Ausarbeitung des Vortrags über Isogenien

Seminar zu Elliptischen Kurven bei Prof. Wingberg im Wintersemester 2012

Konrad Stuhrmann

November 2012

Es seien ab jetzt E, E_1, E_2 und E_3 stets elliptische Kurven mit Ursprüngen O, O_1, O_2 und O_3.

1. Isogenien

Zunächst werden Isogenien eingeführt und elementare Eigenschaften nachgewiesen.

1.1. Definition. Eine *Isogenie* ist ein Morphismus $\phi\colon E_1 \to E_2$ mit $\phi(O_1) = O_2$. Gibt es eine eine solche nichtkonstante Isogenie zwischen den Kurven E_1 und E_2, so heißen diese *isogen*.

1.2. Theorem. Isogenien sind Gruppenhomomorphismen. Genauer gesagt gilt die Darstellung einer Isogenie $\phi\colon E_1 \to E_2$ als $\phi = {\kappa_2}^{-1} \circ \phi_* \circ \kappa_1$, eine Verkettung von Gruppenhomomorphismen.

Beweis. Die erste Aussage folgt selbstverständlich aus der zweiten. Für diese kommen die Gruppenisomorphismen für elliptische Kurven auf deren Picard-Gruppen zum Einsatz:

$$\kappa_1\colon E_1 \xrightarrow{\sim} \mathrm{Pic}^0(E_1),\ P \mapsto [(P) - (O_1)] \quad \text{und} \quad \kappa_2\colon E_2 \xrightarrow{\sim} \mathrm{Pic}^0(E_2),\ P \mapsto [(P) - (O_2)]$$

sowie auch der Pushforward von ϕ auf den Divisoren – ein Gruppenhomomorphismus, welcher sich auf die Picard-Gruppen einschränken lässt:

$$\phi_*\colon \mathrm{Pic}^0(E_1) \to \mathrm{Pic}^0(E_2),\ [(P) - (O_1)] \mapsto [(\phi P) - (\phi O_1)]$$

Wegen $\phi(O_1) = (O_2)$ ist nun für jeden Punkt $P \in E_1$:

$$({\kappa_2}^{-1} \circ \phi_* \circ \kappa_1)(P) = ({\kappa_2}^{-1} \circ \phi_*)\big([(P) - (O_1)]\big) = {\kappa_2}^{-1}\big([(\phi P) - (O_2)]\big) = \phi(P)$$

Also ist $\phi = {\kappa_2}^{-1} \circ \phi_* \circ \kappa_1$ und die Aussage gezeigt. ∎

1.3. Ein noch aufzuwertendes Korollar.

(a) $\mathrm{Hom}(E_1, E_2) = \{\phi\colon E_1 \to E_2;\ \phi \text{ Isogenie}\}$ wird durch punktweise Addition zum $\mathbb{Z}$-Modul.

(b) $\mathrm{End}(E) = \mathrm{Hom}(E, E)$ ist mit der Addition von Isogenien und $\circ$ als Multiplikation ein nullteilerfreier Ring.

(c) Die Abbildung $[\,]\colon \mathbb{Z} \to \mathrm{End}(E),\ m \mapsto [m]$ ist ein Ringhomomorphismus.

Beweis. Aussage (a) und Aussage (c) sind klar, genauso Aussage (b) bis auf das Distributivgesetz nach Multiplikation von links und die Nullteilerfreiheit. Dass das Distributivgesetz gilt, rührt gerade daher, dass Isogenien Gruppenhomomorphismen sind. Für $\phi, \psi \in \mathrm{End}(E)$ mit $\psi \neq [0]$ folgt aus $\phi \circ \psi = [0] = [0] \circ \psi$ nach Kürzung rechts mit dem – da nichtkonstant – surjektiven ψ, dass schon ϕ Null sein muss: Der Ring ist nullteilerfrei. ∎

1.4. Wichtige Beispiele von Isogenien.

(a) Die *Multiplikation* $[m]\colon E \to E$ mit $m \in \mathbb{Z}$, definiert als m-faches Addieren in E.

(b) *Komplexe Multiplikation*, z. B. $[i]\colon (x, y) \mapsto (-x, iy)$ für $E\colon\ y^2 = x^3 - x$ bei $\mathrm{char}\, K \neq 2$, wobei $i = \sqrt{-1} \in \overline{K}$.

(c) Der *Frobenius-Morphismus*. Ist $\mathrm{char}\, K = p > 0$ und $q = p^r$, so ist $E^{(q)}$ eine elliptische Kurve, da sie per definitionem der Weierstraßgleichung von E mit um q potenzierte Koeffizienten genügt und $\Delta(E^{(q)}) = \Delta(E)^q \neq 0$. Der Frobenius-Morphismus

$$\phi_q\colon E \to E^{(q)},\ (X : Y : Z) \mapsto (X^q : Y^q : Z^q)$$

ist daher eine Isogenie. Als Morphismus ist er rein inseparabel von Grad q. Siehe auch Proposition A.5.

(d) *Translationen* $\tau_Q\colon E \to E,\ P \mapsto P + Q$ um $Q \in E$ sind für $Q \neq O_2$ *keine* Isogenien,

(e) aber für Morphismen $F\colon E_1 \to E$ ist dann $\phi = \tau_Q \circ F$ mit $Q = -F(O_1)$ eine Isogenie.

