Berechnung von Isogenien zwischen elliptischen Kurven über endlichen Körpern

Diplomarbeit von Anita Krahmann

Technische Universität Berlin
Berlin 2007

Inhaltsverzeichnis

Einleitung

Die Sicherheit vieler heutzutage verwendeter kryptographischer Verfahren basiert auf der Schwierigkeit, das sogenannte *diskrete Logarithmusproblem* (DLP) auf der unterliegenden Gruppe zu lösen. Das DLP ist folgendermassen definiert:
Sei $(G, +)$ eine zyklische abelsche Gruppe, sei P ein Erzeuger von G und sei $Q \in G$. Gesucht ist nun $r \in \mathbb{Z}$ mit minimalem Betrag, so dass $rP = Q$ gilt.
In der Kryptographie verwendet man als zyklische Gruppe G entweder die multiplikative Gruppe $\mathbb{F}_q^*$ eines endlichen Körpers oder die Punktgruppe $E(\mathbb{F}_q)$ einer elliptischen Kurve über einem endlichen Körper. Während es zur Lösung des DLP in $\mathbb{F}_q^*$ Algorithmen mit subexponentieller Laufzeit in $log(\#G)$ gibt, ist für allgemeine elliptische Kurven kein solcher Algorithmus bekannt. Der Vorteil der Verwendung elliptischer Kurven in kryptographischen Verfahren gegenüber der Verwendung endlicher Körper ist also entweder höhere Sicherheit bei gleicher Schlüssellänge oder kleinere Schlüssellänge bei gleicher Sicherheit. Allerdings gibt es elliptische Kurven, auf die man den GHS-Angriff anwenden kann (siehe [GHS02b] und [GHS02a]). Hierbei wird das DLP auf der Ausgangskurve auf das DLP in der Jakobischen einer hyperelliptischen Kurve reduziert, für das Algorithmen mit subexponentieller Laufzeit existieren. Nun stellt sich die Frage, ob sich die relativ kleine Menge von Kurven, auf die man diesen Angriff anwenden kann, irgendwie vergrössern lässt. Hier kommen dann Isogenien ins Spiel.
Eine K-Isogenie zwischen zwei über demselben endlichen Körper K definierten elliptischen Kurven E_1/K und E_2/K ist eine rationale Abbildung zwischen E_1 und E_2. Sie induziert einen Homomorphismus der Punktgruppen $E_1(K)$ und $E_2(K)$. Ein Satz von Tate aus [Tat66] besagt, dass genau dann eine K-Isogenie zwischen E_1 und E_2 existiert, wenn sie dieselbe Punktanzahl über K haben.
Unser Ziel in dieser Diplomarbeit ist es, einen Algorithmus, welcher eine solche Isogenie berechnet, zu beschreiben und in KASH3 zu implementieren. Wir haben also zwei Kurven E_1/K und E_2/K mit $\#E_1(K) = \#E_2(K)$ gegeben und berechnen eine K-Isogenie $\varphi : E_1 \to E_2$. Das Grundgerüst dieses Algorithmus stammt aus [Gal99] bzw. [GHS02a].
Haben wir nun zwei isogene Kurven E_1 und E_2 gegeben, so dass E_2 anfällig für

den GHS-Angriff ist und E_1 nicht, so dass also das DLP auf $E_2(K)$ leichter zu lösen ist als auf $E_1(K)$, dann können wir mithilfe einer Isogenie $\varphi : E_1 \to E_2$ das DLP von $E_1(K)$ auf $E_2(K)$ übertragen: Wir haben zwei Punkte $P, Q \in E_1(K)$ gegeben und wissen, dass $rP = Q$ für ein $r \in \mathbb{Z}$ mit minimalem Betrag. Dieses r wollen wir finden. Wir lösen das DLP auf E_2 für $\varphi(P)$ und $\varphi(Q)$ und finden $r' \in \mathbb{Z}$ mit $r'\varphi(P) = \varphi(Q)$. Aufgrund der Homomorphieeigenschaft von Isogenien gilt dann auch $\varphi(r'P) = \varphi(Q)$. Durch Anwendung der dualen Isogenie erhalten wir $\widehat{\varphi}\varphi(r'P) = \widehat{\varphi}\varphi(Q)$. Dies bedeutet aber $\ell r'P = \ell Q$, wobei ℓ der Grad der Isogenie ist. Falls $\mathrm{ggT}(\ell, \mathrm{ord}(P)) = 1$ gilt, dann ist $r'P = Q$. Hiervon können wir aber ausgehen, da in kryptographischen Anwendungen meist mit einer Untergruppe von primer Ordnung gearbeitet wird. Allerdings ist dieses Verfahren nicht für die Punkte im Kern der Isogenie anwendbar. Ist der Kern „klein“, so kann man das DLP für diese Punkte durch ein anderes Verfahren, zum Beispiel mit dem BabyStep-GiantStep-Verfahren, lösen.
In unserem Algorithmus berechnen wir eine Isogenie mit möglichst kleinem Grad und somit auch möglichst kleinem Kern, was nicht nur hilft, das oben genannte Problem besser zu lösen, sondern auch die berechnungs- und darstellungstechnischen Aspekte vereinfacht.
Die Arbeit ist folgendermassen aufgebaut:
Im ersten Kapitel definieren wir Varietäten und elliptische Kurven. Im zweiten Kapitel werden Isogenien und deren für uns wichtigste Eigenschaften vorgestellt. Im dritten Kapitel betrachten wir die zahlentheoretischen Grundlagen für unseren Algorithmus. Im vierten Kapitel werden elliptische Kurven als Gitter über $\mathbb{C}$ definiert. Auf dieser Basis kann man weitere Eigenschaften von Isogenien erkennen. Im fünften Kapitel stellen wir einen Algorithmus zur Berechnung des Endomorphismenrings einer elliptischen Kurve über einem endlichen Körper vor. Im sechsten Kapitel erläutern wir verschiedene Teilschritte zur Isogenieberechnung, welchen wir dann im siebenten Kapitel zum kompletten Algorithmus zusammenfassen. Dort finden sich auch einige Beispiele.

Kapitel 1

Grundlagen

Um elliptische Kurven exakt definieren zu können, führen wir zunächst ganz allgemeine affine und projektive Varietäten ein. Die „natürliche“ Vorstellung einer elliptischen Kurve ist zwar die einer affinen Varietät, allerdings wird der „Punkt im Unendlichen“ projektiv sauberer defininert. Auch wenn wir später Isogenien definieren, benötigen wir projektive Varietäten.

1.1 Varietäten

Die Definitionen dieses Abschnitts sind grösstenteils aus [Sil86] entnommen. Als Referenz für hier nicht definierte Begriffe verweisen wir auf [Bos92]. Mit K bezeichnen wir hier immer einen fest gewählten, vollkommenen Körper. Alle vorkommenden Körpererweiterungen sind, sofern nicht anders erwähnt, endliche algebraische Körpererweiterungen.

1.1 Definition. Der *n-dimensionale affine Raum* über K ist die Menge $\mathbb{A}^n := \{P = (x_1, \ldots, x_n) \mid x_i \in \overline{K}\}$. Die Elemente von $\mathbb{A}^n$ heissen Punkte. Wir nennen für einen algebraischen Erweiterungskörper $\widetilde{K}$ von K die Menge $\mathbb{A}^n(\widetilde{K}) := \{P = (x_1, \ldots, x_n) \mid x_i \in \widetilde{K}\}$ die *$\widetilde{K}$-rationalen Punkte* von $\mathbb{A}^n$.

1.2 Definition. Sei $I \subset K[x_1, \ldots, x_n]$ ein Primideal, so dass $I\overline{K}[x_1, \ldots, x_n]$ ein Ideal von $\overline{K}[x_1, \ldots, x_n]$ ist. Die Menge $V_I := \{P \in \mathbb{A}^n \mid f(P) = 0 \; \forall f \in I\}$ heisst dann eine *über K definierte affine Varietät.*

1.3 Definition. Sei $V \subseteq \mathbb{A}^n$ eine affine Varietät. Das *Ideal von V* ist gegeben durch $I(V) := \{f \in \overline{K}[x_1, \ldots, x_n] \mid f(P) = 0 \; \forall P \in V\}$. V ist dann definiert über K, Notation V/K, wenn $I(V)$ durch Funktionen aus $K[x_1, \ldots, x_n]$ erzeugt wird. Der *affine Koordinatenring* von V/K ist definiert als $K[V] := K[x_1, \ldots, x_n]/I(V/K)$. Der *Funktionenkörper* von V/K ist der Körper

$K(V) :=$ Quot $(K[V])$. Analog definieren wir $\overline{K}[V]$ bzw. $\overline{K}(V)$ durch Ersetzen von K durch $\overline{K}$.

1.4 Bemerkung. Da $I(V)$ tatsächlich wieder ein Primideal ist, ist $K[V]$ ein Integritätsring. Somit ist $K(V)$ wohldefiniert.

1.5 Bemerkung. Ein Element $f \in \overline{K}[V]$ induziert eine Funktion $f : V \to \overline{K}$: Sind $f_1, f_2 \in \overline{K}[x_1, \ldots, x_n]$ mit $f_1 \sim f_2$, dann ist $f_1 = f_2 + g$ für ein $g \in I(V/K)$, also gilt für alle $P \in V : f_1(P) = (f_2 + g)(P) = f_2(P) + g(P) = f_2(P)$ wegen $g(P) = 0$.

Wir betrachten ab sofort nur noch Varietäten $V \subseteq \mathbb{A}^n$, deren Ideale von einem Polynom $f \in K[x_1, \ldots, x_n]$ erzeugt werden. In diesem Fall gilt folgende

1.6 Definition. Sei $V \subseteq \mathbb{A}^n$ eine affine Varietät mit $I(V) = (f), f \in K[x_1, \ldots, x_n]$. Ein Punkt $P \in V$ heisst *singulär*, wenn $\partial f/\partial x_1(P) = \cdots = \partial f/\partial x_n(P) = 0$, also alle partiellen Ableitungen von f in P verschwinden. Ein nicht-singulärer Punkt heisst auch *regulär*. Ist jeder Punkt von V regulär, so heisst V eine *glatte Varietät*.

1.7 Definition. Sei V eine affine Varietät, $P \in V$. Der *lokale Ring an P* ist der Ring
$\overline{K}[V]_P := \{\frac{f}{g} \in \overline{K}(V) \mid g(P) \neq 0\}$.

Der lokale Ring an $P \in V$ enthält also alle in P definierten Funktionen.

1.8 Definition. Der *projektive Raum der Dimension n über K* ist die Menge $\mathbb{P}^n := \{(x_0, \ldots, x_n) \in \mathbb{A}^{n+1} \mid \exists i \in \{0, \ldots, n\} : x_i \neq 0\}/\sim$ mit

$$(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n) \Leftrightarrow \exists \lambda \in \overline{K}^* : x_i = \lambda y_i \ \forall i.$$

Wir bezeichnen die Äquivalenzklasse $\{(\lambda x_0, \ldots, \lambda x_n) \mid \lambda \in \overline{K}^*\}$ mit $[x_0, \ldots, x_n]$.

1.9 Definition. Ein Polynom $f \in K[x_0, \ldots, x_n]$ heisst *homogen (vom Grad d)*, $d \in \mathbb{N}$, wenn $f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n)$ für alle $\lambda \in K$ gilt.

Es ist zwar für ein homogenes Polynom $f \in K[x_0, \ldots, x_n]$ das Bild eines Punktes $P \in \mathbb{P}^n$ abhängig von der Wahl des Repräsentanten für P, jedoch sind die Nullstellen von f davon unabhängig. Deshalb macht die folgende Definition Sinn:

1.10 Definition. Sei $f \in K[x_0, \ldots, x_n]$ ein homogenes Primpolynom. Dann definiert f eine *projektive Varietät*
$V_{(f)} := \{P \in \mathbb{P}^n \mid f(P) = 0\}$. Das *Ideal einer projektiven Varietät* $I(V)$ wird analog zum affinen Fall definiert. Wird $I(V)$ durch ein homogenes Polynom in $K[x_0, .., x_n]$ erzeugt, so nennen wir V wieder eine über K definierte projektive Varietät (Notation V/K).

1.11 Bemerkung. Man kann $\mathbb{A}^n$ mithilfe der Abbildungen

$$\varphi_i : \mathbb{A}^n \to \mathbb{P}^n, (x_1, \ldots, x_n) \mapsto [x_1, \ldots, x_{i-1}, 1, x_i, \ldots, x_n], i \in \{1, \ldots, n\}$$

in $\mathbb{P}^n$ einbetten. Definiert man für ein $i \in \{0, \ldots, n\}$ die Menge
$U_i := \{P = [x_0, \ldots, x_n] \in \mathbb{P}^n \mid x_i \neq 0\}$, so kann man φ_i umkehren:

$$\varphi_i^{-1} : U_i \to \mathbb{A}^n, [x_0, \ldots, x_n] \mapsto (\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}).$$

Sei $V \subseteq \mathbb{P}^n$ eine projektive Varietät. Wir wählen $i \in \{0 \ldots n\}$ so, dass
$\varphi_i^{-1}(V \cap U_i) \neq \varnothing$. Diese Menge ist dann eine affine Varietät, welche wir mit $V \cap \mathbb{A}^n$ bezeichnen.
Das Ideal von $V \cap \mathbb{A}^n$ ist dann

$$I(V \cap \mathbb{A}^n) := \{f(X_1, \ldots, X_{i-1}, 1, X_{i+1}, \ldots, X_n \mid f \in I(V)\},$$

es enthält also alle Polynome in $I(V)$, diese werden allerdings durch Setzen von $X_i := 1$ von Polynomen in $n+1$ Variablen in Polynome in n Variablen umgewandelt. Diesen Prozess nennt man *Dehomogenisierung*. Andersherum wird $f(x_1, \ldots, x_n)$ durch

$$f^*(X_0, \ldots, X_n) = X_i^d f(\frac{X_0}{X_i}, \ldots, \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i}, \ldots, \frac{X_n}{X_i}),\ d = \deg(f)$$

zu einem homogenen Polynom f^*. Diesen umgekehrten Prozess nennt man *Homogenisierung von f bezüglich X_i.*

1.12 Beispiel. Homogenisierung eines kubischen Polynoms
Sei $f := y^2 - x^3 - ax - b,\ a, b \in K$ ein kubisches Polynom in $K[x, y]$. Die Homogenisierung von f bzgl. z ist dann gegeben durch
$f^*(x, y, z) = z^3 f(\frac{x}{z}, \frac{y}{z}) = z^3(\frac{y^2}{z^2} - \frac{x^3}{z^3} - a\frac{x}{z} - b) = y^2 z - x^3 - axz^2 - bz^3$.

1.13 Definition. Sei $V \subseteq \mathbb{A}^n$ eine affine Varietät. Man kann V durch die Einbettung φ_i mit einer (bis auf Variablenvertauschung) eindeutig bestimmten projektiven Varietät identifizieren, deren Ideal durch $\{f^*(x_0, \ldots, x_n) \mid f \in I(V)\}$ erzeugt wird. Wir nennen diese projektive Varietät den *projektiven Abschluss von* V (Notation: $\overline{V}$). Es gilt: $V = \overline{V} \cap \mathbb{A}^n$. Die Elemente von $\overline{V} \backslash V$ nennen wir *Punkte im Unendlichen* von V. Dies sind dann genau die Punkte $[x_0, \ldots, x_n] \in \overline{V}$ mit $x_i = 0$.

1.14 Bemerkung. Ist V eine projektive Varietät und $V \cap \mathbb{A}^n \neq \varnothing$, dann gilt $V = \overline{V \cap \mathbb{A}^n}$

1.15 Definition. Sei $V/K \subseteq \mathbb{P}^n$ eine projektive Varietät. Der *Funktionenkörper von* V ist dann definiert als $K(V) := K(V \cap \mathbb{A}^n)$.

