und O den gleichen Wert an. Dies impliziert $T = O$. (Die Koordinatenfunktion x hat genau ein Pol bei O.)

(iii) Ist ϕ separabel, so folgt aus (i) $\#\ker(\phi) = \#\phi^{-1}(O) = \deg(\phi)$. Aus (ii) folgt:

$$\#\operatorname{Aut}(\overline{K}(E_1)/\phi^*\overline{K}(E_2)) = \deg(\phi) = [\overline{K}(E_1) : \phi^*\overline{K}(E_2)] \qquad \square$$

Korollar 4. Seien $\phi : E_1 \to E_2$ und $\psi : E_1 \to E_3$ nichtkonstante Isogenien und sei ϕ separabel. Gilt $\ker(\phi) \subset \ker(\psi)$, so gibt es eine eindeutig bestimmte Isogenie $\lambda : E_2 \to E_3$ mit $\psi = \lambda \circ \phi$:



Beweis. Da ϕ separabel ist, folgt aus (iii) des letzten Theorems, dass die Erweiterung $\overline{K}(E_1)/\phi^*\overline{K}(E_2)$ galoissch ist. Die Inklusion $\ker(\phi) \subset \ker(\psi)$ und die Identifikation in (ii) des letzten Theorems implizieren, dass jedes Element in $\operatorname{Gal}(\overline{K}(E_1)/\phi^*\overline{K}(E_2))$ stets $\psi^*\overline{K}(E_3)$ fixiert. Somit gibt es den Körperturm:

$$\psi^*\overline{K}(E_3) \subset \phi^*\overline{K}(E_2) \subset \overline{K}(E_1)$$

Kategorienäquivalenz gibt uns eine Abbildung $\lambda : E_2 \to E_3$ mit $\phi^* \circ \lambda^* = \psi^*$. Dies impliziert $\lambda \circ \phi = \psi$. Nun ist λ eine Isogenie, da $\lambda(O) = \lambda(\phi(O)) = \psi(O)$. $\square$

2 Die duale Isogenie

Theorem 5. Seien E, E' elliptische Kurven, ω ein invariantes Differential von E und seien $\phi, \psi : E' \to E$ Isogenien. Dann gilt:

$$(\phi + \psi)^*\omega = \phi^*\omega + \psi^*\omega$$

Satz 6. Seien C_1, C_2 Kurven und $\phi : C_1 \to C_2$ ein nichtkonstanter Morphismus. Dann ist ϕ genau dann separabel, wenn $\phi^* : \Omega_{C_2} \to \Omega_{C_1}$ injektiv (äquivalent: nicht null) ist.

Theorem 7. Sei $\phi : E_1 \to E_2$ eine nichtkonstante Isogenie vom Grad m.

(i) Es existiert eine eindeutig bestimmte Isogenie $\hat{\phi} : E_2 \to E_1$ mit:

$$\hat{\phi} \circ \phi = [m]$$

$\hat{\phi}$ heißt *duale Isogenie* zu ϕ. Ist $\phi = [0]$, so setzen wir $\hat{\phi} = [0]$.

(ii) Als Gruppenhomomorphismus ist $\hat{\phi}$ gerade die Komposition:

$$\begin{array}{ccccc} E_2 & \longrightarrow & \operatorname{Div}^0(E_2) & \xrightarrow{\phi^*} & \operatorname{Div}^0(E_1) \xrightarrow{\sigma} E_1 \\ Q & \longmapsto & (Q) - (O) & & \sum n_P(P) \longmapsto \sum [n_P]P \end{array}$$

Beweis. (i) Wir zeigen zunächst die Eindeutigkeit. Seien $\hat{\phi}$ und $\hat{\phi}'$ solche Isogenien. Dann gilt:

$$(\hat{\phi} - \hat{\phi}') \circ \phi = [m] - [m] = [0]$$

Da ϕ nichtkonstant ist, ist $\hat{\phi} - \hat{\phi}'$ konstant, also $\hat{\phi} = \hat{\phi}'$.

Sei nun $\psi : E_2 \to E_3$ eine nichtkonstante Isogenie vom Grad n und wir nehmen an, dass $\hat{\phi}$ und $\hat{\psi}$ existieren. Dann gilt:

$$(\hat{\phi} \circ \hat{\psi}) \circ (\psi \circ \phi) = \hat{\phi} \circ [n] \circ \phi = [n] \circ [m] = [nm]$$

Also ist $\widehat{\psi \circ \phi} = \hat{\phi} \circ \hat{\psi}$. Jeder Morphismus glatter Kurven über Körper positiver Charakteristik lässt sich als Komposition einer separablen Abbildung und einer Frobeniusabbildung schreiben. Wir müssen die Aussage nur für den Fall, dass ϕ separabel ist, und für den Fall, dass ϕ der Frobeniusmorphismus ist, beweisen.

