
Seminar Kryptographie

# Die j-Invariante und Endomorphismen einer elliptischen Kurve

Ausarbeitung zum Seminarvortrag

von

Stephan Hofmann

20.06.2011

Dozent:
Dr. Mohamed Barakat

Technische Universität Kaiserslautern
Fachbereich Mathematik

# Inhaltsverzeichnis



# Bezeichungen

Im Folgenden sei $K$ ein Körper und $\overline{K}$ dessen algebraischer Abschluss. Des weiteren bezeichne $(x, y)$ den projetiven Punkt $(x : y : 1)$ und $\infty$ den projetiven Punkt $(0 : 1 : 0)$. Falls nicht explizit erwähnt, bezeichne $E$ eine elliptische Kurve über $K$.

# 1 Die j-Invariante

In diesem Kapitel werden wir mit Hilfe der j-Invarianten eine Äquivalenzrelation auf der Menge der elliptischen Kurven definieren, die es uns ermöglicht eine Klasse von elliptischen Kurven mit einem Element aus dem Grundkörper zu identifizieren. Wir werden dabei keine Grundkörper der Charakteristik 2 oder 3 betrachten, in diesen Fällen lässt sich die j-Invariante jedoch auch definieren und es gelten ähnliche Ergebnisse wie die hier bewiesenen.

**Definition 1.1.** *Sei $E$ eine elliptische Kurve in Weierstrassform, d.h. $y^2 = x^3 + Ax + B$ wobei $A, B \in K$ und $char(K) \neq 2, 3$. Dann nennen wir*

$$j = j(E) = 1728\frac{4A^3}{4A^3 + 27B^2} \in K$$

*die j-Invariante von $E$.*

**Bemerkung 1.2.** *Der Nenner ist das Negative der Diskriminanten von $x^3 + Ax + B$ und daher ungleich null.*

**Satz 1.3.** *Seien $y_1^2 = x_1^3 + A_1x_1 + B_1$ und $y_2^2 = x_2^3 + A_2x_2 + B_2$ zwei elliptische Kurven mit j-Invarianten $j_1$ und $j_2$. Dann sind die folgenden Aussagen äquivalent:*

*i)* $\exists\ 0 \neq \mu \in \overline{K}$ *, sodass* $A_2 = \mu^4 A_1\ ,\ B_2 = \mu^6 B_1$

*ii)* $j_1 = j_2$

*Die Substitution $x_2 = \mu^2 x_1\ ,\ y_2 = \mu^3 y_1$ transformiert eine Gleichung in die andere.*

*Beweis.* "*i) $\Rightarrow$ ii)*": Folgt durch Ausrechnen der beiden j-Invarianten.
"*ii) $\Rightarrow$ i)*": Sei $j_1 = j_2$

1. Fall: $A_1 \neq 0$

Es gilt: $A_1 \neq 0 \Leftrightarrow j_1 \neq 0 \Rightarrow j_2 \neq 0 \Rightarrow A_2 \neq 0$.
Da $\overline{K}$ algebraisch abgeschlossen ist, existiert ein $\mu \in \overline{K}$ s.d. $A_2 = \mu^4 A_1$.
Dann ist:

$$\frac{4A_2^3}{4A_2^3 + 27B_2^2} = \frac{4A_1^3}{4A_1^3 + 27B_1^2} = \frac{4\mu^{-12}A_2^3}{4\mu^{-12}A_2^3 + 27B_1^2} = \frac{4A_2^3}{4A_2^3 + 27\mu^1 2B_1^2}$$

Damit ist $B_2^2 = \mu^{12}B_1^2 = (\mu^6 B_1)^2 \Rightarrow B_2 = \pm\mu^6 B_1$
Falls $B_2 = \mu^6 B_1$ sind wir fertig.
Falls $B_2 = -\mu^6 B_2$ wähle $\mu' = i \cdot \mu$ (wobei $i^2 = -1$). Dann erfüllt $\mu'$ die Behauptung.

2. Fall: $A_1 = 0$
$A_1 = 0 \Rightarrow j_1 = 0 \Rightarrow j_2 = 0 \Rightarrow A_2 = 0$
Da $4A_j^3 + 27B_j^2 \neq 0$ für $j = 1, 2$ folgt dass $B_1, B_2 \neq 0$.
Somit existiert $\mu \in \overline{K}$ s.d. $B_2 = \mu^6 B_1$.

Dass die oben angegebene Substitution die beiden Gleichungen ineinander transformiert, erhält man durch Einsetzen.

□

**Folgerung 1.4.** *Seien $E_1$ und $E_2$ zwei elliptische Kurven mit j-Invarianten $j_1$ und $j_2$. Die Relation*

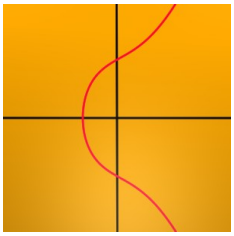
$$E_1 \sim E_2 \;\Leftrightarrow\; j_1 = j_2$$

*ist eine Äquivalenzrelation auf der Menge der elliptischen Kurven.*
*$E_1$ und $E_2$ heißen dann $\overline{K}$-äquivalent.*

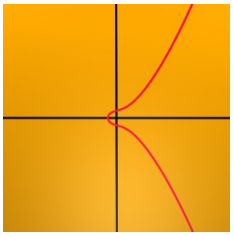
*Beweis.* trivial

□

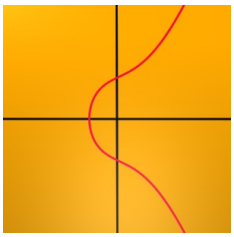
**Beispiel 1.5.** *Drei elliptische Kurven aus der Äquivalenzklasse $j = \frac{55296}{275}$ und zum Vergleich eine elliptische Kurve aus einer anderen Äquivalenzklasse:*