1.5. Definition. Für $m \in \mathbb{Z}, m \neq 0$ heißt $E[m] = \ker[m] = \{P \in E;\ [m]P = 0\}$ die *m-Torsionuntergruppe* und $E_{\mathrm{tors}} = \bigcup_{m \in \mathbb{N}} E[m]$ die *Torsionsuntergruppe* von E. Das sind die Punkte der Ordnung m bzw. endlicher Ordnung in E. Außerdem sei $E_{\mathrm{tors}}(K) = E_{\mathrm{tors}} \cap E(K)$.

1.6. Proposition. Die Multiplikation $[m]\colon E \to E$ mit $m \in \mathbb{Z}, m \neq 0$ ist eine nichtkonstante Isogenie.

Beweis. Weil die Endomorphismen auf E einen nullteilerfreien Ring bilden, reicht zu zeigen, dass

(A) $[2] \neq [0]$, und

(B) $[m] \neq [0]$ für ungerade $m \in \mathbb{Z}$.

Dazu sei E ohne Einschränkung durch eine Weierstraßgleichung $E\colon\ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ gegeben. Für Punkte $P = (x, y) \in E$ liefert die Verdopplungsformel

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

wobei $x([2]P)$ die erste Komponente von P bezeichne. Daher ist $[2]P = O = [0 : 1 : 0]$ genau dann der Fall, wenn x im Nennerpolynom echt höher verschwindet als im Zählerpolynom.

Aussage (A): Ist das Nennerpolynom ein von Null verschiedenes, so kann es nur endlich viele solche $x \in \overline{K}$ geben, welche ebendort verschwinden. Ersteres ist aber sicherlich der Fall, es sei denn $\operatorname{char} K = 2$ und $b_2 = b_6 = 0$. Dann aber wäre $\Delta(E) = -{b_2}^2 b_8 - 8{b_4}^3 - 27{b_6}^2 + 9b_2b_4b_6 = 0$, und die *elliptische* Kurve E somit singulär – was ausgeschlossen ist. Es gibt also auf alle Fälle ein $x \in \overline{K}$, welches im Nenner der Verdopplungsformel nicht verschwindet. Da $\overline{K}$ algebraisch abgeschlossen ist, muss es ein y geben, welches zusammen mit x der Weierstraßgleichung von E genügt. Also gibt es einen Punkt P auf E mit $[2]P \neq O$, was $[2] \neq [O]$ impliziert.

Aussage (B): Falls $\operatorname{char} K \neq 2$, bedingt $\Delta(E) \neq 0$, dass – wie eine Polynomdivision zeigt – in der Verdopplungsformel das Zählerpolynom kein Vielfaches des Nennerpolynoms ist, weswegen es ein $x_0 \in \overline{K}$ geben muss, welches im Nenner echt höher verschwindet als im Zähler. Zu einem solchen gibt es wieder einmal ein $y_0 \in \overline{K}$, sodass $P_0 = (x_0, y_0)$ ein Punkt auf E ist, nun nämlich der Ordnung 2 laut Verdopplungsformel, d. h. $[2]P_0 = O$. Dann aber ist für $m \in \mathbb{Z}$ ungerade $[m]P_0 = P_0 \neq O$, da das gefundene P_0 im affinen Teil liegt, was letztendlich $[m] \neq [0]$ für ungerade $m \in \mathbb{Z}$ impliziert. Zumindest bei $\operatorname{char} K \neq 2$, für $\operatorname{char} K = 2$ sei auf Korollar 2.4 verwiesen. Ansonsten lässt sich auch dieser Fall mit fast derselben Argumentation unter Zuhilfenahme einer herleitbaren Verdreifachungsformel beweisen. ∎

1.3. Die Aufwertung des vorherigen Korollars mithilfe von Proposition 1.6.

(a) $\operatorname{Hom}(E_1, E_2) = \{\phi\colon E_1 \to E_2;\ \phi \text{ Isogenie}\}$ ist ein *torsionsfreier* $\mathbb{Z}$-Modul.

(b) $\operatorname{End}(E) = \{\phi\colon E \to E;\ \phi \text{ Isogenie}\}$ ist ein nullteilerfreier Ring der *Charakteristik* 0.

(c) Die Abbildung $[\,]\colon \mathbb{Z} \to \operatorname{End}(E),\ m \mapsto [m]$ ist ein *injektiver* Ringhomomorphismus.

1.7. Theorem. Sei $\phi\colon E_1 \to E_2$ eine nichtkonstante Isogenie. Dann gilt:

(a) Für jedes $Q \in E_2$ ist $\#\phi^{-1}(Q) = \deg_s \phi$.

(b) Für jedes $P \in E_1$ ist $e_\phi(P) = \deg_i \phi$.

(c) Die Abbildung $\ker\phi \to \operatorname{Aut}\left(\overline{K}(E_1)/\phi^*\overline{K}(E_2)\right),\ T \mapsto {\tau_T}^*$ ist ein Isomorphismus.

(d) Ist ϕ separabel, so ist ϕ unverzweigt mit $\#\ker\phi = \deg\phi$ und $\overline{K}(E_1)/\phi^*\overline{K}(E_2)$ galoissch.

Beweis. Aussage (a): Seien $Q, Q' \in E_2$ und $R \in E_1$ mit $\phi(R) = Q' - Q$. Ein solches R gibt es, da ϕ surjektiv ist. Wegen $\forall P \in \phi^{-1}(Q)\colon\ \phi(P+R) = \phi(P) + \phi(R) = Q'$ ist $\tau_R|\,\phi^{-1}(Q) \to \phi^{-1}(Q')$ eine wohldefinierte Bijektion zwischen den Fasern von Q und Q' mit Umkehrung τ_{-R}, insb. sind alle Fasern gleichmächtig, womit aufgrund Proposition A.3(a) die Aussage folgt.