1.16 Bemerkung. Für zwei verschiedene invertierte Einbettungen $\varphi_i^{-1}, \varphi_j^{-1}$ erhalten wir unterschiedliche Funktionenkörper, diese sind jedoch isomorph.

1.17 Definition. Sei $V \subseteq \mathbb{P}^n$ eine projektive Varietät, $P = [x_0, \ldots, x_n] \in V$. Wir wählen $\mathbb{A}^n \subseteq \mathbb{P}^n$ (mittels passender Einbettung φ_i) so, dass $P \in \mathbb{A}^n$ (also $x_i \neq 0$). P heisst *glatter Punkt von* V, wenn P (bzw. $\varphi^{-1}(P) = (\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i})$) in $V \cap \mathbb{A}^n$ ein glatter Punkt ist.
Der *lokale Ring an* P, Notation $\overline{K}[V]_P$, ist der lokale Ring von $V \cap \mathbb{A}^n$ an P. Eine Funktion $f \in \overline{K}(V)$ heisst *regulär in* $P \in V$, wenn $f \in \overline{K}[V]_P$, denn dann ist f in P definiert.

1.18 Definition. Die *Dimension* einer affinen Varietät V/K ist gegeben als der Transzendenzgrad von $\overline{K}(V)/\overline{K}$, die einer projektiven Varietät V/K als Dimension von $V \cap \mathbb{A}^n$. Varietäten der Dimension 1 heissen *Kurven*.

1.19 Bemerkung. Da uns in dieser Arbeit nur elliptische Kurven interessieren, welche per Definition (siehe unten) nichtsingulär sind, beschränken wir unsere Betrachtungen im Folgenden auf nichtsinguläre Kurven, also Kurven, welche nur glatte Punkte haben.

1.2 Algebraische Funktionenkörper

Dieser Abschnitt enthält die für unsere Zwecke notwendigen grundlegenden Definitionen und Sätze über algebraische Funktionenkörper. Als Beispiel für einen Funktionenkörper haben wir dabei immer den Funktionenkörper einer Kurve im Hinterkopf.

1.20 Definition. Ein *(algebraischer) Funktionenkörper (in einer Variablen) über einem Körper* K, Notation F/K, ist eine endliche algebraische Erweiterung von $K(x)$. Wir nennen $\widetilde{K} := \{x \in F \mid x \text{ algebraisch über } K\}$ den *Konstantenkörper von* F. Der Körper K heisst *voller Konstantenkörper von* F/K, wenn $K = \widetilde{K}$.

1.21 Bemerkung. Wir betrachten im Folgenden nur noch primitive Erweiterungen von $K(x)$, d.h. wir können F/K immer schreiben als $F/K = K(x, y)$ mit $y \in F$.

1.22 Beispiel. Für eine affine Kurve V/K mit $I(V) = (f(x_1, x_2))$ für ein Primpolynom $f(x_1, x_2) \in K[x_1, x_2]$ ist der Funktionenkörper $K(V)$ auch im Sinne der

Definition 1.20 ein Funktionenkörper: Sei $n = \deg_{x_2}$. Wir schreiben

$$f(x_1, x_2) = \sum_{i=0}^{n} g_i(x_1) x_2^i$$

mit Polynomen $g_i \in K(x)$, dann ist $K(V) \cong K(x)(y)$ für eine Nullstelle y dieses Polynoms, da $f \equiv 0$ in $K(V)$.

1.23 Definition. Eine *diskrete exponentielle Bewertung* von F/K ist eine Abbildung $v : F \to \mathbb{Z} \cup \{\infty\}$ mit folgenden Eigenschaften:

(*i*) $\forall a \in F : v(a) = \infty \Leftrightarrow a = 0$.

(*ii*) $\forall a, b \in F : v(ab) = v(a) + v(b)$.

(*iii*) $\forall a, b \in F : v(a + b) \geq \min(v(a), v(b))$.

(*iv*) $\exists z \in F : v(z) = 1$.

(*v*) $v(x) = 0 \ \forall x \in K^*$.

1.24 Definition. Ein *diskreter Bewertungsring* von F/K ist ein Ring $\mathcal{O}$, so dass

- $K \subsetneq \mathcal{O} \subsetneq F$
- $\forall x \in F : x \in \mathcal{O} \vee x^{-1} \in \mathcal{O}$

Da wir nur diskrete exponentielle Bewertungen und diskrete Bewertungsringe betrachten, schreiben wir ab jetzt nur Bewertung bzw. Bewertungsring und meinen damit aber eine diskrete exponentielle Bewertung bzw. einen diskreten Bewertungsring.

1.25 Bemerkung. Zusammenhang zwischen Bewertungsringen und Bewertungen
Man kann mithilfe eines Bewertungsrings $\mathcal{O}$ von F/K eine Bewertung v auf F/K definieren:
Bewertungsringe sind immer sowohl Hauptidealringe als auch lokale Ringe (siehe [Sti93], I.1.5 und I.1.6). Es gibt also ein maximales Ideal $\mathfrak{p}$ von $\mathcal{O}$, welches von einem (bis auf Einheiten von $\mathcal{O}$ eindeutig bestimmten) Element $t \in \mathcal{O}$, dem sogenannten *uniformisierenden Element*, erzeugt wird: $\mathfrak{p} = t\mathcal{O}$.
Man kann zeigen, dass sich dann jedes Element $a \in F^*$ eindeutig als $a = t^n \frac{r_1}{r_2}$ mit $n \in \mathbb{Z}, r_1, r_2 \in \mathcal{O}^*$ schreiben lässt. Wir definieren $v_{\mathcal{O}}(t^n r) := n$ und $v_{\mathcal{O}}(0) := \infty$. Die Abbildung $v_{\mathcal{O}}$ erfüllt dann alle Eigenschaften einer Bewertung und ist unabhängig von der Wahl von t.
Hat man andererseits eine Bewertung v auf F/K gegeben, so definiert man den zu v gehörigen Bewertungsring als $\mathcal{O}_v := \{x \in F \mid v(x) \geq 0\}$.

1.26 Definition. Eine *Stelle* P eines Funktionenkörpers F/K ist das maximale Ideal eines Bewertungsrings von F/K. Wir bezeichnen die Menge der Stellen von F/K mit $\mathbb{P}_F$.

Ist eine Stelle $P \in \mathbb{P}_F$ gegeben, dann ist der zugehörige Bewertungsring eindeutig bestimmt durch $\mathcal{O}_P := \{z \in F \mid z^{-1} \notin P\}$. Die zu $\mathfrak{p}$ gehörige Bewertung $v_\mathfrak{p}$ erhält man wieder wie oben in der Bemerkung über ein uniformisierendes Element. Hat man andererseits eine Bewertung v auf F/K gegeben, so erhält man die zugehörige Stelle durch $P := \{x \in F \mid v(x) > 0\}$.

1.27 Definition. Der *Grad* von P wird definiert durch $\deg(P) := [\mathcal{O}_P/P : K]$.

1.28 Definition. Die *Divisorengruppe* $\mathcal{D}_F$ eines Funktionenkörpers F/K ist die Menge der formalen Summen von Stellen:

$$\mathcal{D}_F := \{ \sum_{P_i \in \mathbb{P}_F} a_i P_i \mid a_i \in \mathbb{Z}, a_i \neq 0 \text{ nur für endlich viele } i\}.$$

Für $D_1, D_2 \in \mathcal{D}_F$ mit $D_1 = \sum\limits_{P_i \in \mathbb{P}_F} a_i P_i,\ D_2 = \sum\limits_{P_i \in \mathbb{P}_F} b_i P_i$, definieren wir

$$D_1 + D_2 := \sum_{P_i \in \mathbb{P}_F} (a_i + b_i) P_i.$$

Damit ist $\mathcal{D}_F$ offensichtlich eine Gruppe mit neutralem Element $(0) := \sum\limits_{P_i \in \mathbb{P}_F} 0 P_i$.
Der *Grad* eines Divisors $D = \sum\limits_{P_i \in \mathbb{P}_F} a_i P_i$ ist $\deg(\mathrm{D}) := \sum\limits_{P_i \in \mathbb{P}_F} a_i \deg(P_i)$.

1.29 Definition. $P \in \mathbb{P}_F$ heisst *Nullstelle* (*Polstelle*) von $f \in F$, wenn $v_P(f) > 0$ ($v_P(f) < 0$). Der *Hauptdivisor* von $x \in F$ ist definiert als $(x) := \sum_{P_i \in \mathbb{P}_F} v_{P_i}(x) P_i$. Man kann zeigen, dass jedes $x \in F$ nur endlich viele Nullstellen und Polstellen hat, deshalb ist die Menge der Hauptdivisoren P_F, welche eine Gruppe ist wegen $(xy) = (x) + (y)\ \forall x, y \in F$, eine Untergruppe von $\mathcal{D}_F$. Wir nennen $\mathcal{C}_F := \mathcal{D}_F/P_F$ die *Divisorenklassengruppe* von F/K. Für $D_1, D_2 \in D_F$ gilt also $D_1 \sim D_2 \Leftrightarrow D_1 = D_2 + (x)$ für ein $x \in F$.

1.30 Definition. Wir definieren den *Riemann-Roch-Raum* von $A \in \mathcal{D}_F$ als $\mathcal{L}(\mathcal{A}) := \{x \in F^* \mid A + (x) \geq (0)\} \cup \{0\}$.

Die Ungleichung in der Definition ist folgendermassen zu verstehen: Für zwei Divisoren $D_1 = \sum\limits_{P_i \in \mathbb{P}_F} a_i P_i$ und $D_2 = \sum\limits_{P_i \in \mathbb{P}_F} b_i P_i$ gilt $D_1 \geq D_2 \Leftrightarrow a_i \geq b_i$ für alle i.
Für den Riemann-Roch-Raum gilt folgender

1.31 Satz. *Für alle $A \in \mathcal{D}_F$ gilt: $\mathcal{L}(A)$ ist ein endlich-dimensionaler K-Vektorraum.*

Beweis. Siehe [Sti93], Proposition I.4.9. □

Deshalb ist die folgende Definition sinnvoll:

1.32 Definition. Wir setzen $dim(A) := dim_K \mathcal{L}(\mathcal{A})$.

Eine wichtige Kennzahl eines Funktionenkörpers ist das Geschlecht:

1.33 Definition. Das *Geschlecht* eines Funktionenkörpers F/K ist definiert durch $g := \max\{\deg A - \dim A + 1 \mid A \in \mathcal{D}_F\}$.

1.3 Elliptische Kurven und elliptische Funktionenkörper

1.34 Definition. Sei F/K ein Funktionenkörper vom Geschlecht g mit einem Divisor $A \in \mathcal{D}_F$ vom Grad eins. Im Fall $g = 0$ heisst F/K ein *rationaler Funktionenkörper*, im Fall $g = 1$ ein *elliptischer Funktionenkörper*.

1.35 Definition. Eine *elliptische Kurve* ist eine glatte projektive Kurve E/K, deren Funktionenkörper $K(E)$ vom Geschlecht eins ist.

1.36 Bemerkung. In dieser Arbeit werden im Folgenden nur elliptische Kurven behandelt. Daher meinen wir, wenn wir Kurven schreiben, immer elliptische Kurven.

1.37 Bemerkung. Sei E/K eine elliptische Kurve mit Ideal $I(V) = (g)$, $g \in K[x, y, z]$. Wir schreiben ab jetzt g dehomogenisiert nach z, ausserdem die Punkte von E als Elemente von $E \cap \mathbb{A}^n$, also $[x, y, z]$ als $(\frac{x}{z}, \frac{y}{z})$. Den „Punkt im Unendlichen“ $[0, 1, 0]$ bezeichnen wir dann mit O.

Die folgenden Sätze aus [Sti93], Proposition VI.1.2 und Proposition VI.1.3, verdeutlichen die Gestalt eines elliptischen Funktionenkörpers.

1.38 Satz. *Sei F/K ein elliptischer Funktionenkörper.*

(a) Wenn $\mathrm{char}(K) \neq 2$*, dann gibt es $x, y \in F$ so dass $F = K(x, y)$ und $y^2 = f(x)$ für ein quadratfreies Polynom $f(x) \in K[x]$ vom Grad* 3.

(b) Wenn $\mathrm{char}(K) = 2$*, dann gibt es $x, y \in F$ so dass $F = K(x, y)$ und*

$$\begin{aligned} y^2 + y &= f(x), f(x) \in K[x] \text{mit } deg(f) = 3 \\ \text{oder } y^2 + y &= x + \frac{1}{ax + b},\ a, b \in K, a \neq 0. \end{aligned}$$

1.39 Satz. *Sei K ein Körper. Eine Gleichung der Form*

(a) $y^2 = f(x), f(x) \in K[x]$ *quadratfrei mit* $\deg(f) = 3, \mathrm{char}(K) > 2$*, oder*

(b)

$$\begin{aligned} y^2 + y &= f(x), f(x) \in K[x] \text{ mit } deg(f) = 3 \\ \text{oder } y^2 + y &= x + \frac{1}{ax+b},\ a, b \in K, a \neq 0, \mathrm{char}(K) = 2 \end{aligned}$$

definiert einen elliptischen Funktionenkörper $F = K(x, y)$.

1.40 Definition. Sei E/K eine elliptische Kurve mit Ideal (f), $\widetilde{K}$ ein algebraischer Erweiterungskörper von K. Die *Punktgruppe der elliptischen Kurve E/K* über dem Körper $\widetilde{K}$ ist die Menge

$$E(\widetilde{K}) := \{(x, y) \in \mathbb{A}^2(\widetilde{K}) \mid f(x, y) = 0\} \cup \{O\}.$$

$E(\widetilde{K})$ bildet eine kommutative Gruppe mit Operation $+$ (siehe [Sil86], III.2, für explizite Formeln) und neutralem Element O.

Über die Kardinalität der Punktgruppen einer elliptischen Kurve über einem endlichen Körper kann man folgende Aussage machen:

1.41 Satz. *(Hasse):*
Sei $E/\mathbb{F}_q$ eine elliptische Kurve. Dann gilt für alle $r \in \mathbb{N}^{\geq 1}$:

$$|\#E(\mathbb{F}_{q^r}) - (q^r + 1)| \leqslant 2\sqrt{q^r}.$$

Beweis. [Sil86], Theorem V.1.1. □

1.42 Definition. Sei E/K eine elliptische Kurve, $m \in \mathbb{Z}$.
Die *m-Torsionsuntergruppe* von E ist die Menge

$$E[m] := \{P \in E(\overline{K}) \mid mP = O\}.$$

Ausserdem definieren wir $E(\widetilde{K})[m] := E(\widetilde{K}) \cap E[m]$ für einen algebraischen Erweiterungskörper $\widetilde{K}$ von K.

1.43 Definition. Sei $P = (x, y) \in E(\overline{K})$. Wir definieren die *Koordinatenabbildungen* $X, Y : E(\overline{K})\backslash\{O\} \to \overline{K}$ durch $X(P) := x, Y(P) := y$.

1.44 Definition. Eine elliptische Kurve $E/\mathbb{F}_{p^r}$ heisst *supersingulär*, wenn $E[(p^r)^n] = O$ für ein (und dann für alle) $n \in \mathbb{N}$ gilt, andernfalls heisst E *ordinär*.