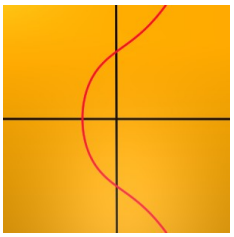
$y^2 = x^3 + 2x + 3$
$j = \frac{55296}{275}$



$y^2 = x^3 + \frac{1}{8}x + \frac{3}{64}$ , $\mu = 2$
$j = \frac{55296}{275}$



$y^2 = x^3 + \sqrt[4]{2}x + \frac{3}{2}$ , $\mu = \sqrt[6]{2}$
$j = \frac{55296}{275}$



$y^2 = x^3 + 3x + 4$
$j = \frac{2728}{5}$

**Satz 1.6.** *Es sei $j \neq 0, 1728$. Dann ist $j$ die j-Invariante von*

$$y^2 = x^3 + \frac{3j}{1728 - j}\ x + \frac{2j}{1728 - j} \tag{1}$$

*Beweis.* Nachrechnen.

□

**Definition 1.7.** *Wir definieren die Standardrepräsentante für $j \neq 0, 1728$ durch (1). Für $j = 0$ sei die Standardrepräsentante durch $y^2 = x^3 + 1$ und für $j = 1728$ durch $y^2 = x^3 + x$ gegeben.*

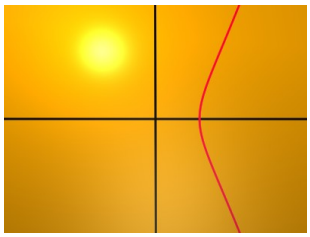
**Folgerung 1.8.** *Es gibt eine Bijektion*

$$K \leftrightarrow \left\{\overline{K}\ \text{Äquivalenzklassen elliptischer Kurven über } K\right\}$$

*Beweis.* Folgt direkt aus Folgerung 1.4 und Satz 1.6.

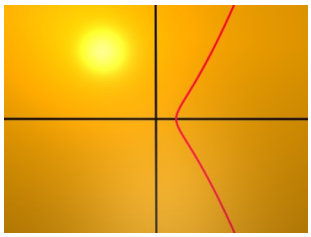
□

**Beispiel 1.9.** *Einige Standardrepräsentanten:*



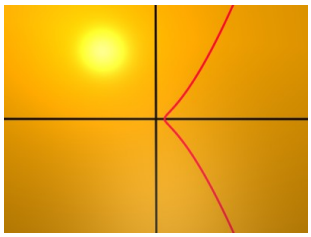
$j = -1000$

$y^2 = x^3 + \frac{3\cdot(-1000)}{1728-(-1000)}x + \frac{2\cdot(-1000)}{1728-(-1000)}$



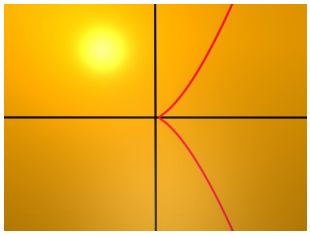
$j = -100$

$y^2 = x^3 + \frac{3\cdot(-100)}{1728-(-100)}x + \frac{2\cdot(-100)}{1728-(-100)}$