Aussage (b): Sei $P \in E_1, Q = \phi(P)$. Für ein beliebiges weiteres $P' \in E_1$ mit $\phi(P') = Q = \phi(P)$ setze $R = P' - P$. Dann ist $\phi(R) = 0$, also $\phi \circ \tau_R = \phi$ und daher:

$$e_\phi(P) = e_{\phi\circ\tau_R}(P) \overset{\text{A.3(c)}}{=} e_{\tau_R}(P)e_\phi(\tau_R(P)) = e_\phi(P'),$$

denn τ_R ist invertierbar und verzweigt wegen Proposition A.3(b) nicht. Folglich verzweigt ϕ in $\phi^{-1}(Q)$ überall gleich und es gilt:

$$\deg_s \phi \cdot \deg_i \phi = \deg \phi \overset{\text{A.3(b)}}{=} \sum_{P' \in \phi^{-1}Q} e_\phi(P') = \sum_{P' \in \phi^{-1}(Q)} e_\phi(P) = \#\phi^{-1}(Q) \cdot e_\phi(P) = \deg_s \phi \cdot e_\phi(P)$$

Nach Kürzen mit $\deg_s \phi \neq 0$ folgt die Aussage.

Aussage (c): Die in Frage stehende Abbildung ist wohldefiniert, da für $T \in \ker \phi$:

$$\forall f \in \overline{K}(E_2)\colon\ \tau_T{}^*(\phi^* f) = (\phi \circ \tau_T)^* f = \phi^* f,$$

denn $\phi \circ \tau_T = \phi$. Somit ist in der Tat $\tau_T{}^* \in \operatorname{Aut}\left(\overline{K}(E_1)/\phi^*\overline{K}(E_2)\right)$. Die Abbildung ist ein Gruppenhomomorphismus:

$$\forall T, S \in \ker \phi\colon\ (\tau_{S+T})^* = (\tau_T \circ \tau_S)^* = \tau_S{}^* \circ \tau_T{}^*$$

Zu zeigen bleibt die Bijektivität der Abbildung, welche schon aus ihrer Injektivität folgen wird, denn:

$$\#\ker \phi \overset{\text{(a)}}{=} \deg_s \phi \geqslant \#\operatorname{Aut}\left(\overline{K}(E_1)/\phi^*\overline{K}(E_2)\right)$$

Sei also $T \in \ker \phi$, sodass $\tau_T{}^* = \mathrm{id}_{\overline{K}(E_1)}$. Dann:

$$\forall f \in \overline{K}(E_1)\colon\ f(O_1) = \tau_T{}^* f(O_1) = f(\tau_T(O_1)) = f(T)$$

Also ist schon $T = O_1$, der Homomorphismus hat also trivialen Kern und ist injektiv.

Aussage (d): Ist ϕ separabel, so ist ϕ nach (b) unverzweigt und

$$\deg \phi \overset{\text{(a)}}{=} \#\ker \phi \overset{\text{(c)}}{=} \#\operatorname{Aut}\left(\overline{K}(E_1)/\phi^*\overline{K}(E_2)\right).$$

Daher ist $\overline{K}(E_1)/\phi^*\overline{K}(E_2)$ galoissch. ∎

1.8. Korollar. Seien $\phi\colon E_1 \to E_2$ und $\psi\colon E_1 \to E_3$ nichtkonstante Isogenien. Ist ϕ separabel mit $\ker \phi \subseteq \ker \psi$, so gibt es eine eindeutige Isogenie $\lambda\colon E_2 \to E_3$ mit $\psi = \lambda \circ \phi$.

Beweis. Aus Theorem 1.7 (d) folgt bei separablem ϕ, dass $\overline{K}(E_1)/\phi^*\overline{K}(E_2)$ galoissch ist. Wegen $\ker \phi \subseteq \ker \psi$ folgt mit Theorem 1.7 (c) $\operatorname{Aut}\left(\overline{K}(E_1)/\phi^*\overline{K}(E_2)\right) \subseteq \operatorname{Aut}\left(\overline{K}(E_1)/\psi^*\overline{K}(E_3)\right)$, was heißt, dass $\psi^*\overline{K}(E_3) \subseteq \phi^*\overline{K}(E_2) \subseteq \overline{K}(E_1)$. Nach Theorem A.1(c) gibt es eine entsprechende rationale Abbildung

$$\lambda\colon E_2 \to E_3, \quad \text{sodass} \quad \phi^*\left(\lambda^*\overline{K}(E_3)\right) = \psi^*\overline{K}(E_3),$$

was $\lambda \circ \phi = \psi$ impliziert. Da außerdem $\lambda(O_2) = \lambda \circ \phi(O_1) = \psi(O_1) = O_3$, ist λ eine Isogenie. Die Eindeutigkeit folgt wieder aus der Surjektivität von φ. ∎

1.9. Proposition. Für jede endliche Untergruppe $\Phi \subseteq E$ gibt es eine eindeutige elliptische Kurve E' und eine separable Isogenie $\phi\colon E \to E'$ mit $\ker \phi = \Phi$.