Die Punkte einer elliptischen Kurve E/K entsprechen eineindeutig den Stellen vom Grad eins des Funktionenkörpers $K(E)$:
Sei $(r,s) \in E(K)$, sei E definiert durch $y^2 = f(x), f(x) \in K[x]$ quadratfrei vom Grad 3. (Wir nehmen, um die Notation zu vereinfachen, $\mathrm{char}(K) > 2$ an, der Fall $\mathrm{char}(K) = 2$ funktioniert analog.) Sei $K(E) = K(x)(y)$ mit $y^2 = f(x)$ der zugehörige elliptische Funktionenkörper. Dann gilt: Das Ideal

$$I = (x-r)K[x,y] + (y-s)K[x,y]$$

ist ein Primideal in $K[x,y]$. Durch Lokalisierung erhalten wir einen lokalen Ring $\mathcal{O}_I := \frac{K[x,y]}{K[x,y]\setminus I}$, welcher isomorph zu einem Bewertungsring von $K(E)$ ist. Das maximale Ideal von $\mathcal{O}_I$ ist $P_I := I\mathcal{O}_I$. Der Punkt O ergibt sich aus der Stelle vom Grad eins des Gradbewertungsrings von $K(E)$, also des Bewertungsrings, welchen man durch Anwendung des in 1.25 beschriebenen Verfahrens für die Fortsetzung v_∞ der Gradbewertung auf $K[x]$ erhält. Die zugehörige Stelle bezeichnen wir mit P_∞. Dies sind alle Stellen von $K(E)$ vom Grad eins (dies folgt aus der Betrachtung der Stellen vom Grad eins des rationalen Funktionenkörpers $K(x)$ und der Tatsache, dass alle Stellen vom Grad ein von $K(E)$ über einer Stelle vom Grad eins von $K(x)$ liegen müssen, siehe [Sti93] für eine detailliertere Erklärung). Wir bezeichnen die aus $P \in E(K)$ auf diese Weise resultierende Stelle vom Grad eins mit (P).
Hat man eine Stelle $P \in \mathbb{P}_F\setminus\{P_\infty\}$ mit $\deg(P) = 1$ gegeben, so gibt es eine eindeutige Darstellung $P = (x-r)K[x,y] + (y-s)K[x,y]$, P korrespondiert also zu dem Punkt (r,s). Desweiteren gilt

$$(P+Q) - (O) \sim (P) - (O) + (Q) - (O)\ \forall P, Q \in E(K),$$

die Addition von Punkten nach dem Gruppengesetz in $E(K)$ und die Addition von Elementen der Divisorenklassengruppe sind demnach äquivalent.
Das oben beschriebene Verfahren zur Umwandlung von Punkten in Stellen bzw. Stellen in Punkten kann man für eine über K definierte Kurve E/K mit zugehörigem elliptischen Funktionenkörper $K(x,y)$ auch auf die Punktgruppe $E(\widetilde{K})$ von E über einem algebraischen Erweiterungskörper $\widetilde{K}$ anwenden. Der passende elliptische Funktionenkörper ist dann $\widetilde{K}(x,y)$.

1.45 Bemerkung. Die Elemente eines elliptischen Funktionenkörpers $K(E)$ kann man sich auch als Funktionen in den Stellen $\mathbb{P}_F$ bzw. in den Punkten $E(K)$ der Kurve in den Grundkörper vorstellen: Sei $P = (r,s) \in E(K),\ f \in K(E)$. Dann ist f von der Form $f = \frac{g}{h}$ mit $g, h \in K[x,y]$. Sei $\mathfrak{p}$ die aus P resultierende Stelle, dann ist f ist also genau dann in P definiert, wenn $f \in \mathcal{O}_\mathfrak{p}$. Dies bedeutet aber, dass es $g, h \in K[x]$ gibt mit $f = \frac{g}{h}$ und $h(r,s) \neq 0$. In diesem Fall setzen wir $f(P) := \frac{g(r,s)}{h(r,s)}$. In dieser Situation nennen wir f auch *regulär* an P.

Diese Korrespondenz zwischen elliptischen Kurven und ihren Punkten auf der einen Seite und Funktionenkörpern und ihren Stellen vom Grad eins auf der anderen Seite erlaubt es uns, beide Repräsentationen einer elliptischen Kurve zu benutzen, je nachdem, welche Darstellung für unsere Zwecke hilfreicher ist.

1.4 Invarianten elliptischer Kurven

Hier definieren wir einige wichtige Invarianten elliptischer Kurven, auf die wir später oft zurückgreifen werden. Als besonders aussagekräftig wird sich die j-Invariante herausstellen.
Sei $E : Y^2+a_1XY+a_3Y = X^3+a_2X^2+a_4X+a_6,\ a_i \in K$ eine elliptische Kurve in *Weierstrass-Form*. Man kann jede elliptische Kurve in diese Form bringen, dazu aber später mehr.

1.46 Definition. Wir definieren
$b_2 := a_1^2 + 4a_2$
$b_4 := 2a_4 + a_1a_3$
$b_6 := a_3^2 + 4a_6$
$b_8 := a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$
$c_4 := b_2^2 - 24b_4$
$c_6 := -b_2^3 + 36b_2b_4 - 216b_6$
$\Delta := -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$ (*Diskriminante von E*).
Falls $\Delta \neq 0$, dann ist $j := c_4^3/\Delta$ die *j-Invariante von E*. Diese werden wir auch oft mit $j(E)$ bezeichnen.

1.47 Proposition. *Für eine Kurve wie oben gilt: E ist glatt* $\Leftrightarrow \Delta \neq 0$.

Beweis. Siehe [Sil86], Proposition III.1.4. □

Die Diskriminante einer elliptischen Kurve E/K ist also immer $\neq 0$, da E per Definition eine glatte Kurve ist. Deshalb ist auch die j-Invariante immer definiert.

Kapitel 2

Isogenien

2.1 Grundlagen

In diesem Abschnitt werden Isogenien definiert und einige wichtige Eigenschaften vorgestellt. Für die exakte Definition benötigen wir noch einmal die projektive Schreibweise einer elliptischen Kurve.

2.1 Definition. Seien $E_1,\ E_2$ elliptische Kurven über demselben Körper K. Eine *rationale Abbildung* $\varphi : E_1 \to E_2$ wird durch $\varphi = [f_0, f_1, f_2], f_i \in \overline{K}(E_1)\backslash\{0\}$ gegeben. Eine rationale Abbildung $\varphi : E_1 \to E_2$ heisst *regulär in* $P \in E_1$, wenn es eine Funktion $g \in \overline{K}(E_1)$ gibt, so dass

(*i*) gf_i regulär an P für alle $i \in \{0, 1, 2\}$ und

(*ii*) es gibt ein $i \in \{0, 1, 2\}$ mit $gf_i(P) \neq 0$

Dann setzen wir $\varphi(P) := [gf_0(P), gf_1(P), gf_2(P)]$.
Eine Abbildung $\varphi : E_1 \to E_2$ welche an jedem Punkt $P \in E_1$ regulär (also auswertbar) ist, heisst ein *Morphismus*.
Eine *Isogenie* ist ein Morphismus $\varphi : E_1 \to E_2$ mit $\varphi([0, 1, 0]) = [0, 1, 0]$. Eine Isogenie $\varphi = [f_0, f_1, f_2] : E_1 \to E_2$ heisst *definiert über* K oder auch *K-Isogenie*, wenn $f_i \in K(E_1)$ für alle $i \in \{0, 1, 2\}$. Existiert eine nicht-konstante Isogenie zwischen E_1 und E_2, so heissen E_1 und E_2 *isogen*.

2.2 Bemerkung. Die einzige konstante Isogenie ist

$$[0] : E_1 \to E_2,\ [0](P) = [0, 1, 0] \text{ für alle } P \in E_1.$$

Da wir nur glatte Kurven betrachten, ist folgender Satz hilfreich:

2.3 Proposition. *Seien C_1 und C_2 Kurven, $\varphi : E_1 \to E_2$ eine rationale Abbildung und $P \in E_1$ ein glatter Punkt. Dann ist φ regulär in P.*

Beweis. Siehe [Sil86], Prop II.2.1. □

Alle rationalen Abbildungen zwischen glatten Kurven sind also Morphismen, das heisst an jedem Punkt auswertbar.

Da wir Kurven und Punkte in affiner Darstellung schreiben, werden wir auch Isogenien auf diese Weise darstellen:
Sei $\varphi : E_1 \to E_2,\ \varphi = [f_0, f_1, f_2], f_i \in \overline{K}(E_1)$ eine Isogenie. Sei φ_2 die in Bemerkung 1.11 definierte Einbettungsabbildung. Die affine Schreibweise eines Punktes $P = [X, Y, Z]$ ist

$$\varphi_2^{-1}(P) = \begin{cases} O & \text{falls } Z = 0 \\ \left(\frac{X}{Z}, \frac{Y}{Z}\right) & \text{sonst} \end{cases}$$

also ist $\varphi(P) = [f_0(P), f_1(P), f_2(P)]$ in affiner Schreibweise $\left(\frac{f_0(P)}{f_2(P)}, \frac{f_1(P)}{f_2(P)}\right)$.
Dieser Ausdruck ist genau dann nicht definiert, wenn $\varphi(P) = O$, denn dann ist $f_2(P) = 0$ wegen $O = [0, 1, 0]$. Für alle $(X, Y, Z) = P \in E_1 \backslash \{O\}$ gilt
$P \sim \left(\frac{X}{Z}, \frac{Y}{Z}, 1\right)$. Wir setzen also $Z := 1$ in allen f_i, schreiben
$\varphi = [f_0(X, Y, 1), f_1(X, Y, 1), f_2(X, Y, 1)]$ als

$$\varphi = \left[\frac{f_0(X,Y,1)}{f_2(X,Y,1)}, \frac{f_1(X,Y,1)}{f_2(X,Y,1)}\right] = \left[\frac{g_1(x,y)}{h(x,y)}, \frac{g_2(x,y)}{h(x,y)}\right]$$

und definieren

$$\begin{aligned} \varphi(O) &:= O, \\ \varphi(x,y) &:= \begin{cases} O & \text{falls } h(x,y) = 0 \\ \left(\frac{g_1(x,y)}{h_1(x,y)}, \frac{g_2(x,y)}{h_2(x,y)}\right) & \text{sonst.} \end{cases} \end{aligned}$$

Eine sehr wichtige Eigenschaft von Isogenien ist, dass sie Homomorphismen der Punktgruppen induzieren:

2.4 Satz. *Sei $\varphi : E_1 \to E_2$ eine Isogenie und seien $P, Q \in E_1$. Dann gilt:*

$$\varphi(P + Q) = \varphi(P) + \varphi(Q)$$

.

Beweis. Siehe [Sil86], Theorem III.4.8. □

Die Isogenien zwischen zwei Kurven E_1 und E_2 bilden eine kommutative Gruppe $(\mathrm{Hom}(E_1, E_2), +)$ mit $(\varphi + \psi)(P) := \varphi(P) + \psi(P)$ und neutralem Element $[0]$. Die Komposition von Isogenien ist auch möglich, wenn Zielkurve der ersten und Ausgangskurve der zweiten Isogenie übereinstimmen: $\varphi : E_1 \to E_2, \psi : E_2 \to E_3$, dann ist $\psi \circ \varphi : E_1 \to E_3, P \mapsto \psi(\varphi(P))$.
Die folgende Definition und den nächsten Satz benötigen wir für die Definition des Grades einer Isogenie.

2.5 Definition. Seien $E_1/K, E_2/K$ elliptische Kurven, $\varphi : E_1 \to E_2$ eine nichtkonstante, über K definierte Isogenie. Dann induziert φ einen Körpermonomorphismus

$$\varphi^* : K(E_2) \to K(E_1), \psi \mapsto \psi \circ \varphi.$$

2.6 Satz. *Seien E_1, E_2 elliptische Kurven und sei $\varphi : E_1 \to E_2$ eine nichtkonstante, über K definierte Isogenie. Dann gilt $[K(E_1) : \varphi^*(K(E_2)] < \infty$.*

Beweis. Siehe [Sil86], Theorem II.2.4. □

2.7 Definition. Sei $\varphi : E_1 \to E_2$ eine Isogenie. Ist φ konstant, so setzen wir $\deg(\varphi) := 0$, ansonsten definieren wir $\deg(\varphi) := [K(E_1) : \varphi^*(K(E_2)]$. Ausserdem nennen wir φ *separabel (inseparabel)*, wenn die Körpererweiterung $K(E_1)/\varphi^*(K(E_2))$ die entsprechende Eigenschaft besitzt. Der Separabilitätsgrad von φ ist gegeben durch $\deg_s(\varphi) = \deg_s(K(E_1)/\varphi^*(K(E_2)))$, analog $\deg_i$.

2.8 Definition. Eine Isogenie $\varphi : E_1 \to E_2$ heisst ein *Isomorphismus*, wenn es eine Isogenie $\psi : E_2 \to E_1$ gibt, so dass $\varphi \circ \psi = \mathrm{id}_{E_1}$. Wir nennen dann E_1 und E_2 *isomorph* (Notation: $E_1 \cong E_2$).

2.9 Korollar. *Sei $\varphi : E_1 \to E_2$ eine Isogenie vom Grad eins. Dann ist φ ein Isomorphismus.*

Beweis. Siehe [Sil86], Corollary II.2.4.1. □

Nun kommen wir noch einmal auf die in Abschnitt 1.4 angesprochene Weierstrass-Form zurück:

2.10 Satz. *Sei E/K eine elliptische Kurve.*

(a) Es gibt Funktionen $x, y \in K(E)$, so dass die Abbildung

$$\varphi : E \to \mathbb{P}^2, \varphi(P) = \begin{cases} [x(P), y(P), 1] & \text{für } P \neq O \\ [0, 1, 0] & \text{sonst} \end{cases}$$

einen Isomorphismus von E/K auf eine Kurve in Weierstrass-Form

$$C : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,\ a_i \in K$$

definiert.

(b) Jede glatte Kurve in Weierstrass-Form ist eine elliptische Kurve.

Beweis. Siehe [Sil86], Proposition III.3.1. □

2.11 Bemerkung. Für E/K mit $\mathrm{char}(K) > 3$ kann man auch immer eine isomorphe Kurve $E' : Y^2 = X^3 + aX + b$ finden. Eine Kurve in dieser Form werden wir als in *kurzer Weierstrass-Form* bezeichnen.

2.12 Satz. *Sei $\varphi : E_1 \to E_2$ eine Isogenie. Dann ist φ entweder konstant (also $= [0]$) oder surjektiv.*

Beweis. Siehe [Sil86], Theorem II.2.3. □

Nun folgt ein Satz, der später eine wichtige Rolle in der Berechnung von Isogenien spielen wird:

2.13 Satz. *Sei E/K eine elliptische Kurve, sei $G \subseteq E(\overline{K})$ eine endliche Untergruppe. Dann gibt es eine (bis auf Isomorphie) eindeutig bestimmte elliptische Kurve E' und eine separable Isogenie $\varphi : E \to E'$ mit $\ker(\varphi) = G$.*

Beweis. Siehe [Sil86], Proposition III.4.12. □

Die Kurve E' wird auch oft mit E/G bezeichnet.

2.14 Definition. Sei E/K eine elliptische Kurve. Ein *Endomorphismus* ist eine Isogenie $\varphi : E \to E$. Der *Endomorphismenring* von E ist die Menge
$\mathrm{End}(E) := \{\varphi : E \to E \mid \varphi \text{ Isogenie}\}$ aller Endomorphismen von E, zusammen mit der oben beschriebenen Addition und der Komposition als Multiplikationsabbildung. Die Menge $\mathrm{End}_{\widetilde{K}}(E)$ ist die Menge aller Endomorphismen von E mit Koeffizienten in $\widetilde{K}$.