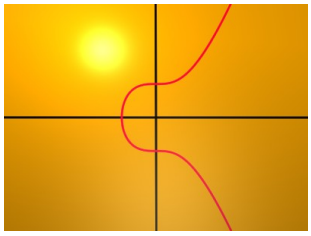
$j = -10$

$y^2 = x^3 + \frac{3\cdot(-10)}{1728-(-10)}x + \frac{2\cdot(-10)}{1728-(-10)}$



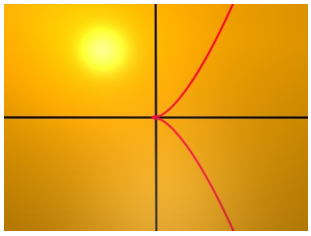
$j = -1$

$y^2 = x^3 + \frac{3\cdot(-1)}{1728-(-1)}x + \frac{2\cdot(-1)}{1728-(-1)}$



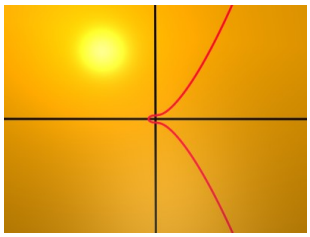
$j = 0$

$y^2 = x^3 + 1$



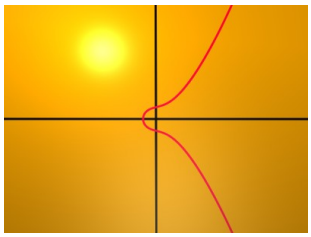
$j = 1$

$y^2 = x^3 + \frac{3\cdot1}{1728-1}x + \frac{2\cdot1}{1728-1}$



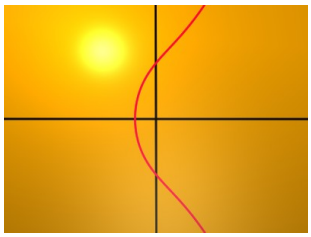
$j = 10$

$y^2 = x^3 + \frac{3\cdot10}{1728-10}x + \frac{2\cdot10}{1728-10}$



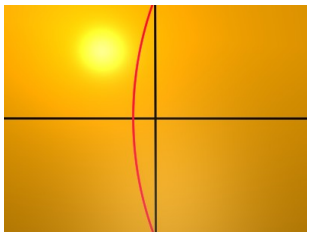
$j = 100$

$y^2 = x^3 + \frac{3\cdot100}{1728-100}x + \frac{2\cdot100}{1728-100}$



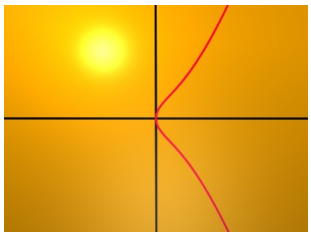
$j = 1000$

$y^2 = x^3 + \frac{3\cdot1000}{1728-1000}x + \frac{2\cdot1000}{1728-1000}$



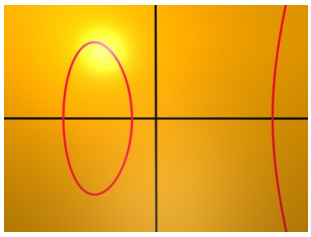
$j = 1500$

$y^2 = x^3 + \frac{3\cdot1500}{1728-1500}x + \frac{2\cdot1500}{1728-1500}$



$j = 1728$

$y^2 = x^3 + x$



$j = 2500$

$y^2 = x^3 + \frac{3\cdot2500}{1728-2500}x + \frac{2\cdot2500}{1728-2500}$

# 2 Endomorphismen

In diesem Kapitel werden wir eine für den Beweis des Satzes von Hasse wichtige Aussage beweisen. Außderm werden wir uns mit Separabilität von Endomorphismen und einigen technischen Aussagen über diese beschäftigen. Die verwendeten Rechenregeln auf einer elliptischen Kurve können z.B. in [Ba] nachgelesen werden.

**Definition 2.1.** *Unter einem Endomorphismus verstehen wir eine Abbildung*

$$\alpha : E(\overline{K}) \to E(\overline{K})$$

*sodass*

$$\alpha(P_1 + P_2) = \alpha(P_1) + \alpha(P_2)$$

*und rationale Funktionen $R_1(x,y), R_2(x,y)$ mit Koeffizienten in $\overline{K}$ existieren, mit*

$$\alpha(x,y) = (R_1(x,y), R_2(x,y)) \quad \forall (x,y) \in E(\overline{K})$$

**Bemerkung 2.2.** *Es gilt immer $\alpha(\infty) = \infty$. Wir notieren den trivialen Endomorphismus, der jeden Punkt auf $\infty$ abbildet, durch $\alpha = 0$ und nehmen an, dass von jetzt an $\alpha \neq 0$.*

**Beispiel 2.3.** *Sei E gegeben durch $y^2 = x^3 + Ax + B$ und sei $\alpha(P) = 2P$.*
*$\alpha$ ist ein Homomorphismus und $\alpha(x,y) = (R_1(x,y), R_2(x,y))$ mit*

$$R_1(x,y) = m^2 - 2x$$
$$R_2(x,y) = m(3x - m^2) - y$$

*wobei $m = \left(\frac{3x^2+A}{2y}\right)$*
*Also ist $\alpha$ sogar ein Endomorphismus.*

Wir wollen nun die Bedingung, dass rationale Funktionen in zwei Variablen existieren aus 2.1 etwas vereinfachen.

**Lemma 2.4.** *Sei $\alpha$ ein Endomorphismus der elliptischen Kurve E und E in Weierstraßform gegeben. Sei weiterhin $\alpha$ gegeben durch $\alpha(x,y) = \left(\frac{p(x)}{q(x)}, y \cdot \frac{s(x)}{t(x)}\right)$ wobei p,q,s,t Polynome sind, mit p und q sowie s und t teilerfremd. Dann gilt:*

$$\exists x_0 \text{ mit } t(x_0) = 0 \Rightarrow q(x_0) = 0$$

*Umgekehrt gilt dann natürlich:*

$$q(x) \neq 0 \ \ \forall x \Rightarrow t(x) \neq 0 \ \ \forall x$$

*Beweis.* Die Punkte $(x, y)$ und $\alpha(x, y) = (\frac{p(x)}{q(x)}, y \cdot \frac{s(x)}{t(x)})$ liegen auf E und erfüllen somit die Weierstraßgleichung:

$$y^2 = x^3 + Ax + B \quad und \quad \left(y \cdot \frac{s(x)}{t(x)}\right)^2 = \left(\frac{p(x)}{q(x)}\right)^3 + A \cdot \left(\frac{p(x)}{q(x)}\right) + B$$

Daraus ergibt sich, dass:

$$(x^3 + Ax + B) \cdot \frac{s(x)^2}{t(x)^2} = y^2 \cdot \frac{s(x)^2}{t(x)^2} = \frac{p(x)^3 + A \cdot p(x)q(x)^2 + B \cdot q(x)^3}{q(x)^3}$$

Wobei $u(x) := p(x)^3 + A \cdot p(x)q(x)^2 + B \cdot q(x)^3$ und $q(x)$ keine gemeinsame Nullstelle haben können, da diese im Widerspruch zur Vorraussetzung auch eine Nullstelle von p wäre.

Sei nun $t(x_0) = 0$ für ein $x_0$. Es ist

$$(x^3 + Ax + B) \cdot q(x)^3 \cdot s(x_0)^2 = u(x) \cdot t(x)^2$$

$x_0$ ist eine Nullstelle der rechten Seite mit mindestens Vielfachheit 2. Da $s$ und $t$ keine gemeinsame Nullstelle haben und $x_0$ in $(x^3 + Ax + B)$ höchstens eine Nullstelle mit Vielfachheit 1 sein kann, muss $x_0$ also mindestens eine einfache Nullstelle von $q^3$ und somit von $q$ sein.