Beweis. Sei $\overline{K}(E)^{\Phi} = \left\{ f \in \overline{K}(E);\ \forall T \in \Phi\colon\ {\tau_T}^* f = f \right\}$ der von Φ über die Wirkung $\mathrm{T} \mapsto \tau_T$ fixierte Unterkörper von $\overline{K}(E)$. Die Erweiterung $\overline{K}(E)/\overline{K(E)}^{\Phi}$ ist galoissch mit Galoisgrupee Φ und insb. eine endliche Erweiterung. Daher liefert Theorem A.1(d) eine eindeutige glatte Kurve $C/\overline{K}$ und einen Morphismus

$$\phi\colon E \to C, \quad \text{mit} \quad \phi^*\overline{K}(C) = \overline{K}(E)^{\Phi}$$

Für beliebige $P \in E, T \in \Phi$ gilt:

$$\forall f \in \overline{K}(C)\colon\ f(\phi(P+T)) = {\tau_T}^*(\phi^* f)(P) \overset{T \in \Phi}{=} \phi^* f(P) = f(\phi(P)),$$

also auch schon $\phi(P+T) = \varphi(P)$. Sei nun $Q \in C$ beliebig und $P \in E$ mit $\phi(P) = Q$. Dann ist einerseits

$$\phi^{-1}(Q) \supseteq \left\{ P+T;\ T \in \Phi \right\} \quad \text{und andererseits} \quad \#\phi^{-1}(Q) \leqslant \deg\phi = \#\Phi$$

Also, da τ_P bijiziert, ist $\#\phi^{-1}(Q) = \#\Phi = \deg\phi$ und wegen Proposition A.3(b) ist also ϕ unverzweigt. Die Formel von Riemann-Hurwitz liest sich nun:

$$2\mathrm{genus}(E) - 2 = \deg\phi \cdot (2\mathrm{genus}(C) - 2).$$

Weil ϕ nichtkonstant ist und die elliptische Kurve E Genus 1 hat, ist auch C von Genus 1 und elliptisch. Nun ist $E' = (C, \varphi(O))$ eine elliptische Kurve, auf welche ϕ dank der Wahlfreiheit des Ursprungs nun isogen abbildet. Da ϕ nicht verzweigt, ist diese Isogenie außerdem separabel. ∎

2. Das Invariante Differential

Ist nun E: $y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$ mit $a_i \in K$ für $i = 1, \ldots, 6$, so heißt $\omega = \frac{\mathrm{d}x}{2y+a_1x+a_3} \in \Omega_E$ das *invariante Differential* auf E. Dieses ist überall regulär und nirgends verschwindend.

2.1. Proposition. Für jedes $Q \in E$ ist $\tau_Q^*\omega = \omega$, es ist also unter Translation invariant.

Beweis. Die Differentiale Ω_E auf E sind ein eindimensionaler $\overline{K}(E)$-Vektorraum. Für ein beliebiges $Q \in E$ gibt es also schon mal ein $a_Q \in \overline{K}(E)$ mit ${\tau_Q}^*\omega = a_Q\omega$. Dabei ist $a_Q \neq 0$, denn mit τ_Q ist auch ${\tau_Q}^*$ invertierbar und annulliert sicher nicht $\omega \neq 0$. Jedoch erhält man aus $\mathrm{div}(\omega) = 0$ das Folgende:

$$\mathrm{div}(a_Q) = \mathrm{div}({\tau_Q}^*\omega) - \mathrm{div}(\omega) = {\tau_Q}^*\,\mathrm{div}(\omega) - \mathrm{div}(\omega) = 0$$

Das bedeutet, dass a_Q konstant sein muss. Der Wert von a_Q hängt rational von den Komponenten $x(Q), y(Q)$ von Q ab: Denn in ${\tau_Q}^*\omega = \frac{\mathrm{d}(x\circ\tau_Q)}{2(y\circ\tau_Q)+a_1(x\circ\tau_Q)+a_3}$ tauchen im Wesentlichen $x \circ \tau_Q \in \overline{K}(x, y)$ und $y \circ \tau_Q \in \overline{K}(x, y)$ auf. Nun ist jedoch die Abbildung $f\colon E \to \mathbf{P}^1,\ Q \mapsto [a_Q : 1]$ nicht surjektiv – sie lässt etwa $[1 : 0]$ aus – aber rational, kann also nur ein konstanter Morphismus sein. So kann man schließen: $\forall Q \in E\colon\ a_Q = a_O$, und wegen $a_O = 1$ folgt die Behauptung. ∎

2.2. Theorem. Für Isogenien $\phi, \psi\colon E_1 \to E$ ist $(\phi + \psi)^*\omega = \phi^*\omega + \psi^*\omega$.

Beweis. Das wird in [Sil, III. §5., Theorem 5.2] bewiesen. ∎

2.3. Korollar. Für $m \in \mathbb{Z}$ ist $[m]^*\omega = m\omega$.

Beweis. Bei $m = 0$ und $m = 1$ ist das klarerweise erfüllt. Eine Induktion nach $m \in \mathbb{Z}$ unter Ausnutzung von $[m+1]^*\omega \overset{2.2}{=} [m]^*\omega + [1]^*\omega$ und $[m-m]^*\omega \overset{2.2}{=} [m]^* + [-m]^*\omega$ erschließt die vollständige Behauptung ∎

2.4. Korollar. Die Multiplikation $[m]\colon E \to E$ mit $m \in \mathbb{Z}, m \neq 0$ ist ein nichtkonstanter, separabler Morphismus, falls $\operatorname{char} K \nmid m$.

Beweis. Sei $m \in \mathbb{Z}, m \neq 0$. Falls $\operatorname{char} K \nmid m$, ist $[m]^*\omega \overset{2.3}{=} m\omega \neq 0$. Also kann $[m]$ nicht Null sein und ist separabel nach Proposition A.7(c). ∎

2.5. Korollar. Für $\operatorname{char} K = p > 0$ sei E über $\mathbb{F}_q$ definiert und $\phi\colon E \to E$ der q-Frobenius-Morphismus mit $q = p^r$. Für $m, n \in \mathbb{Z}$ ist die Abbildung $[m] + [n] \circ \phi\colon E \to E$ genau dann separabel, wenn $p \nmid m$. Insbesondere ist die Abbildung $1 - \phi$ separabel.