Ein sehr wichtiger Endomorphismus elliptischer Kurven über endlichen Körpern ist der folgende:

2.15 Definition. Sei $E/\mathbb{F}_q$ eine elliptische Kurve. Dann ist $\pi : E \to E$,

$$P \mapsto \begin{cases} O & \text{wenn } P = O \\ (x^q, y^q) & \text{wenn } P = (x, y) \end{cases}$$

der *Frobenius-Endomorphismus* von E.

Ein Punkt $P \in E$ wird durch π tatsächlich wieder auf einen Punkt $Q \in E$ abgebildet: Sei $E/\mathbb{F}_q$ eine elliptische Kurve, $P = (x_P, y_P) \in E$ und $I(E) = (f)$ mit $f \in \mathbb{F}_q[x, y]$. Es ist also

$$f(x_P, y_P) = 0 = (f(x_P, y_P))^q = f(x_P^q, y_P^q),$$

da $f \in \mathbb{F}_q[x, y]$, also $(x_P^q, y_P^q) \in E$.

2.16 Definition. Wir nennen $t := q + 1 - \#E(\mathbb{F}_q)$ die *Spur des Frobenius-Endomorphismus.*

2.17 Bemerkung. Es gilt (wie in der linearen Algebra) eine charakteristische Gleichung für π (siehe z.B. [SZ03], Theorem 3.2):

$$\pi^2 - t\pi + q = 0, \text{also}$$
$$\forall (x,y) \in E\backslash\{O\} : (x^{q^2}, y^{q^2}) - [t](x^q, y^q) + [q](x,y) = O.$$

Das charakteristische Polynom von π bezeichnen wir auch mit f_π.
Weitere wichtige Endomorphismen einer elliptischen Kurve sind die

2.18 Definition. *Multiplikation-mit-m-Abbildungen*:
Sei E/K eine elliptische Kurve, $m \in \mathbb{Z}$. Dann definieren wir die Abbildung $[m] : E \to E$ durch

$$P \mapsto \begin{cases} mP & \text{falls } m \geq 0 \\ (-m)(-P) & \text{sonst.} \end{cases}$$

2.19 Definition. Sei E/K eine elliptische Kurve. Das *m-te Divisionspolynom* von E ist ein Polynom $\psi_m \in K[x,y]$ mit

$$\psi_m(X(P), Y(P)) = 0 \Leftrightarrow mP = O \text{ für alle } P \in E\backslash\{O\}.$$

Die Divisionspolynome sind durch folgende Rekursion gegeben:

$$\psi_0 = 0, \psi_1 = 1$$
$$\psi_2 = 2y + a_1x + a_3$$
$$\psi_3 = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8$$
$$\psi_4 = (2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + b_4b_8 - b_6^2)\psi_2$$
$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, \quad m \geqslant 2$$
$$\psi_{2m} = \frac{(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)\psi_m}{\psi_2}, \ m > 2$$

Die Multiplikation-mit-m-Abbildungen werden auch durch die jeweiligen Divisionspolynome definiert:
Sei

$$\theta_m := x\psi_m^2 - \psi_{m-1}\psi_{m+1},$$
$$\omega_m := \frac{\psi_{2m} - (a_1\theta_m + a_3\psi_m^2)\psi_m^2}{2\psi_m}$$

dann ist (in Charakteristik $\neq 2$)

$$[m] = \left(\frac{\theta_m(x,y)}{\psi_m^2(x,y)} \, , \, \frac{\omega_m(x,y)}{\psi_m^3(x,y)} \right) \tag{2.20}$$

Für Charakteristik 2 siehe [BSS99],III.4.2.

2.21 Bemerkung. (**Genauere Bestimmung der Form von** ψ_m)
Mithilfe von Induktion über m kann man zeigen, dass die Polynome ψ_m Polynome nur in x sind, wenn m ungerade ist, bzw. in x und y und teilbar durch ψ_2, wenn m gerade. Eine wichtige Rolle im Beweis spielt die Tatsache, dass ψ_2^2 immer durch ein Polynom in x ersetzt werden kann wegen

$$\psi_2^2 = a_1x^2 + a_3^2 + 4y^2 + 4a_1xy + 4a_3y + 2a_1xa_3$$

und

$$y^2 = -a_1xy - a_3y + x^3 + a_2x^2 + a_4 + a_6.$$

Der Grad der Polynome in y kann also 1 nie überschreiten. Die Divisionspolynome ψ_m sind also „fast univariat“ im Sinne der folgenden

2.22 Definition. Wir definieren für $m \in \mathbb{N}$ und eine feste elliptische Kurve E die Polynome

$$\overline{f}_m := \begin{cases} \psi_m & \text{für } m \text{ ungerade} \\ \frac{\psi_m}{\psi_2} & \text{für } m \text{ gerade} \end{cases}$$

Es gilt: $\overline{f}_m \in K[x]$. Von nun an sind, wenn wir von *Divisionspolynomen* sprechen, die univariaten Polynome gemeint.

Dann gilt das folgende

2.23 Korollar. *Sei $P \in E\backslash\{O\}$ mit $2P \neq O$, sei $m \geqslant 2$. Dann gilt:*

$$P \in E[m] \Leftrightarrow \overline{f}_m(X(P)) = 0$$

.

Beweis. Siehe [BSS99], Corollary III.7. □

Die Punkte der 2-Torsion werden also aus den Divisionspolynomen „herausdividiert“, allerdings sind sie auch immer sehr einfach zu berechnen:
Es gilt $2P = O \Leftrightarrow P = -P$ für alle $P \in E$ und $-(x,y) = (x, -y - a_1x - a_3)$ nach den Additionsformeln. In Charakteristik > 3 gilt also für eine Kurve E in kurzer Weierstrass-Normalform (also mit $a_1 = a_3 = 0$): $(x,y) \in E[2]\backslash\{O\} \Leftrightarrow y = 0$.

2.24 Satz (und Definition). *Sei $\varphi : E_1 \to E_2$ eine Isogenie vom Grad m. Dann gibt es eine eindeutig bestimmte Isogenie $\widehat{\varphi} : E_2 \to E_1$ mit $\varphi \circ \widehat{\varphi} = [m]$. Wir nennen $\widehat{\varphi}$ die zu φ* duale Isogenie.

Beweis. [Sil86], III.6.1. □

2.25 Satz. ***(Eigenschaften der dualen Isogenie)***
Sei $\varphi : E_1 \to E_2$ eine Isogenie. Es gilt:

(a) Sei $m = deg(\varphi)$. Dann ist

$$\widehat{\varphi} \circ \varphi = [m] \text{ auf } E_1 \text{ und } \varphi \circ \widehat{\varphi} = [m] \text{ auf } E_2$$

(b) Sei $\psi : E_2 \to E_3$ eine weitere Isogenie, dann ist

$$\widehat{\psi \circ \varphi} = \widehat{\varphi} \circ \widehat{\psi}$$

(c)

$$\widehat{[m]} = [m] \text{ und } deg([m]) = m^2, \ m \in \mathbb{Z}.$$

(d)

$$deg(\widehat{\varphi}) = \ deg(\varphi)$$

(e)

$$\widehat{\widehat{\varphi}} = \varphi$$

Beweis. siehe [Sil86], III.6.2. □

Dann folgt als

2.26 Korollar. *Seien $\varphi : E_1 \to E_2, \ \psi : E_2 \to E_3$ Isogenien. Es ist*

$$deg(\psi \circ \varphi) = \ deg(\psi) \cdot deg(\varphi)$$

Beweis. Es gilt $\widehat{(\psi \circ \varphi)} \circ (\psi \circ \varphi) = [\deg(\psi \circ \varphi)]$. Nach 2.25(b) ist

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

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

□

Einen Algorithmus zur Berechnung der dualen Isogenie werden wir in Kapitel 6 vorstellen.
Wir werden grösstenteils mit separablen Isogenien arbeiten. Für diese gilt folgender

2.27 Satz. *Sei $\varphi : E_1 \to E_2$ eine separable Isogenie. Dann gilt:*

$$\#\ker(\varphi) = \deg(\varphi). \tag{2.28}$$

Beweis. Siehe [Sil86], Theorem 4.10.c □

Sehr wichtig für unsere Zwecke ist auch noch folgende Aussage aus [Sil86](II.6.4) über die Struktur der m-Torsionsgruppen:

2.29 Korollar. *Sei E/K eine ordinäre elliptische Kurve, $m \in \mathbb{Z}$ mit $gcd(m, char(K)) = 1$. Dann ist*

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Beweis. [Sil86], Corollary 6.4. □

2.2 j-Invariante, Isomorphismen und Normalformen

Unser Programm zur Isogenieberechnung arbeitet mit Kurven über endlichen Körpern mit grosser Charakteristik oder mit Charakteristik 2. Um die Berechnungen so schnell wie möglich zu machen, wird zu jeder elliptischen Kurve eine isomorphe Kurve in möglichst knapper Form berechnet. Dies ist in Charakteristik > 3 immer $y^2 = x^3 + ax + b$, in Charakteristik 2 die Form $y^2 + xy = x^3 + bx^2 + a$. Es wird auch immer der zugehörige Isomorphismus berechnet. Da das Endergebnis des Programms eine Isogenie ist, kann dieser noch davorgeschaltet werden. Zunächst überlegen wir ganz allgemein, unter welchen Voraussetzungen Isomorphismen zwischen elliptischen Kurven existieren. Die Formeln hierfür sind aus [Sil86], III.1 bzw. Appendix A übernommen. Vorher benötigen wir allerdings noch eine

2.30 Definition. Sei $\widetilde{K} = K(\alpha), [\widetilde{K} : K] = n$. Für $\beta \in \widetilde{K}$ gibt es eine Matrix $M_\beta \in K^{n\times n}$, so dass die folgende Gleichung gilt:

$$\beta(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) = (1, \alpha, \alpha^2, \ldots, \alpha^{n-1})M_\beta$$

M_β ist also die Darstellungsmatrix der Multiplikation-mit-β-Abbildung zur Basis $(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$. Dann ist die *Spur* von β definiert als $\mathrm{Tr}_{\widetilde{K}/K}(\beta) := \mathrm{Tr}(M_\beta)$, also die Summe der Diagonalelemente von M_β. Wenn klar ist, welche Körpererweiterung wir betrachten, dann schreiben wir auch oft $\mathrm{Tr}(\beta)$ anstelle von $\mathrm{Tr}_{\widetilde{K}/K}(\beta)$.

Wir werden auch noch ein kleines Lemma benötigen:

2.31 Lemma. *Sei $\widetilde{K}/K$ eine endliche Körpererweiterung und K' ein Zwischenkörper von $\widetilde{K}/K$. Dann gilt*

$$Tr_{\widetilde{K}/K}(\beta) = [\widetilde{K} : K']\, Tr_{K'/K}(\beta) \text{ für alle } \beta \in K'.$$

Beweis. Siehe [Hes04], Satz 2.87(ii). □

Seien nun $E_i : Y^2 + a_{i1}XY + a_{i3}Y = X^3 + a_{i2}X^2 + a_{i4}X + a_{i6}, i \in \{1, 2\}$ zwei elliptische Kurven über K. Dann gibt es genau dann einen K-Isomorphismus $\varphi : E_1 \to E_2$, wenn es $r, s, t, \in K$ und $u \in K^*$ gibt, so dass die Gleichung für E_1 mittels $X \mapsto u^2X + r, Y \mapsto u^3Y + su^2X + t$ in die Gleichung für E_2 überführt wird, wenn es also solche r, s, t, u gibt, dass $\varphi = [u^2x + r, u^3y + su^2x + t]$ eine Isogenie (dann vom Grad eins, also ein Isomorphismus) zwischen E_1 und E_2 ist. Die Umkehrabbildung ist dann $\varphi^{-1} = [\frac{x-r}{u^2}, \frac{y-s(x-r)-t}{u^3}]$.
Sei also $E/K : y^2 + a_1xy + a_3x = x^3 + a_2x^2 + a_4x + a_6$ eine beliebige elliptische Kurve in Weierstrass-Form. Die kurze Normalform beruht auf folgenden Variablentransformationen
(Charakteristik >3)

$$x = \frac{x' - 3b_2}{36} \Rightarrow x' = 36x + 3b_2$$

$$y = \frac{1}{2}(y' - a_1x - a_3) \text{ und } y' = \frac{y''}{108} \Rightarrow y'' = 108y' = 108(2y + a_1x + a_3),$$

Hierbei ist b_2 die in Abschnitt 1.4 definierte Grösse. Die resultierende isomorphe Kurve in kurzer Weierstrass-Normal-Form ist dann

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

Der zugehörige Isomorphismus ist gegeben durch

$$\varphi : E \to E',\ \varphi = [36x + 3b_2, 108(2y + a_1x + a_3)]$$

(Charakteristik 2)
In Charakteristik 2 wird die Formel für die j-Invariante einer Kurve
$E : y^2 + a_1xy + a_3x = x^3 + a_2x^2 + a_4x + a_6$ zu $j(E) = \frac{a_1^{12}}{\Delta}$. Ausserdem gilt hier: $j(E) = 0 \Leftrightarrow E$ supersingulär (siehe [BSS99], III.3.2). Da wir aber in unserem Algorithmus nur ordinäre Kurven betrachten, ist immer $a_1 \neq 0$ gegeben. Somit sind die folgenden Variablentransformationen definiert:

$$x = a_1^2x' + \frac{a_3}{a_1} \Rightarrow x' = \frac{1}{a_1^2}\left(x + \frac{a_3}{a_1}\right),$$

$$y = a_1^3 y' + \frac{(a_1^2 a_4 + a_3^2)}{a_1^3} \Rightarrow y' = \frac{1}{a_1^3}\left(y + \frac{(a_1^2 a_4 + a_3^2)}{a_1^3}\right)$$

Die resultierende isomorphe Kurve ist hier

$$E' : y'^2 + x'y' = x'^3 + bx'^2 + a$$

mit

$$a = \frac{a_1^4 a_4^2 + a_3^4 + a_1^3 a_3^3 + a_1^4 a_2 a_3^2 + a_1^5 a_3 a_4 + a_1^6 a_6}{a_1^{12}},\ b = \frac{a_1^3 a_3 + a_1^4 a_2}{a_1^6}$$

Ist ausserdem $\mathrm{Tr}_{K/\mathbb{F}_2}(b) = 0$, dann können wir zur weiteren Vereinfachung der Kurvengleichung $b = 0$ setzen:
Zwischen zwei Kurven $E_i/\mathbb{F}_{2^n} : y^2 + xy = x^3 + b_i x^2 + a$, welche nach den Formeln in Abschnitt 1.4 dieselbe j-Invariante $\frac{1}{a}$ haben, gibt es genau dann einen $\mathbb{F}_{2^n}$-Isomorphismus, wenn $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(b_1) = \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(b_2)$, denn: Ein Isomomorphismus zwischen E_1 und E_2 ist unter diesen Voraussetzungen gegeben durch

$$x \mapsto x',\ y \mapsto y' + sx', \tag{2.32}$$

wobei s eine Lösung der Gleichung $x^2 + x + (b_1 + b_2)$ ist. Eine Gleichung der Form $y^2 + y + \beta = 0$ hat aber genau dann Lösungen in $\mathbb{F}_{2^n}$, wenn $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\beta) = 0$ (siehe [BSS99],II.2.4). Die Isomorphieeigenschaft der Abbildung 2.32 kann man durch Einsetzen in die Kurvengleichungen nachprüfen.
Falls $\mathrm{Tr}(b) = 0$, setzen wir $s :=$ Nullstelle von x^2+x+b und $E' : y'^2+x'y' = x'^3+a$, sonst defininieren wir $s := 0$.
Ein Isomorphismus von E nach E' ist dann gegeben durch

$$\varphi = \left[\frac{1}{a_1^2}\left(x + \frac{a_3}{a_1}\right),\ \frac{1}{a_1^3}\left(y + \frac{a_1^2 a_4 + a_3^2}{a_1^3} + s\frac{(x + \frac{a_3}{a_1})}{a_1^2}\right)\right]$$

Es gilt hier, dass $j(E) = j(E')$.