□

**Lemma 2.5.** *Sei $\alpha : E(\overline{K}) \to E(\overline{K})$ ein Endomorphismus und E in Weierstrassform gegeben. Dann existieren rationale Funktionen $r_1(x), r_2(x)$ sodass*

$$\alpha(x, y) = (r_1(x), r_2(x)y) = \left(\frac{p(x)}{q(x)}, y \cdot r_2(x)\right) \tag{2}$$

*wobei $p(x)$ und $q(x)$ teilerfremde Polynome sind.*

*Beweis.* Sei $R(x, y)$ eine rationale Funktion. Da E in Weierstrassform gegeben ist, können wir jede gerade Potenz von y als Polynom in x und jede ungerade Potenz von y als y mal ein Polynom in x schreiben. D.h. es existieren Polynome $p_i(x)$, $i = 1, 2, 3, 4$ sodass:

$$R(x, y) = \frac{p_1(x) + y \cdot p_2(x)}{p_3(x) + y \cdot p_4(x)}$$

Nach Erweitern mit $p_3(x) - y \cdot p_4(x)$ und substituieren von $y^2$ mit $x^3 + Ax + B$ ergibt sich daraus:

$$R(x, y) = \frac{q_1(x) + y \cdot q_2(x)}{q_3(x)} \text{ für gewisse Polynome } q_j(x), j = 1, 2, 3 \tag{3}$$

Sei nun $\alpha(x,y) = (R_1(x), R_2(x))$. Es gilt:

$$\alpha(x,-y) \underset{\text{Formel für -P}}{\overset{\uparrow}{=}} \alpha(-(x,y)) \underset{\text{Morphismuseigenschaft}}{\overset{\uparrow}{=}} -\alpha(x,y)$$

und somit $R_1(x,-y) = R_1(x,y)$ und $R_2(x,-y) = -R_2(x,y)$.
Schreibe $R_1(x,y)$ und $R_2(x,y)$ in der Form (3):

$$\frac{q_1(x) + y \cdot q_2(x)}{q_3(x)} = R_1(x,y) = R_1(x,-y) = \frac{q_1(x) - y \cdot q_2(x)}{q_3(x)} \Rightarrow q_2 = 0$$
$$\frac{q_1'(x) + y \cdot q_2'(x)}{q_3'(x)} = R_2(x,y) = -R_2(x,-y) = \frac{-q_1'(x) + y \cdot q_2'(x)}{q_3'(x)} \Rightarrow q_1' = 0$$

Also lässt sich $\alpha$ schreiben als $\alpha(x,y) = (r_1(x), y \cdot r_2(x))$ wobei $r_1(x)$ und $r_2(x)$ rationale Funktionen sind.

Seien $p(x)$ und $q(x)$ Polynome, sodass $r_1(x) = \frac{p(x)}{q(x)}$.
Falls $q(x) = 0$ für einen Punkt $(x,y)$ so setze $\alpha(x,y) = \infty$.
Falls $q(x) \neq 0$ so ist $r_2(x)$ nach Lemma 2.4 definiert.

□

**Definition 2.6.** *Wir definieren den Grad eines Endomorphismus $\alpha$ durch*

$$deg(\alpha) := max\{deg(p(x)), deg(q(x))\}$$

*wobei p und q die Polynome aus Lemma 2.5 sind.*

**Definition 2.7.** *Wir nennen einen Endomorphismus separabel, wenn $r_1'(x) \neq 0$, wobei $r_1(x)$ die rationale Funktion aus Lemma 2.5 und $r_1'(x)$ die Ableitung von $r_1(x)$ ist.*

**Lemma 2.8.**

*i)* $r_1'(x) \neq 0 \Leftrightarrow p'(x) \neq 0$ *oder* $q'(x) \neq 0$

*ii) Falls char(K)=0 haben alle nichtkonstanten Polynome eine Ableitung ungleich null.*

*iii) Falls char(K)=p haben alle Polynome der Form $f(x^p)$ eine Ableitung gleich null.*

*Beweis. i):* $0 \neq r_1'(x) = \frac{d}{dx}\frac{p(x)}{q(x)} = \frac{p'(x)q(x) - p(x)q'(x)}{q(x)^2} \Rightarrow p'(x) \neq 0$ oder $q'(x) \neq 0$
*ii),iii):* trivial.

□

**Beispiel 2.9.** *Sei $\alpha(P) = 2P$. Dann ist $R_1(x,y) = \left(\frac{3x^2+A}{2y}\right)^2 - 2x$. Mit $y^2 = x^3 + Ax + B$ folgt dass:*

$$r_1(x) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)}$$

*Damit ist $deg(\alpha) = 4$.*
*Außerdem ist $q'(x) = 4(3x^2 + A) \neq 0$, auch falls $char(K) = 3$ da $A = 0$ nicht auftreten darf, und somit ist $\alpha$ separabel.*

Die Frobenius Abbildung spielt eine wichtige Rolle, wenn man elliptische Kurven über endlichen Körpern betrachtet. Wir werden im Folgenden einige Eigenschaften der Frobenius Abbildung nachweisen.

**Definition 2.10.** *Sei $E$ eine elliptische Kurve über $\boldsymbol{F}_q$. Wir definieren die Frobenius Abbildung durch*

$$\phi_q(x,y) := (x^q, y^q).$$

**Lemma 2.11.** *$\phi_q$ ist ein Endomorphismus. Es gilt $deg(\phi_q) = q$ und $\phi_q$ ist nicht separabel.*

*Beweis.* Klar: Die Frobeniusabbildung ist durch die Polynome $x^q$ und $y^q$, also insbesondere durch rationale Funktionen gegeben und $deg(x^q) = q$.
Zeige: $\phi_q$ ist ein Homomorphismus, d.h. $\phi_q((x_1,y_1)+(x_2,y_2)) = \phi_q(x_1,y_1)+\phi_q(x_2,y_2) \quad \forall (x_1,y_2),(x_2,y_2)$
Seien $(x_1,y_1),(x_2,y_2) \in E$.
1. Fall: $x_1 \neq x_2$

Nach der Additionsformel gilt:

$$(x_1,y_1)+(x_2,y_2) = (x_3,y_3) \text{ mit } x_3 = m^2 - x_1 - x_2 \text{ und } y_3 = m(x_1 - x_3) - y_1, \text{ wobei } m = \tfrac{y_2-y_1}{x_2-x_1}$$

Da wir über $\mathbf{F}_q$ rechnen, können wir alles mit $q$ potenzieren:

$$x_3^q = m^2 - x_1^q - x_2^q \text{ und } y_3^q = m'(x_1^q - x_3^q) - y_1^q, \text{ wobei } m' = \tfrac{y_2^q - y_1^q}{x_2^q - x_1^q}$$