Beweis. Wegen Theorem 2.2 und Korollar 2.3 ist für $m, n \in \mathbb{Z}$:

$$([m] + [n] \circ \phi)^*\omega = m\omega + n\phi^*\omega \overset{\text{A.7(c)}}{=} m\omega$$

Aber genau dann ist $m\omega = 0$, wenn $p \mid m$. Wegen Proposition A.7(c) folgt die Behauptung. ∎

3. Die Duale Isogenie

3.1. Theorem. (a) Zu jeder nichtkonstanten Isogenie $\phi\colon E_1 \to E_2$ von Grad m gibt es eine eindeutige Isogenie $\widehat{\phi}\colon E_, \to E_1$, sodass $\widehat{\phi} \circ \phi = [m]$.

3.2. Definition. Diese Isogenie $\widehat{\phi}$ heißt die zu ϕ *duale Isogenie*. Im Fall $\phi = 0$ setzt man $\widehat{\phi} = 0$.

3.1. Theorem. (b) Die zu ϕ duale Isogenie ist gegeben durch $\widehat{\phi} = \kappa_1^{-1} \circ \phi^* \circ \kappa_2$.

Beweis. Zunächst wird Teil (b) bewiesen, nämlich unter der Annahme der Existenz von dualen Isogenien. Sei $P \in E_1$ beliebig und $Q = \phi(P)$. Nun wird P unter $\kappa_1 \circ \phi^* \circ \kappa_2 \circ \varphi$ verfolgt.

$$\begin{aligned}
\phi^* \circ \phi_*\big((P) - (O_1)\big) = \phi^*\big((Q) - (O_2)\big) &\overset{\text{A.7(b)}}{=} \sum_{P' \in \phi^{-1}(Q)} e_\phi(P')(P') - \sum_{T' \in \phi^{-1}(O_2)} e_\phi(T')(T') \\
&\overset{1.7(b)}{=} \deg_i \phi \cdot \Big(\sum_{T \in \ker \phi} (P+T) - \sum_{T \in \ker \phi} (T) \Big),
\end{aligned}$$

Es wird verwendet, dass ϕ überall gleichverzweigt, dass Fasern von Isogenien Translate des Kerns sind und $\phi(O_1) = O_2$. Jetzt außerdem noch $\#\ker\phi = \deg_s \phi$:

$$\begin{aligned}(\kappa_1 \circ \phi^* \circ \kappa_2 \circ \varphi)(P) &= ({\kappa_1}^{-1} \circ \phi^* \circ \kappa_2 \circ {\kappa_2}^{-1} \circ \phi_* \circ \kappa_1)(P)\\ &= ({\kappa_1}^{-1} \circ \phi^* \circ \phi_* \circ \kappa_1)(P)\\ &= [\deg_i \phi]\Big(\sum_{T\in\ker\phi} P + T - \sum_{T\in\ker\phi} T\Big)\\ &= [\deg_i \phi] \circ [\deg_s \phi](P)\\ &= [\deg \phi](P) = (\widehat{\phi} \circ \phi)(P)\end{aligned}$$

Da $P \in E_1$ beliebig war: $\kappa_1 \circ \phi^* \circ \kappa_2 \circ \varphi = \widehat{\phi} \circ \phi$. Abermaliges Rechtskürzen des nichtkonstanten ϕ liefert dann die Behauptung.

Nun zu (a), der Existenz einer dualen Isogenie, deren Eindeutigkeit wieder durch Rechtskürzen folgt. Die erste Beobachtung ist, dass für gefundene duale Isogenien $\widehat{\phi}$ und $\widehat{\psi}$ von φ und einer weiteren Isogenie $\psi\colon E_2 \to E_3$ die Komposition $\widehat{\varphi} \circ \widehat{\psi}$ eine duale Isogenie zu $\psi \circ \varphi$ liefert:

$$(\widehat{\phi} \circ \widehat{\psi}) \circ (\psi \circ \phi) = \widehat{\phi} \circ [\deg\psi] \circ \phi = [\deg\psi] \circ [\deg\varphi] = [\deg\psi \circ \phi]$$

Gemäß Korollar A.6 reicht es daher, die Existenz von dualen Isogenien zu separablen Isogenien einerseits, zu Frobenius-Morphismen andererseits zu zeigen.

Falls ϕ separabel ist, folgt mit Theorem 1.7 (a) $\#\ker\phi = m$, also auch $\ker\phi \subseteq \ker[m]$. Wegen Korollar 1.8 gibt es daher auch ein $\widehat{\phi}\colon E_2 \to E_1$ mit $\widehat{\phi} \circ \phi = [m]$, also eine duale Isogenie.