Man kann weiterhin folgende bedeutende Aussage über den Zusammenhang zwischen j-Invarianten elliptischer Kurven und Isomorphismen machen:

2.33 Satz. *Zwei elliptische Kurven sind genau dann $\overline{K}$-isomorph, wenn sie dieselbe j-Invariante haben.*

Beweis. Siehe [Sil86], III. 1.4. □

Für Kurven $E_1/K, E_2/K$ in kurzer Weierstrass-Form mit $\mathrm{char}(K) > 3$ ist ein solcher Isomorphismus folgendermassen zu finden: Ist $j(E_1) = j(E_2)$, dann existiert ein $u \in \overline{K}^*$, so dass $\varphi : E_1 \to E_2, (x, y) \mapsto (u^2 x, u^3 y)$ ein Isomorphismus ist. (siehe [Sil86], Beweis zu III. 1.4.)
Daraus lässt sich folgender Algorithmus ableiten:

2.34 Algorithmus. ***Berechnung eines Isomorphismus zwischen Kurven in kurzer Weierstrass-Normal-Form (char(K) >3)***
Input: $E_1/K : y^2 = x^3 + ax + b,\ E_2/K : y^2 = x^3 + Ax + B$,
$\widetilde{K}$ *algebraischer Erweiterungskörper von* K
Output: $\widetilde{K}$*-Isomorphismus* $\varphi : E_1 \to E_2$ *oder ERROR, falls* E_1 *und* E_2 *nicht* $\widetilde{K}$*-isomorph*

- *IF* $j(E_1) \neq j(E_2)$ *THEN RETURN ERROR*
- *IF* $E_1 = E_2$ *THEN RETURN* Id_{E_1}
- *Finde* $u \in \overline{K}$ *mit* $u = \sqrt[4]{\frac{A}{a}} = \sqrt[6]{\frac{B}{b}}$
- *IF* $u \notin \widetilde{K}$ *THEN RETURN ERROR*
- *RETURN* $\varphi := [\frac{x}{u^2}, \frac{y}{u^3}]$

Nun geben wir noch den Algorithmus für Charakteristik 2 an, dessen Korrektheit sich aus den Ausführungen auf Seite 19 ergibt:

2.35 Algorithmus. ***Berechnung eines Isomorphismus zwischen ordinären Kurven in Charakteristik-2-Normalform***
Input: $E_1/\mathbb{F}_{2^n} : y^2 + xy = x^3 + b_1x^2 + a_1, E_2/\mathbb{F}_{2^n} : y^2 + xy = x^3 + b_2x^2 + a_2$,
$\widetilde{K}$ *algebraischer Erweiterungskörper von* $\mathbb{F}_{2^n}$
Output: $\widetilde{K}$*-Isomorphismus* $\psi : E_1 \to E_2$ *oder ERROR, falls* E_1 *und* E_2 *nicht* $\widetilde{K}$*-isomorph*

- *IF* $a_1 \neq a_2$ *THEN RETURN ERROR*
- s*:= Nullstelle von* $x^2 + x + b_1 + b_2$
- *IF* $s \notin \widetilde{K}$ *THEN RETURN ERROR*
- *RETURN* $\psi := [x, y + sx]$

Wann ist ein solcher Isomorphismus schon über K definiert? Eine Aussage dazu finden wir in folgendem

2.36 Lemma. $E_1/K \cong_K E_2/K \Leftrightarrow j(E_1) = j(E_2)$ *und* $\#E_1(K) = \#E_2(K)$

Beweis. [Hen02], Lemma 5.1.4. □

Nun definieren wir den quadratischen Twist einer elliptischen Kurve E/K, welcher eine spezielle, zu E isomorphe Kurve darstellt.

2.37 Definition. Sei E/K eine elliptische Kurve. Ein *quadratischer Twist* von E ist eine Kurve E^t/K, so dass es keinen K-Isomorphismus zwischen E und E^t gibt, aber einen $\widetilde{K}$-Isomorphismus zwischen E und E^t für einen quadratischen Erweiterungskörper $\widetilde{K}$ von K.

Eine elliptische Kurve und ihr quadratischer Twist müssen also dieselbe j-Invariante haben.

Nun geben wir zwei Algorithmen zum Finden eines quadratischen Twists einer elliptischen Kurve an, zunächst für Charakteristik > 3, danach für Charakteristik 2.

2.38 Algorithmus. ***Finden eines quadratischen Twists zu einer Kurve*** E/K ***in Charakteristik*** > 3
Input: *$E/K : y^2 = x^3 + ax + b$ elliptische Kurve in kurzer Weierstrass-Form*
Output: *Ein quadratischer Twist E^t/K von E*

- *Suche $v \in K$ mit $\nexists\, q \in K : q^2 = v$*
- *RETURN $E^t : y^2 = x^3 + v^2ax + v^3b$*

Man sieht ganz einfach, dass es keinen K-Isomorphismus zwischen E und E^t gibt, denn dann müsste es ein $u = \sqrt[4]{\frac{v^2a}{a}} = \sqrt{v}(= \sqrt[6]{\frac{v^3b}{b}}) \in K$ geben, was ja gerade bei der Suche nach v ausgeschlossen wurde. Allerdings gilt $u = \sqrt{v} \in \widetilde{K}$, wobei $\widetilde{K}$ eine quadratische Erweiterung von K ist, somit gibt es einen $\widetilde{K}$-Isomorphismus zwischen E und E^t.

2.39 Algorithmus. ***Finden eines quadratischen Twists zu einer ordinären Kurve*** $E/\mathbb{F}_{2^n}$
Input: *$E/\mathbb{F}_{2^n} : y^2 + xy = x^3 + bx^2 + a$ elliptische Kurve in Normalform*
Output: *quadratischer Twist $E^t/\mathbb{F}_{2^n}$ von E*

- *$\omega :=$ Erzeuger von $\mathbb{F}_{2^n}^*, i := 1$*
- *WHILE $Tr(\omega^i) = Tr(b)$ DO*
  - *$i := i + 1$*
- *END WHILE*
- *$b_2 := \omega^i$*
- *RETURN $E^t : y^2 + xy = x^3 + b_2x^2 + a$*

Auch hier gibt es (vgl. Seite 19) wegen $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(b_2) \neq \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(b)$ keinen $\mathbb{F}_{2^n}$-Isomorphismus zwischen E und E^t, aber einen $\mathbb{F}_{2^{2n}}$-Isomorphismus, da $\mathrm{Tr}_{\mathbb{F}_{2^{2n}}/\mathbb{F}_2}(b_2) = \mathrm{Tr}_{\mathbb{F}_{2^{2n}}/\mathbb{F}_2}(b) = 0$ wegen Lemma 2.31.
Über die Grösse der Punktgruppen einer elliptischen Kurve und ihres quadratischen Twists kann man folgende Aussage machen:

2.40 Lemma. *Sei $E/\mathbb{F}_q$ eine elliptische Kurve und $E^t/\mathbb{F}_q$ ihr quadratischer Twist. Dann gilt:*

$$\#E(\mathbb{F}_q) + \#E^t(\mathbb{F}_q) = 2q + 2$$

Beweis. Wir beschränken uns im Beweis auf Körper der Charakteristik > 2. Die Argumente für den Beweis in Charakteristik 2 sind dieselben. Wir können E also schreiben als $E : y^2 = g(x)$, wobei $g(x) \in \mathbb{F}_q[x]$ ein kubisches Polynom ist. Dann ist die Gleichung für E^t gegeben durch $E^t : y^2 = v^3 g(\frac{x}{v}) =: g_v(x)$, wobei $v \in \mathbb{F}_q$ kein quadratischer Rest ist. Falls für $\alpha \in \mathbb{F}_q$ $g_v(\alpha) = 0$, dann gilt auch $g(\frac{\alpha}{v}) = 0$. Es gilt also $(\alpha, 0) \in E^t$ bzw. $(\frac{\alpha}{v}, 0) \in E$. Solche Körperelemente sind also die x-Koordinaten je eines Punktes auf jeder Kurve. Ist $g_v(\alpha)$ ein quadratischer Rest $\neq 0$, dann ist $g(\frac{\alpha}{v}) = \frac{g_v(\alpha)}{v^3}$ kein quadratischer Rest. Solche Körperelemente sind daher die x-Koordinaten von zwei Punkten auf E^t, aber keines Punktes auf E. Ist andererseits $g_v(\alpha)$ kein quadratischer Rest, dann ist $g(\frac{\alpha}{v})$ ein quadratischer Rest wegen der Multiplikativität des Legendre-Symbols. Also geben solche Körperelemente als x-Koordinaten zwei Punkte auf E, aber keinen auf E^t. Es folgt, dass jedes Element $\alpha \in \mathbb{F}_q$ bzw. $\frac{\alpha}{v}$ insgesamt die x-Koordinate zweier Punkte ist. Hinzu kommen noch die beiden „Punkte im Unendlichen“. □

2.3 Modulpolynome und Isogenieklassen

Seien $E_1/K, E_2/K$ elliptische Kurven über dem endlichen Körper K. In diesem Abschnitt untersuchen wir die Frage, wann eine K-Isogenie zwischen E_1 und E_2 existiert. Eine Auskunft darüber gibt uns folgender

2.41 Satz. *Es gilt:*
E_1 und E_2 sind K-isogen $\Leftrightarrow \#E_1(K) = \#E_2(K)$.

Beweis. Siehe [Tat66],§ 3,Theorem 1 (für allgemeine abelsche Varietäten), [Cha04] für elliptische Kurven. Wir präsentieren hier die (einfachere) Richtung ($\Rightarrow$) aus [Cha04]. (Die andere Richtung erfordert viele zusätzliche Definitionen, die wir in dieser Arbeit nicht weiter benötigen werden).
Sei $\varphi : E_1 \to E_2$ eine über $K := \mathbb{F}_q$ definierte Isogenie. Seien π_1 der Frobenius-Endomorphismus von E_1 und π_2 der von E_2. Wir zeigen nun, dass die charakteristische Gleichung von π_{E_1} gleich der von π_{E_2} ist, denn dann folgt
$\#E_1(K) = \#E_2(K)$. Die Gleichheit der Punktanzahl gilt, wenn wir das gezeigt haben, dann aber auch über allen Erweiterungskörpern von K, denn φ ist als über K definierte Isogenie natürlich auch über allen Erweiterungskörpern definiert. Seien nun $P \in E_1$ beliebig und t die Spur von π_{E_1}. Dann ist

$$\varphi(\pi_1^2(P) - t\pi_1(P) + qP) = \varphi(O_{E_1}) = O_{E_2}.$$

Nun schreiben wir $\varphi = [\varphi_x(x,y), \varphi_y(x,y)]$, dann ist

$$\begin{aligned}\varphi(\pi_1(P)) &= (\varphi_x(X(P)^q, Y(P)^q), \varphi_y(X(P)^q, Y(P)^q)) \\ &= (\varphi_x(X(P), Y(P))^q, \varphi_y(X(P), Y(P))^q) \\ &= \pi_2(\varphi(P))\end{aligned}$$

da für $f \in \mathbb{F}_q(x,y)$ gilt: $f(x^q, y^q) = f(x,y)^q$.
Dann ist also

$$\begin{aligned}\varphi(\pi_1^2(P) - t\pi_1(P) + qP) &= \varphi(\pi_1^2(P)) - t\varphi(\pi_1(P)) + q\varphi(P) \\ &= \pi_2^2(\varphi(P)) - t\pi_2\varphi(P) + q\varphi(P).\end{aligned}$$

Da Isogenien nach Satz 2.12 surjektiv sind, gilt

$$\pi_2^2(Q) - t\pi_2(Q) + qQ = O_{E_2} \text{ für alle } Q \in E_2,$$

somit ist die charakteristische Gleichung für π_2 dieselbe wie für π_1. □

Ein wichtiges Hilfsmittel bei der Bestimmung der zu einer Kurve K-isogenen Kurven sind die sogenannten Modulpolynome:

2.42 Definition. Das *n-te Modulpolynom* ist ein Polynom $\Psi_n \in \mathbb{Z}[x,y]$ mit der Eigenschaft:
Es existiert eine K-Isogenie vom Grad n zwischen E_1 und E_2
$\Leftrightarrow \Psi_n(j(E_1/K), j(E_2/K)) = 0$.

Für eine ausführliche Definition verweisen wir auf [BSS99],III.8, für unsere Zwecke genügt es jedoch, zu wissen, dass die Modulpolynome obige Eigenschaft erfüllen. Wir haben sie aus MAGMA in KASH3 kopiert und erhalten sie dort mithilfe der Funktion ModularPolynomial(n) für primes $n \in \{1 \ldots 59\}$.
Wir können also elliptische Kurven über einem Körper K in *Isogenieklassen* einteilen:
$E \sim E' \Leftrightarrow$ Es existiert eine K-Isogenie $\varphi : E \to E'$.
Alle Elemente in einer Isogenieklasse haben dieselbe Anzahl von Punkten über K.

Kapitel 3

Zahlentheoretische Grundlagen

In diesem Kapitel fassen wir die grundlegenden Definitionen und Sätze aus der Zahlentheorie zusammen, welche wir später für unseren Algorithmus benötigen werden.
Unter einem Ring verstehen wir immer einen kommutativen Integritätsring mit Eins.

3.1 Definition. Ein *Zahlkörper* F ist eine endliche algebraische Erweiterung von $\mathbb{Q}$.

Nach dem Satz vom primitiven Element ist ein Zahlkörper F immer darstellbar als $F = \mathbb{Q}(\alpha), \alpha \in F$.

3.2 Definition. Sei R ein Ring, $(M, +)$ eine abelsche Gruppe. M heisst *R-Modul*, wenn es eine Verknüpfung $\cdot : R \times M \to M$ gibt mit

(i) $\forall\ r_1, r_2 \in R, m \in M :\ (r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$

(ii) $\forall\ r \in R, m_1, m_2 \in M :\ r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$

(iii) $\forall\ r_1, r_2 \in R, m \in M :\ (r_1 r_2) \cdot m = r_1(r_2 \cdot m)$

(iv) $\forall m \in M :\ 1 \cdot m = m.$

3.3 Definition. Ein R-Modul M heisst *frei*, wenn es Elemente
$B = \{m_1, \ldots, m_n\} \subseteq M$ gibt mit $M = \langle B \rangle$ und B linear unabhängig über R ist (wenn also für alle $r_i \in R$ aus $r_1 m_1 + \cdots + r_n m_n = 0$ folgt, dass $r_i = 0\ \forall i$).
B heisst dann *R-Basis* von M.

3.4 Satz. *Seien R ein kommutativer Ring und M ein freier R-Modul. Dann besitzen je zwei R-Basen von M dieselbe Mächtigkeit.*

Beweis. Siehe [Wil93], Satz 1.14. □

Daher ist die folgende Definition sinnvoll:

3.5 Definition. Sei M ein freier R-Modul und B eine R-Basis von M. Der *Rang* von M ist dann definiert als $\#B$.

3.6 Definition. Sei F ein Zahlkörper. Ein Element $\beta \in F$ heisst *ganz* (über $\mathbb{Z}$), wenn es Nullstelle eines normierten Polynoms $f \in \mathbb{Z}[x]$ ist. Die Menge der über $\mathbb{Z}$ ganzen Elemente von F bezeichnen wir mit $Cl(\mathbb{Z}, F)$. Wir nennen $Cl(\mathbb{Z}, F)$ auch oft *Maximalordnung* von F, Notation: $\mathcal{O}_F$.