Damit folgt, dass $\phi_q(x_3,y_3) = (x_3^q, y_3^q) = (x_1^q, y_1^q) + (x_2^q, y_2^q) = \phi_q(x_1,y_1) + \phi_q(x_2,y_2)$.
Der Fall, dass $x_1 = x_2, y_1 \neq y_2$ und der Fall, dass einer der Punkte $\infty$ ist, folgen analog.
2. Fall: $(x_1,y_1) = (x_2,y_2)$

Die Formel für die Verdopplung eines Punktes liefert:

$$2(x_1,y_1) = (x_3,y_3) \text{ mit } x_3 = m^2 - 2x_1 \text{ und } y_3 = m(x_1 - x_3) - y_1, \text{ wobei } m = \tfrac{3x_1^2+A}{2y_1}$$

Wie im ersten Fall können wir alles mit $q$ potenzieren:

$$x_3^q = m'^2 - 2^q x_1^q \text{ und } y_3^q = m'(x_1^q - x_3^q) - y_1^q, \text{ wobei } m' = \tfrac{3^q (x_1^q)^2 + A^q}{2^q y_1^q}$$

Da $2, 3, A \in \mathbf{F}_q$ gilt $2^q = 2, 3^q = 3, A^q = A$ und wir erhalten die Formel für die Verdopplung des Punktes $(x_1^q, x_2^q)$.
Also ist $\phi_q(x_3, y_3) = (x_3^q, y_3^q) = (x_1^q, y_1^q) + (x_1^q, y_1^q) = \phi_q(x_1, y_1) + \phi_q(x_1, y_1)$.

Da $\phi_q$ durch rationale Funktionen gegeben ist, ist er ein Endomorphismus.
Außerdem gilt $r_1'(x) = (x^q)' = qx^{q-1} = 0$, da $q = 0$ in $\mathbf{F}_q$ und somit ist $\phi_q$ nicht separabel.

□

Der folgende Satz liefert ein Resultat, das essenziell für den Beweis des Satzes von Hasse ist.

**Satz 2.12.** *Sei $\alpha \neq 0$ ein Endomorphismus. Dann gilt:*

*i.) Falls $\alpha$ separabel $\Rightarrow deg(\alpha) = |ker(\alpha)|$*

*ii.) Falls $\alpha$ nicht separabel $\Rightarrow deg(\alpha) > |ker(\alpha)|$*

*Beweis.* Wir betrachten zunächst den Fall, dass $\alpha$ separabel ist.
Nach Lemma 2.5 lässt sich $\alpha$ schreiben als $\alpha(x, y) = (r_1(x), y \cdot r_2(x))$ und $r_1(x) = \frac{p(x)}{q(x)}$.
Nach Vorraussetzung ist $r_1'(x) \neq 0$ und somit $p'q - pq' \neq 0$.
Sei $S = \left\{x \in \overline{K} | (pq' - p'q)(x) \cdot q(x) = 0\right\}$. Wähle $(a, b) \in E(\overline{K})$, sodass:

1. $a \neq 0$ , $b \neq 0$ , $(a, b) \neq \infty$
2. $deg(p(x) - aq(x)) = max\left\{deg(p(x)), deg(q(x))\right\} = deg(\alpha)$
3. $a \notin r_1(S)$
4. $(a, b) \in \alpha(E(\overline{K})) = Im(\alpha)$

Da $pq' - p'q \neq 0$ ist $S$ endlich und somit auch $\alpha(S)$. Die Funktion $r_1(x)$ nimmt unendlich viele verschiedene Werte für $x \in \overline{K}$ an. Für jedes x gibtes einen Punkt $(x, y) \in E(\overline{K})$, daher ist $|\alpha(E(\overline{K}))| = \infty$. Somit existiert ein Punkt $(a, b)$ der 1. bis 4. erfüllt.
Behauptung: Es gibt genau $deg(\alpha)$ Punkte $(x, y) \in E(\overline{K})$, sodass $\alpha(x_1, y_1) = (a, b)$.
Für einen solchen Punkt $(x_1, y_1)$ gilt:

$$\frac{p(x_1)}{q(x_1)} = a \ , \ y_1 \cdot r_2(x_1) = b.$$

Wegen 1. ist $(a, b) \neq \infty$ und somit $q(x_1) \neq 0$. Also ist $r_2(x_1)$ nach Lemma 2.4 definiert und da nach 1. $b \neq 0$ ist, muss gelten:

$$y_1 = \frac{b}{r_2(x_1)}$$

Daher ist $y_1$ durch $x_1$ festgelegt und es genügt Werte für $x_1$ zu betrachten.
Wegen 2. und da wir $\overline{K}$ als Grundkörper haben, hat $p(x) - aq(x)$ , $deg(\alpha)$ Nullstellen (mit Multiplizitäten gezählt).

Zeige: $p - aq$ hat keine mehrfachen Nullstellen.
Angenommen: $x_0$ sei eine mehrfache Nullstelle von $p - aq$. Dann gilt:

$$p(x_0) - aq(x_0) = 0 \text{ und } p'(x_0) - aq'(x_0) = 0$$

Multiplizieren von $p(x_0) = aq(x_0)$ und $aq'(x_0) = p'(x_0)$ liefert:

$$a \cdot p(x_0)q'(x_0) = a \cdot p'(x_0)q(x_0) \Rightarrow a \cdot (p(x_0)q'(x_0) - p'(x_0)q(x_0)) = 0$$