Falls ϕ der q-Frobenius-Morphismus ist, etwa $q = p^r$ bei $\operatorname{char} K = p > 0$, so ist dieser eine r-fache Komposition des einfachen p-Frobenius-Morphismus. Mit dem Argument von oben über die Komposition von dualen Isogenien reicht es also, allein letzteren zu betrachten. Sei also ohne Einschränkung $r = 1$ und ϕ der p-Frobenius-Morphismus. Wegen $[p]^*\omega = p\omega = 0$ folgt aus Proposition A.7(c), dass $[p]$ inseparabel ist, also gibt es laut Korollar A.6 ein $e \in \mathbb{N}$ und eine separable Isogenie $\psi\colon E^{(p^e)} \to E$ mit $[p] = \psi \circ \phi^e$. Dann aber definiert $\widehat{\phi} = \psi \circ \phi^{e-1}$ eine zu ϕ duale Isogenie. ∎

3.3. Theorem. Sei $\phi\colon E_1 \to E_2$ eine Isogenie.

(a) Dann ist $\widehat{\phi} \circ \phi = [\deg\phi]$ auf E_1, und $\phi \circ \widehat{\phi} = [\deg\phi]$ auf E_2.
(b) Mit einer weiteren Isogenie $\lambda\colon E_2 \to E_3$ ist $\widehat{\lambda \circ \phi} = \widehat{\phi} \circ \widehat{\lambda}$.
(c) Mit einer anderen Isogenie $\psi\colon E_1 \to E_2$ ist $\widehat{\phi + \psi} = \widehat{\phi} + \widehat{\psi}$.
(d) Für jedes $m \in \mathbb{Z}$ ist $\widehat{[m]} = [m]$ und $\deg[m] = m^2$.
(e) Es ist $\deg\widehat{\phi} = \deg\phi$.
(f) Es ist $\widehat{\widehat{\phi}} = \phi$.

Beweis. Für konstante Isogenien werden die Aussagen trivial, daher seien alle auftretenden Isogenien nichtkonstant. Dass die Isogenie ϕ nichtkonstant ist, impliziert dabei auch dasselbe für ihre duale $\widehat{\phi}$.

(a): Die erste Aussage gilt per definitionem, die zweite folgt aus $\phi \circ \widehat{\phi} \circ \phi = \phi \circ [\deg \phi] = [\deg \phi] \circ \phi$ durch eine erneute Kürzung rechts.

(b) Das ist schon im Existenzbeweis von dualen Isogenien in Theorem 3.1 mitbewiesen worden:

$$(\widehat{\phi} \circ \widehat{\lambda}) \circ (\lambda \circ \phi) = \widehat{\phi} \circ [\deg \lambda] \circ \phi = [\deg \lambda] \circ [\deg \phi] = [\deg \lambda \circ \phi]$$

Die Identität $\widehat{\phi} \circ \widehat{\lambda} = \widehat{\lambda \circ \phi}$ folgt aus der Eindeutigkeit einer dualen Isogenie.

(c) Seien $x_1, y_1 \in K(E_1)$ sowie $x_2, y_2 \in K(E_2)$ Weierstraß-Koordinaten. Nun ist E_2 auch eine elliptische Kurve über dem Körper $K(x_1, y_1$. Da $\phi\colon E_1 \to E_2$ und $\psi\colon E_1 \to E_2$ Morphismen sind, muss $\phi(x_1, y_1) = \phi \circ (x_1, y_1)\colon E_1 \to E_2$ selbst ein Punkt auf $E_2(K(x_1, y_1))$ sein, und ebenso mit ψ und $\phi + \psi$. Der Divisor:

$$D = ((\phi + \psi)(x_1, y_1) - (\phi(x_1, y_1)) - (\psi(x_1, y_1)) + (O) \in \mathrm{Div}_{K(x_1, y_1)}(E_2)$$

ist ein Hauptdivisor, da sich sowohl seine Punkte als auch seine Koeffizienten auf Null summieren. Es gibt also eine Funktion

$$f \in K(x_1, y_1)(E_2) = K(x_1, y_1, x_2, y_2),$$

welche als Funktion $f\colon E_2(K(x_1, y_1)) \to K(x_1, y_2)$ gerade den Divisor D hat.

Nun lässt sich diese auch als Funktion $f\colon E_1(K(x_2, y_2)) \to K(x_2, y_2)$ interpretieren. Betrachtet man ihren Divisor, so sieht man, dass f als Funktion auf E_2 einen Pol in $\phi(x_1, y_1)$ hat, also als Funktion auf E_1 auch einen Pol derselben Ordnung in jedem P mit $\phi(P) = (x_2, y_2)$. Weiterhin ist $\mathrm{ord}_{P_1}(f) = e_\phi(P_1)$. Ganz analog hat f einen Pol in P_1 falls $\psi(P_1) = (x_2, y_2)$ und eine Nullstelle in P_1, falls $\varphi + \psi(P_1) = (x_2, y_2)$. Daher ist der Divisor von f als Funktion auf E_1 von der Form:

$$(\phi + \psi)^*((x_2, y_2)) - \phi^*((x_2, y_2)) - \psi^*((x_2, y_2)) + \sum n_i(P_i) \in \mathrm{Div}_{\overline{K(x_2, y_2)}}(E_1),$$

wobei die Punkte P_i in $E_1(\overline{K})$ liegen. Da dies ein Hauptdivisor ist, summieren sich seine Punkte auf O_1 auf. Nach Theorem 3.1 (b) folgt also:

$$(\widehat{\phi + \psi})(x_2, y_2) - \widehat{\phi}(x_2, y_2) - \widehat{\psi}(x_2, y_2)$$

schon konstant sein muss. Da die Funktion für O_2 wiederum O_2 annimmt, folgt:

$$\widehat{\phi + \psi} = \widehat{\phi} + \widehat{\psi},$$

was zu zeigen war.