In dieser Situation gelten folgende Sätze:

3.7 Satz. *Die über $\mathbb{Z}$ ganzen Elemente eines Zahlkörpers F bilden einen Ring.*

Beweis. Siehe [Poh93], IV.1. □

3.8 Satz. *Die Maximalordnung $\mathcal{O}_F$ eines Zahlkörpers F der Ordnung n über $\mathbb{Q}$ ist ein freier $\mathbb{Z}$-Modul vom Rang n.*

Beweis. Siehe [Wil93], Satz 4.30. □

3.9 Definition. Ein Teilring $\mathcal{O}$ von $\mathcal{O}_F$ heisst *Ordnung* von F, falls $\mathcal{O}$ ein freier $\mathbb{Z}$-Modul vom Rang n mit $1 \in \mathcal{O}$ ist. Wir nennen $\mathcal{O}_F$ in diesem Fall auch Maximalordnung von $\mathcal{O}$.
Sei $f \in \mathbb{Z}[x]$ normiert und irreduzibel, α eine Nullstelle von f. Dann heisst $\mathbb{Z}[\alpha]$ die *Gleichungsordnung* von f.

3.10 Beispiel. Sei $F = \mathbb{Q}(\alpha)$ mit $[F : \mathbb{Q}] = n$, so dass das Minimalpolynom f_α von α, welches per Definition normiert ist, ganze Koeffizienten hat. Dann ist $\mathcal{O} = \mathbb{Z}[\alpha]$ eine Ordnung von F mit Basis $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$, nämlich die Gleichungsordnung von f_α.

Die Spur eines Körperelements haben wir schon in Kapitel 2 definiert. Wir geben die Definition hier noch einmal an, da wir auch die Multiplikationsmatrix für weitere Definitionen benötigen.

3.11 Definition. Sei $K = \mathbb{Q}(\alpha), [K : \mathbb{Q}] = n$. Für $\beta \in K$ gibt es eine Matrix $M_\beta \in \mathbb{Q}^{n \times n}$, so dass die folgende Gleichung gilt:

$$\beta(1, \alpha, \alpha^2, ..., \alpha^{n-1}) = (1, \alpha, \alpha^2, ..., \alpha^{n-1}) M_\beta$$

Die *Spur* von β ist definiert als $\mathrm{Tr}(\beta) := \mathrm{Tr}(M_\beta)$.
Die *Norm* von β ist definiert als $\mathcal{N}(\beta) := det(M_\beta)$.
Die *Diskriminante* von $\{\omega_1, ..., \omega_m\} \subseteq F$ wird definiert als

$$\mathrm{disc}(\omega_1, ..., \omega_m) := \det(\mathrm{Tr}(\omega_i\omega_j)_{1 \leqslant i,j \leqslant m}).$$

Ist $\{\omega_1, ..., \omega_n\}$ eine Basis von F bzw. eine Basis einer Ordung $\mathcal{O}$ von F, dann nennen wir $\mathrm{disc}(\omega_1, ..., \omega_n)$ auch Diskriminante von F bzw. $\mathcal{O}$. Diese Invariante ist unabhängig von der Wahl der Basis.

Wir betrachten ab jetzt nur noch *imaginärquadratische* Zahlkörper, d.h. Zahlkörper F mit $[F : \mathbb{Q}] = 2$ und $F \nsubseteq \mathbb{R}$.
Das folgende Lemma trägt einige wichtige Eigenschaften von Norm und Spur in imaginärquadratischen Zahlkörpern zusammen, die wir später noch benötigen werden.

3.12 Lemma. *Seien $F = \mathbb{Q}(\omega)$ ein imaginärquadratischer Zahlkörper und $f_\omega(x) = x^2 + ax + b \in \mathbb{Q}[x]$ das Minimalpolynom von ω. Sei $\sigma \in \mathrm{Gal}_\mathbb{Q}(F)$ die Abbildung, welche ω auf die andere Nullstelle von f_ω abbildet. Dann gilt:*

(i) $\mathcal{N}(\omega) = b,\ Tr(\omega) = -a.$

(ii) $\forall \beta \in F : \mathcal{N}(\beta) \in \mathbb{Q}, Tr(\beta) \in \mathbb{Q}$

(iii) $\forall \beta \in F : \mathcal{N}(\beta) = \beta\sigma(\beta),\ Tr(\beta) = \beta + \sigma(\beta)$

(iv) $\forall a \in \mathbb{Q} : \mathcal{N}(a) = a^2,\ Tr(a) = 2a$

Beweis.

(*i*) Die Multiplikation-mit-ω-Matrix ist

$$M_\omega = \begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix} \Rightarrow \text{ Behauptung}$$

(*ii*) Dies folgt aus der Definition der Norm als Determinante und der Spur als Spur einer Matrix über $\mathbb{Q}$.

(*iii*) Sei $\beta = r_1 + r_2\omega \in F$, sei $\omega_2 = \sigma(\omega)$. Es gilt

$$f_\omega(x) = (x - \omega)(x - \omega_2) = x^2 - (\omega + \omega_2)x + \omega\omega_2,$$

also $(\omega + \omega_2) = -a,\ \omega\omega_2 = b$. Die Multiplikation-mit-β-Matrix ist dann

$$M_\beta = \begin{pmatrix} r_1 & -r_2 b \\ r_2 & r_1 - r_2 a \end{pmatrix} \Rightarrow Tr(\beta) = 2r_1 - r_2 a,\ N(\beta) = r_1^2 - r_1 r_2 a + r_2^2 b.$$

Aber

$$\begin{aligned}
\beta + \sigma(\beta) &= r_1 + r_2\omega + \sigma(r_1 + r_2\omega) \\
&= 2r_1 + r_2(\omega + \sigma(\omega)) \\
&= 2r_1 + r_2(\omega + \omega_2) \\
&= 2r_1 - r_2 a, \\
\beta\sigma(\beta) &= (r_1 + r_2\omega)\sigma(r_1 + r_2\omega) \\
&= r_1^2 + r_1 r_2(\omega + \omega_2) + r_2^2\omega\omega_2 \\
&= r_1^2 - r_1 r_2 a + r_2^2 b
\end{aligned}$$

Damit folgt die Behauptung.

(*iv*) Dies folgt aus (*iii*), da $\sigma(a) = a \ \forall a \in \mathbb{Q}$

□

3.13 Satz (und Definition). *Sei F ein imaginärquadratischer Zahlkörper, $\mathcal{O}_F$ die Maximalordnung mit Basis $\{1, \omega\}$, $\mathcal{O}$ eine andere Ordnung von F.*
(i) Dann existiert $c \in \mathbb{Z}$ mit $\mathcal{O} = \mathbb{Z} + c\mathcal{O}_F$. c heisst auch Führer *von $\mathcal{O}$.*
(ii) $disc(\mathcal{O}) = c^2 disc(\mathcal{O}_F)$.

Beweis. Seien F und $\mathcal{O}_F$ wie oben . Sei $\mathcal{O}$ eine andere Ordnung von F mit Basis $(1, \omega')$. Dann ist $\omega' = r + c\omega,\ r, c \in \mathbb{Z}$. Für jedes $a \in \mathcal{O}$ existiert eine Darstellung mit $z_1, z_2 \in \mathbb{Z} : a = z_1 + z_2\omega' = z_1 + z_2(r + c\omega) = z_1 + z_2 r + c\omega \in \mathbb{Z} + c\mathcal{O}_F$. Andersherum gilt für $\alpha \in \mathbb{Z} + c\mathcal{O}_F$

$$\begin{aligned}
\alpha &= z_1 + c(a + b\omega) \\
&= z_1 + ca + cb\omega \\
&= z_1 + ca + cb\left(\frac{\omega' - r}{c}\right) \\
&= z_1 + ca - br + bc\omega' \in \mathcal{O}
\end{aligned}$$

Daraus folgt (i).
Es ist also auch $(1, c\omega)$ eine Basis von $\mathcal{O}$. Sei $f = x^2 + ax + b \in \mathbb{Z}[x]$ das Minimalpolynom von ω. Dann ist (siehe unten) $\mathrm{disc}(\mathcal{O}_F) = a^2 - 4b$ und
$\mathrm{disc}(\mathcal{O}) = c^2(a^2 - 4b) = c^2\mathrm{disc}(\mathcal{O}_F)$.

Zur Berechnung der Diskriminanten von $\mathcal{O}$ bzw. $\mathcal{O}_F$:

$$\omega^2 = -b - a\omega,\ \omega^3 = ab + a^2\omega - b\omega \text{ (siehe Minimalpolynom)}$$

$$\operatorname{disc}(\mathcal{O}_F) = \det \begin{pmatrix} \operatorname{Tr}(1) & Tr(\omega) \\ \operatorname{Tr}(\omega) & \operatorname{Tr}(\omega^2) \end{pmatrix}$$

$$\operatorname{Tr}(1) : (1, \omega) = (1, \omega) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow \operatorname{Tr}(1) = 2$$

$$\operatorname{Tr}(\omega) : (\omega, \omega^2) = (1, \omega) \begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix} \Rightarrow \operatorname{Tr}(\omega) = -a$$

$$\operatorname{Tr}(\omega^2) : (\omega^2, \omega^3) = (1, \omega) \begin{pmatrix} -b & ab \\ -a & a^2 - b \end{pmatrix} \Rightarrow \operatorname{Tr}(\omega^2) = a^2 - 2b$$

$$\Rightarrow \operatorname{disc}(\mathcal{O}_F) = \det \begin{pmatrix} 2 & -a \\ -a & a^2 - 2b \end{pmatrix} = a^2 - 4b$$

$$\operatorname{disc}(1, c\omega) = \det \begin{pmatrix} 2 & -ca \\ -ca & c^2(a^2 - 2b) \end{pmatrix} = c^2(a^2 - 4b)$$

□

3.14 Definition. Sei F ein Zahlkörper mit Maximalordnung $\mathcal{O}_F$, sei $\mathcal{O}$ eine Ordnung von F. Dann ist das *Führerideal* von $\mathcal{O}$ definiert als

$$\mathfrak{F} := \{x \in \mathcal{O} \mid x\mathcal{O}_F \subset \mathcal{O}\}.$$

Es gilt: Das Führerideal $\mathfrak{F}$ von $\mathcal{O}$ ist ein Ideal in $\mathcal{O}$ und in $\mathcal{O}_F$. Ausserdem ist $c\mathcal{O} \subset \mathfrak{F}$ für den Führer c von $\mathcal{O}$, es ist also $\mathfrak{F} \neq \emptyset$ (und $\mathfrak{F} \neq \mathcal{O} \Leftrightarrow \mathcal{O} \neq \mathcal{O}_F$).

3.15 Definition. Sei F ein Zahlkörper, $\mathcal{O}$ eine Ordnung von F.
Eine Teilmenge $\mathfrak{a} \subset F$ heisst *gebrochenes Ideal* von $\mathcal{O}$, falls es ein $\xi \in F$ und ein Ideal $\mathfrak{b} \subset \mathcal{O}$ gibt, so dass $\xi\mathfrak{b} = \mathfrak{a}$.

3.16 Definition. Sei F ein Zahlkörper, $\mathcal{O}$ eine Ordnung von F, seien $\mathfrak{a}$ und $\mathfrak{b}$ gebrochene Ideale von $\mathcal{O}$. Dann heisst $\mathfrak{a}$

- *ganz*, wenn $\mathfrak{a} \subset \mathcal{O}$
- *Hauptideal*, wenn es ein $a \in F$ gibt, so dass $\mathfrak{a} = a\mathcal{O}$.
- *invertierbar*, wenn es ein gebrochenes Ideal $\mathfrak{b}$ von $\mathcal{O}$ gibt, so dass $\mathfrak{b}\mathfrak{a} = \mathcal{O}$.
- *Primideal*, wenn $\forall a, b \in \mathcal{O} : ab \in \mathfrak{a} \Rightarrow a \in \mathfrak{a}$ oder $b \in \mathfrak{a}$.
- *maximales Ideal*, wenn es kein nichttriviales Ideal von $\mathcal{O}$ gibt, welches $\mathfrak{a}$ enthält.
- ein *Teiler* von $\mathfrak{b}$, Notation $\mathfrak{a} \mid \mathfrak{b}$, wenn $\mathfrak{b} \subset \mathfrak{a}$.

- *prim* zu $c \in \mathbb{Z}$, wenn $\mathfrak{a} + c\mathcal{O} = \mathcal{O}$.
- *eigentliches Ideal* von $\mathcal{O}$, wenn $\mathfrak{a} \subset \mathcal{O}$ und $[\mathfrak{a}/\mathfrak{a}] := \{\alpha \in F \mid \alpha\mathfrak{a} \subset \mathfrak{a}\} = \mathcal{O}$. Man nennt $[\mathfrak{a}/\mathfrak{a}]$ auch den *Multiplikatorring* von $\mathfrak{a}$.

Die folgenden Lemmata geben Auskunft darüber, wie man Ideale imaginärquadratischer Zahlkörper darstellen kann.

3.17 Lemma. *Ein gebrochenes Ideal $\mathfrak{a}$ einer Ordnung $\mathcal{O}$ ist ein freier $\mathbb{Z}$-Modul vom Rang 2, hat also eine Darstellung $\mathfrak{a} = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ mit $\omega_1, \omega_2 \in F$.*

Beweis. $\mathcal{O}$ ist als Ordnung in einem imaginärquadratischen Zahlkörper ein freier $\mathbb{Z}$-Modul vom Rang 2. Ist $\mathfrak{a}$ ein ganzes Ideal von $\mathcal{O}$, dann ist $\mathfrak{a}$ ein Untermodul von $\mathcal{O}$ (siehe Definition 1.2 in [Wil93]). Dann ist $\mathfrak{a}$ nach Satz 1.15 in [Wil93] ein freier Modul vom Rang 1 oder 2. Falls $\mathfrak{a}$ Rang 1 hätte, dann könnte man $\mathfrak{a}$ darstellen als $\mathfrak{a} = \alpha\mathbb{Z}, \alpha \in \mathcal{O}$. Sei $(1, \omega)$ eine Basis von $\mathcal{O}$. Dann können wir immer ein $\beta \in \mathcal{O}$ so wählen, dass $\alpha\beta \notin \alpha\mathbb{Z}$ ist wegen

$$\alpha\beta = (a_1 + a_2\omega)(b_1 + b_2\omega) = a_1b_1 + a_1b_2\omega + a_2b_1\omega + a_2b_2\omega^2.$$

Also muss der Rang von $\mathfrak{a}$ als $\mathbb{Z}$-Modul 2 sein.
Falls $\mathfrak{a} \neq \{0\}$ ein gebrochenes Ideal von $\mathcal{O}$ ist, dann gibt es ein ganzes Ideal $\mathfrak{b}$ von $\mathcal{O}$ mit $\mathfrak{a} = \xi\mathfrak{b}, \xi \in F^*$. Sei $\mathfrak{b} = \omega_1\mathbb{Z} + \omega_2\mathbb{Z} \Rightarrow \mathfrak{a} = \xi\omega_1\mathbb{Z} + \xi\omega_2\mathbb{Z}$ und $(\xi\omega_1, \xi\omega_2)$ linear unabhängig wegen (ω_1, w_2) linear unabhängig. □

3.18 Definition. Die *Norm* eines ganzen Ideals $\mathfrak{a}$ von $\mathcal{O}$ ist definiert als

$$\mathcal{N}(\mathfrak{a}) := \#\mathcal{O}/\mathfrak{a}.$$

Alternativ kann man, da $\mathfrak{a} = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ ein Untermodul von $\mathcal{O} = \mathbb{Z} + \omega\mathbb{Z}$ vom Rang 2 ist, die Norm von $\mathfrak{a}$ auch als

$$\mathcal{N}(\mathfrak{a}) := |\det M_\mathfrak{a}| \text{ mit } (1, \omega)M_\mathfrak{a} = (\omega_1, \omega_2), M_\mathfrak{a} \in \mathbb{Z}^{2\times 2}$$

definieren (siehe [Coh96], Proposition 4.7.4). $M_\mathfrak{a}$ ist also die Transformationsmatrix einer $\mathbb{Z}$-Basis von $\mathcal{O}$ in eine $\mathbb{Z}$-Basis von $\mathfrak{a}$. Für eine solche Matrix $M_\mathfrak{a}$ gibt es immer eine invertierbare Matrix $U \in \mathbb{Z}^{2\times 2}$, so dass $M_\mathfrak{a}U$ eine obere Dreiecksmatrix, die sogenannte *Hermite-Normalform* von $M_\mathfrak{a}$, ist. Da U invertierbar ist, definieren dann (ω_1, ω_2) und $(\omega_1, \omega_2)U = (1, \omega)M_\mathfrak{a}U$ denselben $\mathbb{Z}$-Modul. Daher können wir jedes ganze Ideal $\mathfrak{a}$ von $\mathcal{O}$ schreiben als $\mathfrak{a} = a\mathbb{Z} + (b + c\omega)\mathbb{Z}, a, b, c \in \mathbb{Z}$. Genauer gilt:

3.19 Proposition. *([Coh96], Proposition 5.2.1)*
Jedes ganze Ideal $\mathfrak{a}$ von $\mathcal{O}$ lässt sich darstellen als $\mathfrak{a} = a\mathbb{Z} + (b + c\omega)\mathbb{Z}$ mit $c|a$ und $c|b$ und $0 \leq b < a$. Weiter gilt $\mathcal{N}(\mathfrak{a}) = ac$.