Wegen 1. ist $a \neq 0$ und somit muss $x_0$ eine Nullstelle von $pq' - p'q$ sein, also $x_0 \in S$. Dann ist $a = r_1(x_0) \in r_1(S)$ was aber ein Widerspruch zu 3. ist.
Also hat $p - aq$ keine mehrfachen Nullstellen.
Damit hat $p - aq$ $deg(\alpha)$ verschiedene Nullstellen, d.h. es existieren genau $deg(\alpha)$ Punkte $(x_1, y_1)$ mit $\alpha(x_1, y_1) = (a, b)$ oder anders ausgedrückt:

$$M := \{(x_1, y_1) | \alpha(x_1, y_1) = (a, b)\} \text{ dann ist } |M| = deg(\alpha)$$

Dann gilt: Sei $(\hat{x}, \hat{y}) \in ker(\alpha)$ , $(x_1, y_1) \in M$
$\Rightarrow \alpha((x_1, y_1) + (\hat{x}, \hat{y})) = \alpha(x_1, y_1) + \alpha(\hat{x}, \hat{y}) = (a, b) + \infty = (a, b)$
$\Rightarrow (x_1, y_1) + (\hat{x}, \hat{y}) \in M$
$\Rightarrow |ker(\alpha)| \leq |M| = deg(\alpha)$
Außerdem: Seien $(x_i, y_i), (x_j, y_j) \in M$
$\Rightarrow \alpha((x_i, y_i) - (x_j, y_j)) = \alpha(x_i, y_i) - \alpha(x_j, y_j) = (a, b) - (a, b) = \infty$
$\Rightarrow (x_i, y_i) - (x_j, y_j) \in ker(\alpha)$
$\Rightarrow |ker(\alpha)| \geq |M| = deg(\alpha)$
Also ist $|ker(\alpha)| = deg(\alpha)$.

Im Fall, dass $\alpha$ nicht separabel ist, gelten alle Schritte des obigen Beweises außer, dass $p'(x) - aq'(x) = 0 \; \forall x$. Somit hat $p(x) - aq(x)$ immer mehrfache Nullstellen und wir erhalten weniger als $deg(\alpha)$ Lösungen. □

**Satz 2.13.** *Sei $E$ eine elliptische Kurve über $K$ und $0 \neq \alpha$ ein Endomorphismus von $E$.*
*Dann ist $\alpha : E(\overline{K}) \to E(\overline{K})$ surjektiv.*

**Bemerkung 2.14.** *Es ist dabei wichtig, dass wir über $\overline{K}$ statt $K$ arbeiten. Tatsächlich kann man zeigen, dass die Verdopplung eines Punktes auf $E(\mathbb{Q})$ bereits nicht mehr surjektiv ist.*

*Beweis von Satz 2.13.* Sei $(a,b) \in E(\overline{K})$ und o.E. $(a,b) \neq \infty$ (da $\alpha(\infty) = \infty$).
Nach Lemma 2.5 können wir $\alpha$ schreiben als $\alpha(x,y) = (r_1(x), y \cdot r_2(x)) = (\frac{p(x)}{q(x)}, y \cdot r_2(x))$.
1.Fall: $p(x) - aq(x)$ nicht konstant

Dann hat $p(x) - aq(x)$ nach dem Hilbertschen Nullstellensatz über $\overline{K}$ eine Nullstelle $x_0 \in \overline{K}$. Da $p$ und $q$ nach Vorraussetzung keine gemeinsame Nullstelle haben und $a \neq 0$, muss $q(x_0) \neq 0$ gelten. Sei $y_0$ eine Wurzel von $x_0^3 + Ax_0 + B$. Dann ist $\alpha(x_0, y_0)$ nach Lemma 2.4 definiert und $\alpha(x_0, y_0) = (a, b')$ mit $(a, b') \in E(\overline{K})$. Da $(a,b)$ und $(a,b')$ auf $E(\overline{K})$ liegen gilt:

$$b'^2 = a^3 + Aa + B = b^2 \Rightarrow b = \pm b'$$

Falls $b' = b$ ist $(x_0, y_0)$ ein Urbild von $(a,b)$.
Falls $b' = -b$ dann ist $\alpha(x_0, -y_0) = -\alpha(x_0, y_0) = -(a,b') = (a, -b') = (a,b)$ und somit ist $(x_0, -y_0)$ ein Urbild von $(a,b)$.

2.Fall: $p(x) - aq(x)$ konstant

Da $|E(\overline{K})| = \infty$ und $|ker(\alpha)| < \infty$ nach Satz 2, können nur endlich viele Punkte $(x,y) \in E(\overline{K})$ auf einen Punkt mit gegebener x-Koordinate abgebildet werden.
*(Denn je zwei Punkte $(x_i, y_i), (x_j, y_j)$ mit $\alpha(x_i, y_i) = (c, y_i \cdot r_2(x_i))$ und $\alpha(x_j, y_j) = (c, y_j \cdot r_2(x_j))$ für ein $c \in \overline{K}$ liefern einen Punkt $(x_i, y_i) - (x_j, y_j)$ mit $\alpha((x_i, y_i) - (x_j, y_j)) = \alpha(x_i, y_i) - \alpha(x_j, y_j) = (c, y_i \cdot r_2(x_i)) - (c, y_j \cdot r_2(x_j)) = (c, y_i \cdot r_2(x_i)) + (c, -y_j \cdot r_2(x_j)) = \infty$, der also im Kern von $\alpha$ liegt.)*
Daher ist entweder $p(x)$ nicht konstant oder $q(x)$ nicht konstant. Da aber $p(x) - aq(x)$ konstant ist, müssen beide nicht konstant sein. Dann existiert höchstens ein $a$, sodass $p - aq$ konstant ist.
*(wäre $a'$ mit $a' \neq a$ eine weitere solche Zahl, dann ist $(a - a')q = (p - aq) - (p - a'q)$ konstant und $(a' - a)p = a'(p - aq) - a(p - a'q)$ konstant, woraus folgen würde, dass p und q konstant sind.)*
Daher existieren höchstens zwei Punkte $(a,b)$ und $(a,-b)$ die nicht im Bild von $\alpha$ liegen könnten. Sei $(a_1, b_1)$ ein weiterer Punkt, dann existiert ein Punkt $P_1$ mit $\alpha(P_1) = (a_1, b_1)$. Wir können $(a_1, b_1)$ so wählen, dass $(a_1, b_1) + (a,b) \neq (a, \pm b)$, also existiert ein Punkt $P_2$ mit $\alpha(P_2) = (a_1, b_1) + (a,b)$. Dann gilt:

$$\alpha(P_2 - P_1) = (a,b) \quad und \quad \alpha(P_1 - P_2) = -(a,b) = (a,-b)$$

Somit haben wir für alle Punkte ein Urbild gefunden.