1. Fall: ϕ ist separabel. Da ϕ vom Grad m ist, gilt nach Theorem 3 stets $\#\ker(\phi) = m$. Jedes Element in $\ker(\phi)$ hat eine Ordnung, das m teilt, d.h. $\ker(\phi) \subset \ker([m])$. Nach Korollar 4 gibt es eine Isogenie $\hat{\phi} : E_2 \to E_1$ mit $\hat{\phi} \circ \phi = [m]$.
2. Fall: ϕ ist der Frobeniusmorphismus. Sei $p = \mathrm{char}(K) > 0$. Wir können o.B.d.A. ϕ als p-te Potenz annehmen, also $\deg(\phi) = p$. Sei ω ein invariantes Differential von E_1. Aus Theorem 5 folgt:

$$[p]^*\omega = p\omega = 0$$

Aus Satz 6 folgt, dass $[p]$ nicht separabel ist. Wir können $[p] = \psi \circ \phi^e$ als Komposition einer separablen Isogenie ψ und ϕ^e mit $e \geq 1$ schreiben. Somit ist $\hat{\phi} = \psi \circ \phi^{e-1}$.

(ii) Sei $Q \in E_2$. Für ein beliebiges $P' \in \phi^{-1}(\phi)$ gilt:

$$\begin{aligned}
\sigma(\phi^*((Q) - (O))) &= \sum_{P \in \phi^{-1}(Q)} [e_\phi(P)]P - \sum_{T \in \phi^{-1}(O)} [e_\phi(T)]T \\
&\overset{3}{=} [\deg_{\mathrm{i}}(\phi)]\Big(\sum_{P \in \phi^{-1}(Q)} P - \sum_{P \in \phi^{-1}(Q)} (P - P')\Big) \\
&= [\deg_{\mathrm{i}}(\phi)] \circ [\#\phi^{-1}(Q)]P' \overset{3}{=} [\deg(\phi)]P'
\end{aligned}$$

Nach Konstruktion gilt $\hat{\phi}(Q) = \hat{\phi} \circ \phi(P') = [\deg(\phi)]P'$. □

Theorem 8. Sei $\phi : E_1 \to E_2$ eine Isogenie.

(i) Es gilt $\hat{\phi} \circ \phi = [\deg(\phi)]$ und $\phi \circ \hat{\phi} = [\deg(\phi)]$.

(ii) Ist $\lambda : E_2 \to E_3$ eine Isogenie, so gilt $\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}$.

(iii) Ist $\psi : E_1 \to E_2$ eine Isogenie, so gilt $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$.

(iv) Es ist $\widehat{[m]} = [m]$ und $\deg([m]) = m^2$.

(v) $\deg(\phi) = \deg(\hat{\phi})$ und $\hat{\hat{\phi}} = \phi$

Korollar 9. Sei E eine elliptische Kurve und $m \in \mathbb{Z},\ m \neq 0$.

(i) Ist $m \neq 0$ in K, so gilt $E[m] = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

(ii) Ist $\mathrm{char}(K) = p > 0$, so gilt eines der beiden Aussagen:

(a) Für alle $e \in \mathbb{N}$ gilt $E[p^e] = \{O\}$.

(b) Für alle $e \in \mathbb{N}$ gilt $E[p^e] = \mathbb{Z}/p^e\mathbb{Z}$.

Beweis. (i) $[m]$ ist separabel, da $[m]^*\omega = m\omega \neq 0$, wobei ω ein invariantes Differential von E ist (Satz 6). Nach Theorem 3 (iii) gilt:

$$\#E[m] = \#\ker([m]) = \deg([m]) = m^2$$

Für jedes $d \mid m$ gilt analog $\#E[d] = d^2$. Schreiben wir die endliche Gruppe $E[m]$ als Produkt von zyklischen Gruppen, so ist die einzige Möglichkeit $E[m] = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

(ii) Sei ϕ die p-Potenz Frobeniusmorphismus. Weil ϕ rein inseparabel ist, gilt:

$$\#E[p^e] = \#\ker([p^e]) \overset{3}{=} \deg_s[p^e] = \deg_s(\hat{\phi} \circ \phi)^e = \deg_s(\hat{\phi})^e$$

Es gilt $\deg(\hat{\phi}) = \deg(\phi) = p$, also gibt es zwei Fälle. Ist $\hat{\phi}$ inseparabel, so ist $\deg_s(\hat{\phi}) = 1$, also $\#E[p^e] = 1$ für alle e. Andernfalls ist $\hat{\phi}$ separabel und es gilt $\deg_s(\hat{\phi}) = p$ und $\#E[p^e] = p^e$ für alle e. Schreiben wir $E[p^e]$ als Produkt von zyklischen Gruppen, so ist die einzige Möglichkeit $E[p^e] = \mathbb{Z}/p^e\mathbb{Z}$. □