(d) Die Aussage gilt klarerweise für $m = 0$ und $m = 1$. Mithilfe von (c) folgt die Behauptung bei positiven $m \in \mathbb{Z}$ induktiv über $\widehat{[m+1]} = \widehat{[m]} + \widehat{[1]}$ und wird für die negativen durch $[0] = \widehat{[m-m]} = \widehat{[m]} + \widehat{[-m]}$ geliefert. Deswegen gilt auch $\big[\deg[m]\big] = \widehat{[m]} \circ [m] = [m] \circ [m] = [m^2]$. Aus der Injektivität von $[\,]$ folgt $\deg[m] = m^2$.

(e) Sei $m = \deg \phi$. Mithilfe von (d) ist

$$[m^2] = \left[\deg [m]\right] = [\deg \widehat{\phi} \circ \phi] = [\deg \phi \cdot \deg \widehat{\phi}] = [m \deg \widehat{\phi}]$$

Wieder aus der Injektivtät von [ ] folgt $\deg \widehat{\phi} = m$.

(f) Dies folgt aus $\widehat{\widehat{\phi}} \circ \widehat{\phi} = [\deg \widehat{\phi}] \overset{\text{(e)}}{=} [\deg \phi] \overset{\text{(a)}}{=} \phi \circ \widehat{\phi}$, denn $\widehat{\phi}$ ist ja nichtkonstant. ∎

3.4. Definition. Eine *quadratische Form* auf einer abelschen Gruppe A ist eine Abbildung $d\colon A \to \mathbb{R}$, sodass:

(i) $\forall \alpha \in A\colon\ d(\alpha) = d(-\alpha)$.

(ii) Die Paarung $A \times A \to \mathbb{R},\ (\alpha, \beta) \mapsto d(\alpha + \beta) - d(\alpha) - d(\beta)$ ist bilinear.

Eine solche heißt *positiv definit*, falls:

(iii) $\forall \alpha \in A\colon\ d(\alpha) \geqslant 0$.

(iv) $\forall \alpha \in A\colon\ d(\alpha) = 0 \Leftrightarrow \alpha = 0$.

3.5. Korollar. Der Grad $\deg\colon \mathrm{Hom}(E_1, E_2) \to \mathbb{R}$ ist eine positiv definite quadratische Form.

Beweis. Zu zeigen ist lediglich die Bilinearität der Paarung:

$$\langle \cdot, \cdot \rangle\colon \mathrm{Hom}(E_1, E_2) \times \mathrm{Hom}(E_1, E_2) \to \mathbb{R},\ (\varphi, \psi) \mapsto \deg(\varphi + \psi) - \deg \varphi - \deg \psi$$

Da $[\,]\colon \mathbb{Z} \to \mathrm{End}(E)$ injektiver Ringhomomorphismus ist und $\deg|\ \mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$, kann man stattdessen $[\langle \cdot, \cdot \rangle] = [\,] \circ \langle \cdot, \cdot \rangle$ betrachten.

$$\begin{aligned} \forall \phi, \psi \in \mathrm{Hom}(E_1, E_2)\colon\ [\langle \varphi, \psi \rangle] &= [\deg(\phi + \psi)] - [\deg \phi] - [\deg \psi] \\ &= (\widehat{\phi + \psi}) \circ (\varphi + \psi) - \widehat{\phi} \circ \phi - \widehat{\psi} \circ \psi \\ &\overset{3.3(c)}{=} \widehat{\phi} \circ \psi + \widehat{\psi} \circ \phi \end{aligned}$$

Der letzte Ausdruck ist aber bilinear in ϕ und ψ. Und so sind $[\langle \cdot, \cdot \rangle]$ und $\langle \cdot, \cdot \rangle$ bilinear. ∎

3.6. Korollar. (a) Für $m \in \mathbb{Z}, m \neq 0$, sodass $\mathrm{char}\, K \nmid m$, ist $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

(b) Bei $\mathrm{char}\, K = p$ ist entweder $E[p^e] \cong 0\ \forall e \in \mathbb{N}$ oder $E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z}\ \forall e \in \mathbb{N}$.

Beweis. (a): Korollar 2.4 sagt, $[m]$ ist in diesem Fall separabel. Wegen $\deg[m] = m^2$ gibt Theorem 1.7 (a) her, dass $\#E[m] = \deg[m] = m^2$, und insbesondere genau das für jeden Teiler $d \in \mathbb{Z}$ von m, nämlich: $\#E[d] = d^2$, woraus schon folgt, dass $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ ist. Denn es kann, da alle Punkte in $E[m]$ der Ordnung m sind, kein Faktor wie $\mathbb{Z}/M\mathbb{Z}$ von höherer Ordnung $M > m$ auftauchen. Auch feiner kann die Gruppe nicht zerfallen, da zur jeder gegebenen Ordnung d ein Faktor $\mathbb{Z}/d\mathbb{Z}$ höchstens zweimal auftauchen kann, sonst gäbe es mehr als d^2 Punkte dieser Ordnung. Zerfiele die Gruppe feiner, so tauchte ein Faktor mindestens drei Mal auf.

(b): Sei ϕ der p-Frobenius-Morphismus. Dann ist:

$$\#E[p^e] = \deg_s[p^e] = \left(\deg_s(\widehat{\phi} \circ \phi)\right)^e = (\deg_s \widehat{\phi})^e$$

Falls $\deg_s \widehat{\phi} = 1$, ist $\#E[p^e] = 1 \forall e \in \mathbb{N}$. Ansonsten ist $\deg_s \widehat{\phi} = p$, denn der Separabilitätsgrad muss $\deg \widehat{\phi} = \deg \phi = p$ teilen. Und damit gilt $\#E[p^e] = p^e \ \forall e \in \mathbb{N}$. Wie oben folgt dann $E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z} \ \forall e \in \mathbb{N}$. ■

A. Vorangehendes

Sei K stets ein *perfekter* Körper, $\overline{K}$ sein algebraischer Abschluss.
Seien C/K, C_1/K, C_2/K und C_3/K über K definierte Kurven.