□

Im Folgenden werden wir ein etwas einfacher zu überprüfendes Kriterium für Separabilität herleiten, welches für die meisten Endomorphismen angewendet werden kann.

**Bemerkung 2.15.** *Wenn $(x,y)$ ein variabler Punkt auf $y^2 = x^3 + Ax + B$ ist, dann können wir bezüglich $x$ ableiten und erhalten:*

$$2yy' = 3x^2 + A.$$

*Ähnlich können wir eine rationale Funktion $f(x,y)$ bezüglich $x$ ableiten, wenn wir $y$ als Funktion von $x$ auffassen und erhalten:*

$$\frac{d}{dx}f(x,y) = f_x(x,y) + f_y(x,y)y'$$

*wobei $f_x$ und $f_y$ partielle Ableitungen sind.*

**Lemma 2.16.** *Sei $E$ eine elliptische Kurve in Weierstrassform. Wähle einen festen Punkt $(u,v)$ auf $E$. Schreibe*

$$(x,y) + (u,v) = (f(x,y), g(x,y)),$$

*wobei $(x,y) \in E$ und $f(x,y), g(x,y)$ rationale Funktionen sind, deren Koeffizienten von $u$ und $v$ abhängen. Dann gilt:*

$$\frac{\frac{d}{dx}f(x,y)}{g(x,y)} = \frac{1}{y}$$

*Beweis.* Die Additionsformeln liefern:

$$\begin{aligned} f(x,y) &= \frac{y-v}{x-u}^2 - x - u \\ g(x,y) &= \frac{-(y-v)^3 + x(y-v)(x-u)^2 + 2u(y-v)(x-u)^2 - v(x-u)^3}{(x-u)^3} \\ \frac{d}{dx}f(x,y) &= \frac{2y'(y-v)(x-u) - 2(y-v)^2 - (x-u)^3}{(x-u)^3}. \end{aligned}$$

Eine längliche aber elementarmathematische Rechnung, unter Verwendung dass $2yy' = 3x^2 + A$, ergibt:

$$(x-u)^3\left(y \cdot \frac{d}{dx}f(x,y) - g(x,y)\right) = v(Au + u^3 - v^2 - Ax - x^3 + y^2) + y(-Au - u^3 + v^2 + Ax + x^3 - y^2).$$

Da $(u,v)$ und $(x,y)$ auf $E$ liegen, gilt $v^2 = u^3 + Au + B$ und $y^2 = x^3 + Ax + B$. Damit ergibt der obige Ausdruck, dass:

$$(x-u)^3\left(y \cdot \frac{d}{dx}f(x,y) - g(x,y)\right) = v(-B+B) + y(B-B) = 0.$$

Damit ist $y \cdot \frac{d}{dx}f(x,y) - g(x,y) = 0$, also $\frac{\frac{d}{dx}f(x,y)}{g(x,y)} = \frac{1}{y}$.

□

**Lemma 2.17.** *Seien $\alpha_1, \alpha_2, \alpha_3$ Endomorphismen einer elliptischen Kurve $E$ und $\alpha_1 + \alpha_2 = \alpha_3$. Schreibe*

$$\alpha_j(x,y) = (R_{\alpha_j}(x), yS_{\alpha_j}(x)) \quad \forall j = 1,2,3$$

*Falls Konstanten $c_{\alpha_1}$ und $c_{\alpha_2}$ existieren, sodass:*

$$\frac{R'_{\alpha_1}(x)}{S_{\alpha_1}(x)} = c_{\alpha_1} \ , \ \frac{R'_{\alpha_2}(x)}{S_{\alpha_2}(x)} = c_{\alpha_2}$$

*dann gilt:*

$$\frac{R'_{\alpha_3}(x)}{S_{\alpha_3}(x)} = c_{\alpha_1} + c_{\alpha_2}.$$

*Beweis.* Seien $(x_1, y_1) = \alpha_1(x, y)$ und $(x_2, y_2) = \alpha_2(x, y)$ variable Punkte auf $E$ und $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$. Dann sind $x_3$ und $y_3$ rationale Funktionen von $x_1, x_2, y_1, y_2$, welche wiederum rationale Funktionen von $x, y$ sind. Nach Lemma 2.16 mit $(u, v) = (x_2, y_2)$ und Bermerkung 2.15 gilt:

$$\frac{\frac{d}{dx_1}x_3}{y_3} = \frac{1}{y_1} \ \Rightarrow \ \frac{\partial x_3}{\partial x_1} + \frac{\partial x_1}{\partial y_1}\frac{dy_1}{dx_1} = \frac{y_3}{y_1}$$

Analog gilt mit $(u, v) = (x_1, y_1)$:

$$\frac{\partial x_3}{\partial x_2} + \frac{\partial x_2}{\partial y_2}\frac{dy_2}{dx_2} = \frac{y_3}{y_2}$$