Zwei wichtige Eigenschaften der Norm sind:

3.20 Lemma. *Für eine Ordnung $\mathcal{O}$ gilt:*
(i) $\forall \alpha \in \mathcal{O} : \mathcal{N}(\alpha\mathcal{O}) = |\mathcal{N}(\alpha)|$
(ii) Seien $\mathfrak{a}, \mathfrak{b}$ ganze Ideale von $\mathcal{O}$. Falls $\mathfrak{a}$ oder $\mathfrak{b}$ invertierbar sind, dann ist $\mathcal{N}(\mathfrak{ab}) = \mathcal{N}(\mathfrak{a})\mathcal{N}(\mathfrak{b})$.

Beweis. (i) folgt aus $\alpha(\mathbb{Z} + \omega\mathbb{Z}) = \alpha\mathbb{Z} + \alpha\omega\mathbb{Z}$ und

$$(1, \omega)\begin{pmatrix}\alpha & 0\\ 0 & \alpha\end{pmatrix} = (\alpha, \alpha\omega)$$

(ii) Siehe [Coh96], Proposition 4.6.8

□

Für gebrochene Ideale gilt folgendes Lemma:

3.21 Lemma. *Sei $\{0\} \neq \mathfrak{b} \subset F$ ein gebrochenes Ideal einer Ordnung $\mathcal{O}$ von F. Dann gibt es ein Ideal $\mathfrak{a} \subset O$, so dass $\mathfrak{b} = r\mathfrak{a}, r \in \mathbb{Q}^*$.*

Beweis. Seien $\xi \in \mathcal{O}$ und $\mathfrak{a}$ ein ganzes Ideal von $\mathcal{O}$ mit $\xi\mathfrak{b} = \mathfrak{a}$. Das Ideal $\mathfrak{a}$ hat Hermite-Normalform $\mathfrak{a} = a\mathbb{Z} + (b + c\omega)\mathbb{Z}$, daher ist

$$\mathfrak{b} = \frac{a\mathbb{Z} + (b + c\omega)\mathbb{Z}}{\xi} = \frac{a}{\xi}\mathbb{Z} + \frac{b + c\omega}{\xi}\mathbb{Z}.$$

Eine $\mathbb{Z}$-Basis für $\mathfrak{b}$ ist also $(\omega_1, \omega_2) := \left(\frac{a}{\xi}, \frac{b+c\omega}{\xi}\right)$. Nun sind aber $\omega_1, \omega_2 \in F$ und haben somit eine Darstellung $\omega_1 = \frac{\alpha_1}{d_1}, \omega_2 = \frac{\alpha_2}{d_2}, \alpha_i \in \mathcal{O}, d_i \in \mathbb{Z}$ (siehe [Wil93], Satz 4.22). Sei $d = \mathrm{kgV}(d_1, d_2)$, dann können wir $\mathfrak{b}$ schreiben als

$$\mathfrak{b} = \frac{\alpha_1\frac{d}{d_1}\mathbb{Z} + \alpha_2\frac{d}{d_2}\mathbb{Z}}{d}.$$

Aber $\alpha_1\frac{d}{d_1}\mathbb{Z} + \alpha_2\frac{d}{d_2}\mathbb{Z}$ ist ein ganzes Ideal von $\mathcal{O}$, denn $\frac{d}{d_i} \in \mathbb{Z}$ und

$$\left(\alpha_1\frac{d}{d_1}, \alpha_2\frac{d}{d_2}\right) = \left(\frac{ad}{\xi d_1}, \frac{(b + c\omega)d}{\xi d_2}\right)$$

sind linear unabhängig und somit Basis eines $\mathbb{Z}$-Moduls vom Rang 2. □

Nun können wir den Normbegriff auf gebrochene Ideale ausweiten:

3.22 Definition. Seien $\mathfrak{b}$ ein gebrochenes und $\mathfrak{a}$ ein ganzes Ideal von $\mathcal{O}$, so dass $\mathfrak{b} = \frac{\mathfrak{a}}{d}, d \in \mathbb{Z}$. Dann definieren wir $\mathcal{N}(\mathfrak{b}) := \frac{\mathcal{N}(\mathfrak{a})}{d^2}$

Jetzt betrachten wir die eigentlichen Ideale einer Ordnung etwas genauer:
Für jedes Ideal $\mathfrak{a} \subset \mathcal{O}$ gilt natürlich, dass $[\mathfrak{a}/\mathfrak{a}] \supseteq \mathcal{O}$, das folgt schon aus der Idealdefinition. Desweiteren ist auch jedes Element $\alpha \in [\mathfrak{a}/\mathfrak{a}]$ ganz über $\mathbb{Z}$, dies folgt mit dem *Kroneckerkriterium*, welches besagt, dass für einen Ring R mit $\mathrm{Quot}(R) =: F$ ein Element $\lambda \in F$ ganz über R ist, wenn es endlich viele Elemente $\omega_1, ..., \omega_n \in F$ gibt, so dass $\lambda(\omega_1, ..., \omega_n) = (\omega_1, ..., \omega_n)M$ für eine Matrix $M \in \mathbb{Z}^{(n\times n)}$. Dies ist hier aber der Fall, da jedes Ideal $\mathfrak{a}$ von $\mathcal{O}$ als $\mathfrak{a} = a\mathbb{Z} + (b + c\omega)\mathbb{Z}, a, b, c \in F$ darstellbar ist, also gilt (wegen $\lambda\mathfrak{a} \subset \mathfrak{a}$) das Gleichungssystem

$$\begin{aligned} \lambda a &= az_1 + (b + c\omega)z_2 \\ \lambda(b + c\omega) &= az_1' + (b + c\omega)z_2', \end{aligned}$$

mit $z_i, z_i' \in \mathbb{Z}$, also

$$\lambda(a, b + c\omega) = (a, b + c\omega)\begin{pmatrix} z_1 & z_1' \\ z_2 & z_2' \end{pmatrix}$$

Somit ist das Kronecker-Kriterium erfüllt, also α ganz über $\mathbb{Z}$. Daher gilt für jedes ganze Ideal $\mathfrak{a}$ einer Ordnung $\mathcal{O} : \mathcal{O} \subseteq [\mathfrak{a}/\mathfrak{a}] \subseteq \mathcal{O}_F$.
Allerdings ist zum Beispiel das Führerideal $\mathfrak{F}$ kein eigentliches Ideal von $\mathcal{O}$, da es ein Ideal sowohl von $\mathcal{O}$ also auch von $\mathcal{O}_F$ ist und somit $[\mathfrak{F}/\mathfrak{F}] = \mathcal{O}_F$.
Über eigentliche Ideale kann man folgende Aussage machen:

3.23 Satz. *Sei $\mathcal{O}$ eine Ordnung eines quadratischen Zahlkörpers, $\mathfrak{a}$ ein ganzes Ideal von $\mathcal{O}$. Dann gilt:*

$$\mathfrak{a} \textit{ invertierbar } \Leftrightarrow \mathfrak{a} \textit{ eigentliches Ideal von } \mathcal{O}$$

Beweis. Siehe [Lan73], Corollary auf Seite 91. □

3.24 Definition. Ein Ring R heisst *Dedekindring*, falls gelten:
- R ist noethersch
- jedes Primideal $\mathfrak{p} \subseteq R, \mathfrak{p} \neq \{0\}$ ist maximal
- R ist ganzabgeschlossen in seinem Quotientenkörper $\mathrm{Quot}(R)$

Die für uns wichtigste Aussage über einen Dedekindring R ist, dass es für jedes Ideal $\mathfrak{a} \subseteq R$ dann eine eindeutige Faktorisierung in Primideale gibt: $\mathfrak{a} = \prod_{i=1}^{n} \mathfrak{p}_i^{\mu_i}$ (siehe z.B. [PZ97],Theorem 4.5.6). Es gilt: Die Maximalordnung eines Zahlkörpers ist ein Dedekindring ([PZ97],Theorem 4.5.9).
Ist die von uns betrachtete Ordung keine Maximalordnung, so gilt immerhin folgender Satz über die Faktorisierung von Idealen:

3.25 Satz. *Sei $\mathcal{O}_F$ die Maximalordnung von $\mathcal{O}$, sei c der Führer von $\mathcal{O}$. Seien $I_F(c)$ bzw. $I_{\mathcal{O}}(c)$ die ganzen Ideale von $\mathcal{O}_F$ bzw. $\mathcal{O}$, welche prim zu c sind. Dann gibt es eine multiplikative Bijektion zwischen $I_F(c)$ und $I_{\mathcal{O}}(c)$, welche durch die inversen Abbildungen*

$$I_{\mathcal{O}}(c) \ni \mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_F \tag{3.26}$$

$$I_F(c) \ni \mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O} \tag{3.27}$$

gegeben ist. Alle Ideale in $I_{\mathcal{O}}(c)$ sind eigentliche Ideale von $\mathcal{O}$, also insbesondere invertierbar.

Beweis. siehe [Lan73], Theorem 8.1.4 □

Man kann daher ein zum Führer teilerfremdes ganzes Ideal $\mathfrak{a}$ von $\mathcal{O}$ in Primideale faktorisieren, indem man es mittels der in 3.26 beschriebenen Abbildung hochliftet ($\mathfrak{a}' = \mathfrak{a}\mathcal{O}_F$), dann dort faktorisiert ($\mathfrak{a}' = \prod \mathfrak{p}_i^{e_i}$) und dann jedes in der Faktorisierung von $\mathfrak{a}'$ enthaltene Primideal mittels der Abbildung aus 3.27 wieder herunterschneidet. Dann ist eine Faktorisierung von $\mathfrak{a}$ in Primideale gegeben durch $\mathfrak{a} = \prod(\mathfrak{p}_i \cap \mathcal{O})^{e_i}$, denn aus $\mathfrak{p}$ Primideal von $\mathcal{O}_F$ folgt $\mathfrak{p} \cap \mathcal{O}$ Primdeal von $\mathcal{O}$. Für alle nicht zum Führer teilerfremden Ideale ist nicht klar, wie man diese faktorisieren kann.

3.28 Lemma. *Seien $\mathfrak{b}$ ein gebrochenes, $\mathfrak{a}$ ein ganzes Ideal von $\mathcal{O}$ mit $\mathfrak{b} = \frac{\mathfrak{a}}{d}$ für ein $d \in \mathbb{Z}$. Dann gilt:*

(i) $\mathfrak{a}$ *invertierbar* $\Leftrightarrow$ $\mathfrak{b}$ *invertierbar.*

(ii) $[\mathfrak{a}/\mathfrak{a}] = \mathcal{O} \Leftrightarrow [\mathfrak{b}/\mathfrak{b}] = \mathcal{O}$.

Beweis. (i) $\mathfrak{a}$ invertierbar $\Leftrightarrow$ Es gibt ein gebrochenes Ideal $\mathfrak{a}'$ von $\mathcal{O}$ mit $\mathfrak{a}\mathfrak{a}' = \mathcal{O} \Leftrightarrow \frac{\mathfrak{a}}{d} d\mathfrak{a}' = \mathcal{O} \Leftrightarrow \mathfrak{b}$ invertierbar.

(ii) Es gilt für alle $a_1, a_2 \in \mathcal{O} : \lambda a_1 = a_2 \Leftrightarrow \lambda \frac{a_1}{d} = \frac{a_2}{d}$. Also

$$\begin{aligned} [\mathfrak{a}/\mathfrak{a}] = \mathcal{O} &\Leftrightarrow \{\lambda \in F \mid \lambda\mathfrak{a} \subset \mathfrak{a}\} = \mathcal{O} \\ &\Leftrightarrow \{\lambda \in F \mid \lambda\mathfrak{b} \subset \mathfrak{b}\} = \mathcal{O} \Leftrightarrow [\mathfrak{b}/\mathfrak{b}] = \mathcal{O}. \end{aligned}$$

□

3.29 Definition. Sei F ein Zahlkörper, p eine Primzahl und $\mathfrak{p}$ ein Primideal einer Ordnung von F. Falls $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$, dann sagen wir, dass $\mathfrak{p}$ über p liegt.
Sei nun $\mathcal{O}_F$ die Maximalordnung von F, sei $p\mathcal{O}_F = \mathfrak{p}_1\mathfrak{p}_2$ die Faktorisierung von $p\mathcal{O}_F$ in Primideale. Dann heisst p in F

- *verzweigt*, falls $\mathfrak{p}_1 = \mathfrak{p}_2$
- *träge*, falls $\mathfrak{p}_1 \neq \mathcal{O}_F = \mathfrak{p}_2$, falls also $p\mathcal{O}_F$ ein Primideal ist

- *zerlegt*, falls $\mathfrak{p}_1$ und $\mathfrak{p}_2$ nicht triviale unterschiedliche Primideale sind.

Falls p in F träge oder zerlegt ist, dann heisst p auch *unverzweigt* in F.

3.30 Definition. Sei $\mathcal{O}$ eine Ordnung in einem imaginärquadratischen Zahlkörper F, sei $I_\mathcal{O}$ die Gruppe der invertierbaren gebrochenen Ideale von $\mathcal{O}$, sei $P_\mathcal{O} \subset I_\mathcal{O}$ die Gruppe der gebrochenen Hauptideale von $\mathcal{O}$. Wir nennen $Pic(\mathcal{O}) = I_\mathcal{O}/P_\mathcal{O}$ die *Picardgruppe* von $\mathcal{O}$. Ist $\mathcal{O}$ die Maximalordnung von F, so bezeichnen wir $Pic(\mathcal{O})$ mit $Cl(F)$ und nennen es *Klassengruppe* von $\mathcal{O}$ bzw. von F. Die Anzahl der Elemente der Picardgruppe von $\mathcal{O}$ nennen wir die *Picardzahl*, Notation $h_\mathcal{O}$. Die Anzahl der Elemente der Klassengruppe von F heisst *Klassenzahl* von F, Notation h_F.