A.1. Theorem.

(a) Ein nichtkonstanter Morphismus $\phi\colon C_1 \to C_2$ ist surjektiv.

(b) Ist $\phi\colon C_1 \to C_2$ eine über K definierte, nichtkonstant rationale Abb. so ist $K(C_1)/\phi^*K(C_2)$ eine endliche Körpererweiterung.

(c) Ist $\iota\colon K(C_2) \to K(C_1)$ ein K-Algebren-Homomorphismus, so gibt es eine eindeutige über K definierte, nichtkonstant rationale Abb. $\lambda\colon C_1 \to C_2$ mit $\lambda^* = \iota$.

(d) Ist $L \subseteq K(C)$ ein Unterkörper von endlichem Index mit $K \subseteq L$, so gibt es eine bis auf K-Isomorphie eindeutige glatte Kurve C'/K und eine über K definierte, nichtkonstant rationale Abb. $\phi\colon C \to C'$ mit $\phi^*K(C') = L$.

Siehe [Sil, II. §2., Theorem 2.3 und Theorem 2.4].

A.2. Definition. Sei $\phi\colon C_1 \to C_2$ eine nichtkonstant rationale Abb. glatter Kurven und $P \in C_1$. Der *Verzweigungsindex* von ϕ bei P ist $e_\phi(P) = \operatorname{ord}_P(\phi^* t_{\phi(P)})$, wobei $t_{\phi(P)} \in K(C_2)$ das uniformisierende Element bei $\phi(P)$ sei.

A.3. Proposition. Seien $\phi\colon C_1 \to C_2$, $\psi\colon C_2 \to C_3$ nichtkonstant rationale Abb. glatter Kurven.

(a) Für alle bis auf endlich viele $Q \in C_2$ ist $\#\phi^{-1}(Q) = \deg_s \phi$.

(b) Für jedes $Q \in C_2$ ist $\sum_{P\in\phi^{-1}(Q)} e_\phi(P) = \deg \phi$.

(c) Der Verzweigungsindex ist multiplikativ, d. h. $\forall P \in C_1\colon\ e_{\psi\circ\phi}(P) = e_\phi(P)\, e_\psi(\phi(P))$.

Siehe [Sil, II. §2., Proposition 2.6].

A.4. Definition. Ist $\operatorname{char} K = p > 0$ und $q = p^r$, so heißt der Morphismus $\phi\colon C \to C^{(q)},\ [x_0, \dots, x_n] \mapsto [x_0^q, \dots, x_n^q]$ der q-Frobenius-Morphismus, wobei die Kurve $C^{(q)}/K$ durch die Gleichungen $f^{(q)},\ f \in I(C)$ gegeben ist und $f^{(q)}$ stets aus dem Polynom $f \in K[X]$ entsteht, indem seine Koeffizienten mit q potenziert werden.

A.5. Proposition. Sei $\operatorname{char} K = p > 0$, $q = p^r$ und $\phi\colon C \to C^{(q)}$ der q-Frobenius-Morphismus.

(a) $\phi^*K(C^{(q)}) = K(C)^q$.

(b) ϕ ist rein inseparabel.

(c) $\deg \phi = q$.

Siehe [Sil, II. §2., Proposition 2.11].

A.6. Korollar. Jede rationale Abb. $\lambda\colon C_1 \to C_2$ faktorisiert als $\psi\circ\varphi$, wobei $\phi\colon C_1 \to C_1^{(q)}$ der q-Frobenius-Morphismus ist mit $q = \deg_i \lambda$ und $\psi\colon C^{(q)} \to C_1$ eine separable rationale Abb. Siehe [Sil, II. §2., Corollary 2.12].

A.7. Proposition. Eine nichtkonstant rationale Abb. $\phi\colon C_1 \to C_2$ induziert sowohl Homomorphismen:

(a) $\phi_*\colon \mathrm{Div}(C_1) \to \mathrm{Div}(C_2),\ (P) \mapsto (\phi P)$, und

(b) $\phi^*\colon \mathrm{Div}(C_2) \to \mathrm{Div}(C_1),\ (Q) \mapsto \sum_{P\in\phi^{-1}(Q)} e_\phi(P)(P)$,

die sich ihrerseits auf $\mathrm{Pic}^0(C_1) \to \mathrm{Pic}^0(C_2)$ bzw. $\mathrm{Pic}^0(C_2) \to \mathrm{Pic}^0(C_1)$ einschränken lassen, als auch einen $\overline{K}$-linearen Pullback auf den Differentialen:

(c) $\phi^*\colon \Omega_{C_2} \to \Omega_{C_1},\ \left(\sum_i f_i \mathrm{d}x_i\right) \mapsto \sum_i (\phi^* f_i)\mathrm{d}(\phi^* x_i)$,

welcher genau dann injektiv ist, wenn ϕ separabel ist. Siehe [Sil, II. §3., Remark 3.7, und §4., Proposition 4.2].

A.8. Theorem. Ist E eine elliptische Kurve mit Ursprung O, so ist durch $\kappa\colon E \to \mathrm{Pic}^0(E),\ P \mapsto [(P) - (O)]$ ein Gruppenisomorphismus gegeben. Siehe [Sil, III. §3., Proposition 3.4].

Literatur

[Sil] Joseph H. Silverman. *The Arithmetic Of Elliptic Curves*. New York: Springer, 1986.