Nach Voraussetzung gilt außerdem:

$$\frac{dx_j}{dx} = c_{\alpha_1} \cdot \frac{y_j}{y} \text{ für } j = 1, 2.$$

Mit der Kettenregel und obigen Gleichungen ergibt sich, dass:

$$\begin{aligned}
\frac{dx_3}{dx} &= \frac{\partial x_3}{\partial x_1}\frac{dx_1}{dx} + \frac{\partial x_3}{\partial y_1}\frac{dy_1}{dx_1}\frac{dx_1}{dx} + \frac{\partial x_3}{\partial x_2}\frac{dx_2}{dx} + \frac{\partial x_3}{\partial y_2}\frac{dy_2}{dx_2}\frac{dx_2}{dx} \\
&= \left(\frac{y_3}{y_1} - \frac{\partial x_3}{\partial y_1}\frac{dy_1}{dx_1}\right)\frac{dx_1}{dx} + \frac{\partial x_3}{\partial y_1}\frac{dy_1}{dx_1}\frac{dx_1}{dx} + \left(\frac{y_3}{y_2} - \frac{\partial x_3}{\partial y_2}\frac{dy_2}{dx_2}\right)\frac{dx_2}{dx} + \frac{\partial x_3}{\partial y_2}\frac{dy_2}{dx_2}\frac{dx_2}{dx} \\
&= \frac{y_3}{y_1}\frac{y_1}{y}c_{\alpha_1} + \frac{y_3}{y_2}\frac{y_2}{y}c_{\alpha_2} \\
&= (c_{\alpha_1} + c_{\alpha_2})\frac{y_3}{y}.
\end{aligned}$$

Multiplikation beider Seiten mit $\frac{y}{y_3}$ liefert die Behauptung.

□

**Proposition 2.18.** *Sei $E$ eine elliptische Kurve über einem Körper $K$ und $0 \neq n \in \mathbb{Z}$. Sei die Multiplikation mit $n$ auf $E$ gegeben durch:*

$$n(x, y) = (R_n(x), yS_n(x)) \ \ \forall (x, y) \in E(\overline{K})$$

*wobei $R_n$ und $S_n$ rationale Funktionen sind.*

*Dann gilt:*

$$\frac{R'_n(x)}{S_n(x)} = n.$$

*Somit ist die Multiplikation mit n genau dann separabel, wenn gilt $p \nmid n$ wobei $p = char(K)$.*

*Beweis.* Da $R_{-n} = R_n$ und $S_{-n} = -S_n$ gilt:

$$\frac{R'_{-n}}{S_{-n}} = -\frac{R'_n}{S_n}.$$

Daher genügt es positive $n$ zu betrachten.
Wir beweisen den ersten Teil der Proposition mit vollständiger Induktion über $n$:
$\underline{n = 1:}$ trivial.
$\underline{n \to n+1:}$ Wenn die Aussage für $n$ und für 1 gilt, so gilt sie nach Lemma 2.17 auch für $n+1$.
Damit gilt: $\frac{R'_n(x)}{S_n(x)} = n$ für alle n.
Des weiteren gilt:

$$R'_n(x) \neq 0 \quad \Leftrightarrow \quad \frac{R'_n}{S_n(x)} \neq 0 \quad \Leftrightarrow \quad n \neq 0 \quad \Leftrightarrow \quad p \nmid n.$$

Damit ist $n(x, y)$ nach Definition 2.7 separabel, genau dann wenn $p \nmid n$, was den zweiten Teil der Proposition zeigt.

□

**Proposition 2.19.** *Sei E eine elliptische Kurve über dem Körper $\boldsymbol{F}_q$, wobei $q = p^n$, $p \in \mathbb{P}$, $0 \neq n \in \mathbb{N}$ und seien $0 \neq r, s \in \mathbb{Z}$. Dann ist der Endomorphismus*

$$r\phi_q + s$$

*separabel, genau dann wenn $p \nmid s$.*

*Beweis.* Sei die Multiplikation mit $r$ als Endomorphismus gegeben durch $r(x, y) = (R_r(x), y \cdot S_r(x))$ und die Multiplikation mit $s$ durch $s(x, y) = (R_s(x), y \cdot S_s(x))$.
Dann gilt:

$$\begin{aligned}(R_{r\phi_q}(x), y \cdot S_{r\phi_q}(x)) &= (\phi_q r)(x, y) \\ &= (R_r^q \ , \ y^q S_r^q(x)) \\ &= \left(R_r^q(x) \ , \ y(x^3 + Ax + B)^{\frac{q-1}{2}} S_r^q(x)\right).\end{aligned}$$

Daraus folgt, dass:

$$c_{r\phi_q} = \frac{R'_{r\phi_q}}{S_{r\phi_q}} = \frac{qR_r^{q-1}R'_r}{S_{r\phi_q}} = 0$$

da in $\mathbf{F}_q$ gilt, dass $q = 0$.

Des weiteren gilt wegen Proposition 2.18:

$$c_s = \frac{R_s'(x)}{S_s(x)} = s.$$

Nach Lemma 2.17 gilt dann:

$$\frac{R'_{r\phi_q+s}}{S_{r\phi_q+s}} = c_{r\phi_q+s} = c_{r\phi_q} + c_s = 0 + s = s$$

Damit ist $r\phi_q + s$ separabel, genau dann wenn:

$$R'_{r\phi_q+s} \neq 0 \;\Leftrightarrow\; c_{r\phi_q+s} \neq 0 \;\Leftrightarrow\; s \neq 0 \;\Leftrightarrow\; p \nmid s.$$

□

# Literatur

[Wa] L. Washington: “Elliptic curves: number theory and cryptography“, Chapman & Hall/CRC, 2008

[Ba] M. Barakat: “Cryptography“, Lecture notes, TU Kaiserslautern, 2011
http://www.mathematik.uni-kl.de/~barakat/Lehre/WS10/Cryptography/lecture_notes/Cryptography.pdf

[Ma] T. Markwig: “Theorie und Visualisierung algebraischer Kurven und Flächen“, Fortbildung für Mathematiklehrer, TU Kaiserslautern, 2009
http://www.mathematik.uni-kl.de/~keilen/download/Lehre/EMWS08/fortbildung.pdf