Durch Faktorisierung nach den Hauptidealen wird also $I_\mathcal{O}$ mittels einer Äquivalenzrelation $\sim$ in Klassen von Idealen aufgeteilt: Für zwei gebrochenen Ideale $\mathfrak{a}, \mathfrak{b}$ von $\mathcal{O}$ gilt $\mathfrak{a} \sim \mathfrak{b} \Leftrightarrow \exists \xi \in F : \mathfrak{a} = \xi\mathfrak{b}$.
Über die Klassenzahl von F kann man folgende Aussage machen:

3.31 Satz. *Die Klassenzahl ist endlich.*

Beweis. Siehe [PZ97], Corollary 6.2.9. □

Es gibt in KASH3 auch eine Funktion zum Berechnen der Klassenzahl eines Zahlkörpers, so dass wir uns um die genaue Formel keine weiteren Gedanken machen. Diese Funktion ist anwendbar auf quadratische Zahlkörper mit einer Diskriminante von bis zu 50 Dezimalstellen. Noch nicht implementiert ist allerdings ein Algorithmus, der die Picardzahl einer beliebigen Ordnung berechnet. Hier gilt folgende Beziehung:

3.32 Satz.

$$h_\mathcal{O} = h_F \frac{c}{(\mathcal{O}_F^* : \mathcal{O}^*)} \prod_{p \mid c} \left(1 - \left(\frac{F}{p}\right)\frac{1}{p}\right),$$

wobei c der Führer von $\mathcal{O}$ ist, $\mathcal{O}_F^*$ bzw. $\mathcal{O}^*$ die Einheiten von $\mathcal{O}_F$ bzw. von $\mathcal{O}$ bezeichnen und

$$\left(\frac{F}{p}\right) = \begin{cases} 1 & \text{für } p \text{ in } F \text{ zerlegt} \\ -1 & \text{für } p \text{ in } F \text{ träge} \\ 0 & \text{für } p \text{ in } F \text{ verzweigt} \end{cases}$$

Beweis. Siehe [Lan73], Theorem 8.1.7. □

Insbesondere ist auch die Picardzahl einer Ordnung endlich. Ausserdem gilt:

3.33 Lemma. *Seien $\mathfrak{a}, \mathfrak{b}$ ganze invertierbare Ideale von $\mathcal{O}$, $\xi \in F$.*

(i) $\mathfrak{ab}$ *ist invertierbar.*
(ii) $\xi\mathfrak{a}$ *ist invertierbar.*

Beweis. (i) $(\mathfrak{ab})(\mathfrak{b}^{-1}\mathfrak{a}^{-1}) = \mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}$.
(ii) $(\xi\mathfrak{a})(\mathfrak{a}^{-1}\xi^{-1}\mathcal{O}) = \xi\xi^{-1}\mathcal{O} = \mathcal{O}$.

□

Wir zitieren noch eine vereinfachte Version eines Satzes aus [PZ97] über die Faktorisierung von Idealen, welche über Primzahlen liegen:

3.34 Satz. *Seien F ein imaginärquadratischer Zahlkörper mit Maximalordnung $\mathcal{O}_F$, so dass $F = \mathbb{Q}(\rho)$, $\rho \in \mathcal{O}_F$. Sei f das Minimalpolynom von ρ und c der Führer von $\mathbb{Z}[\rho]$. Sei p eine Primzahl mit $p\mathcal{O}_F$ teilerfremd zu c. Sei $f \equiv f_1^{e_1} f_2^{e_2} \mod p$ die Faktorisierung von f modulo p in verschiedene normierte irreduzible Polynome (wobei $f_2 = 1$ und damit $e_2 = 0$ auch erlaubt ist). Dann ist die Faktorisierung von $p\mathcal{O}_F$ in Primideale gegeben durch $p\mathcal{O}_F = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}$ mit $\mathfrak{p}_i = p\mathcal{O}_F + f_i(\rho)\mathcal{O}_F$.*

Beweis. [PZ97], Theorem 6.2.27. □

Man erkennt also, falls $p\mathcal{O}_F$ teilerfremd zum Führer von $\mathcal{O}$ ist, ob p verzweigt, träge oder zerlegt ist, daran, wie das Minimalpolynom eines über $\mathbb{Z}$ ganzen Erzeugers von F modulo p zerfällt. Über die in einem Zahlkörper verzweigten Primzahlen kann man folgende wichtige Aussage machen:

3.35 Satz. *Eine Primzahl p ist genau dann verzweigt über einem Zahlkörper F, wenn $p|disc(F)$.*

Beweis. [Neu99], Theorem III.2.6. □

Es gilt also für alle Diskriminantenteiler $p \in \mathbb{P} : f \equiv (x-\lambda)^2 \mod p$.
Über Ideale kleiner Norm in der Picardgruppe gibt die Minkowskischranke Auskunft:

3.36 Satz. *Sei $\mathcal{O}$ eine Ordnung in einem imaginärquadratischen Zahlkörper. Dann enthält jede Idealklasse von $Pic(\mathcal{O})$ ein Ideal, deren Norm nicht grösser als die Minkowki-Schranke*

$$M_{\mathcal{O}} = \frac{2}{\pi}\sqrt{-disc(\mathcal{O})}$$

ist.

Beweis. siehe [Ste05], Theorem 5.8 □

Ist $\mathcal{O} = \mathcal{O}_F$ die Maximalordnung von F, dann bezeichnen wir die Minkowski-Schranke von $\mathcal{O}$ auch mit M_F.
Weiterhin gilt:

3.37 Lemma. *Die Klassengruppe $Cl(F)$ eines Zahlkörpers F lässt sich durch Produkte von über verzweigten und zerlegten Primzahlen liegenden Primidealen $\mathfrak{p}_i$ mit $\mathcal{N}(\mathfrak{p}_i) \leq M_F$ erzeugen.*

Beweis. Wegen Satz 3.36 gibt es in jeder Klasse von Idealen ein Ideal $\mathfrak{a}$ mit $\mathcal{N}(\mathfrak{a}) \leq M_F$. Sei $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_r^{e_r}$ die Primidealfaktorisierung eines solchen Ideals. Dann ist auch $\mathcal{N}(\mathfrak{p}_i) \leq M_F$ wegen der Multiplikativität der Norm. Also gibt es für jede Idealklasse einen Vertreter, der ein Produkt von Primidealen ist, deren Norm nicht grösser als die Minkowski-Schranke ist. Desweiteren gilt, dass jedes Primideal der Maximalordnung über einem Primideal von $\mathbb{Z}$ liegt: Sei $\mathfrak{P}$ ein Primideal von $\mathcal{O}_F$. Zunächst ist $\mathfrak{p} := \mathfrak{P} \cap \mathbb{Z} \neq \emptyset$ wegen $\mathcal{N}(\mathfrak{P}) \in \mathfrak{P} \cap \mathbb{Z}$. Es ist auch klar, dass $\mathfrak{p}$ wieder ein Primideal ist, da sonst $\mathfrak{P}$ kein Primideal sein könnte. Also ist $\mathfrak{p} = p\mathbb{Z}$ für eine Primzahl $p \in \mathbb{P}$. Da aber über trägen Primzahlen nur Hauptideale liegen, brauchen wir diese nicht zu betrachten. □

Über die Erzeuger der Picardgruppe einer beliebigen Ordung $\mathcal{O}$ kann man schwieriger Aussagen machen. Auch hier gilt natürlich, dass es in jeder Idealklasse ein Ideal $\mathfrak{a}$ mit $\mathcal{N}(\mathfrak{a}) \leq M_{\mathcal{O}}$ gibt. Allerdings können wir, falls dieses Ideal nicht teilerfremd zum Führer ist, keine Aussage über seine Primfaktoren machen. Aber es gilt noch folgender

3.38 Satz. *In der Äquivalenzklasse eines jeden invertierbaren Ideals einer Ordnung gibt es ein Ideal, welches teilerfremd zum Führer von $\mathcal{O}$ ist.*

Beweis. siehe [Lan73], Theorem 8.1.5. □

Man erzeugt also die Picardgruppe einer Ordnung aus Produkten von zum Führer der Ordnung teilerfremden Primidealen, welche über zerlegten oder verzweigten Primzahlen liegen.

Kapitel 4

Komplexe Multiplikation und Isogenien

Die dritte Möglichkeit der Definition einer elliptischen Kurve ist, neben den Zugängen über Varietäten und Funktionenkörpern, die über Gitter in $\mathbb{C}$. Hier zählen wir viele wichtige Fakten auf, ohne sie zu beweisen. Für einen weitergehenden Einblick in das Thema und nötige Beweise verweisen wir auf [Lan73], [Sil86] und [Sil94].

4.1 Grundlagen

4.1 Definition. Unter einem *Gitter* verstehen wir im folgenden eine Teilmenge $\Lambda \subseteq \mathbb{C}$, welche ein $\mathbb{Z}$-Modul vom Rang 2 mit Basis $(\omega_1, \omega_2), \omega_1 \in \mathbb{R}, \omega_2 \in \mathbb{C}\backslash\mathbb{R}$ ist. Wir gehen im Folgenden immer davon aus, dass $Im(\omega_1/\omega_2) > 0$.
Zwei Gitter Λ, Λ' heissen *homothetisch*, wenn es ein $\alpha \in \mathbb{C}$ gibt, so dass $\alpha\Lambda = \Lambda'$.

Zwei homothetische Gitter sind als $\mathbb{Z}$-Moduln isomorph, da sich die Basiselemente jeweils als Element des anderen Gitters darstellen lassen.

4.2 Definition. Eine Funktion $f : \mathbb{C} \to \mathbb{C}$ heisst *holomorph* in einem Punkt $z \in \mathbb{C}$, wenn für eine offene Umgebung U von z gilt: f ist in allen $x \in U$ komplex differenzierbar. Ist f in allen $z \in \mathbb{C}$ holomorph, so nennen wir f eine *holomorphe Funktion*. Die Funktion f heisst *meromorph*, wenn sie Quotient holomorpher Funktionen ist.

4.3 Definition. Sei $\Lambda \subseteq \mathbb{C}$ ein Gitter. Eine meromorphe Funktion $f : \mathbb{C} \to \mathbb{C}$ heisst eine (bzgl. Λ) *elliptische Funktion*, wenn $f(z + \omega) = f(z)\ \forall z \in \mathbb{C}, \omega \in \Lambda$. Die bezüglich Λ elliptischen Funktionen bilden einen Körper $\mathbb{C}(\Lambda)$.

Um einen vollständigen Überblick über eine bzgl. Λ elliptische Funktion f zu erhalten, genügt es, sie auf $\mathbb{C}/\Lambda$ zu betrachten. Eindeutige Repräsentanten für $\mathbb{C}/\Lambda$ werden durch ein sogenanntes *Fundamentalparallelotop* für Λ geliefert, d.h. die Menge $P_\Lambda := \{t_1\omega_1 + t_2\omega_2 \mid 0 \leqslant t_i < 1\}$.
Die wichtigste elliptische Funktion für unsere Zwecke ist die folgende:

4.4 Definition. Sei $\Lambda \subseteq \mathbb{C}$ ein Gitter. Die *Weierstrass-Funktion* $\wp_\Lambda : \mathbb{C} \to \mathbb{C}$ ist dann definiert als

$$\wp_\Lambda(z) := \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

(Für den Nachweis der Konvergenz, Meromorphie und Periodizität siehe z.B. [Sil86], VI.3.1)

4.5 Bemerkung. Notation: Wir werden im folgenden, wenn klar ist, um welches Gitter es sich handelt, statt $\wp_\Lambda$ nur $\wp$ schreiben. Dies gilt ebenso für die weiter unten definierten, eigentlich auch von Λ abhängigen Konstanten.

4.6 Lemma. *Die Ableitung von $\wp$ ist*

$$\wp'(z) = -2\sum_{\omega \in \Lambda} \frac{1}{(z-\omega)^3}.$$

Beweis. Siehe Beweis zu [Sil86], VI.3.1. □

Damit erhält man folgende Aussage:

4.7 Satz. *Für den Körper $\mathbb{C}(\Lambda)$ der bzgl. eines Gitters Λ elliptischen Funktionen gilt:*

$$\mathbb{C}(\Lambda) = \mathbb{C}(\wp, \wp').$$

Beweis. [Sil86],VI.3.2 □

4.8 Satz. *Für ein Gitter $\Lambda \subseteq \mathbb{C}$ setzen wir*

$$s_m := \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^m}, \;\; g_2 := 60s_4 \text{ und } \;\; g_3 := 140s_6$$

Dann gilt folgende Beziehung:

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3$$

Beweis. [Lan73], 1.2.5 □

Dies sieht doch sehr nach der Gleichung für eine elliptische Kurve aus! Es gilt tatsächlich, dass für ein Gitter $\Lambda \subseteq \mathbb{C}$ die Gleichung $y^2 = 4x^3 - g_2x - g_3$ eine elliptische Kurve über $\mathbb{C}$ definiert, d.h. die Diskriminante des Polynoms auf der rechten Seite ist $\neq 0$. Diese Kurve bezeichnen wir mit E_Λ. Haben wir also ein Gitter $\Lambda \subseteq \mathbb{C}$ gegeben, dann haben wir auch eine Abbildung

$$\mathbb{C}/\Lambda \to E_\Lambda, z \mapsto \begin{cases} (\wp(z), \wp'(z)) & \text{für } z \neq 0 \\ O & \text{sonst} \end{cases}$$

Auch die Umkehrung gilt:

4.9 Satz. *Sei $E : y^2 = 4x^3 - Ax - B,\ A, B \in \mathbb{C}$ eine elliptische Kurve. Dann gibt es ein Gitter $\Lambda \subseteq \mathbb{C}$ mit $g_2 = A$ und $g_3 = B$.*

Beweis. [Lan73], 3.3.2 □

Eine solche Kurve ist aber isomorph zu einer Kurve in kurzer Weierstrass-Form, so dass man andersherum zu einer Kurve der Form $y^2 = x^3 + ax + b$ immer eine isomorphe Kurve in der Form aus Satz 4.9 mit zugehörigem Gitter findet.
Im nächsten Abschnitt untersuchen wir die Frage, welche Aussagen man mithilfe der Gitterdarstellung über Isogenien machen kann.

4.2 Gitter und Isogenien

Sind $\Lambda_1, \Lambda_2 \subseteq \mathbb{C}$ Gitter mit $\alpha\Lambda_1 \subseteq \Lambda_2, \alpha \in \mathbb{C}$, dann induziert α eine Abbildung $\varphi_\alpha : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2,\ z \mapsto \alpha z \bmod \Lambda_2$. Diese Abbildung ist wohldefiniert, also unabhängig von der Wahl des Repräsentanten für z wegen

$$\varphi_\alpha(z + \omega) = \alpha(z + \omega) \bmod \Lambda_2 = (\alpha z + \alpha\omega) \bmod \Lambda_2 = \alpha z \bmod \Lambda_2\ \forall \omega \in \Lambda_1.$$

Hat man eine solche Gitterabbildung gegeben und definiert man die zugehörigen Kurven E_{Λ_1} und E_{Λ_2}, dann induziert α auch dort eine Abbildung

$$\begin{array}{llll} E_{\Lambda_1} \to & \mathbb{C}/\Lambda_1 \to & \mathbb{C}/\Lambda_2 \to & E_{\Lambda_2}, \\ P \mapsto & z \mapsto & \alpha z \bmod \Lambda_2 \mapsto & (\wp_{\Lambda_2}(\alpha z), \wp'_{\Lambda_2}(\alpha z)), \end{array}$$

wobei die erste Abbildung die „Umkehrabbildung“ von $z \mapsto (\wp_{\Lambda_1}(z), \wp'_{\Lambda_1}(z))$ ist. Andererseits definiert aber eine Isogenie $\varphi : E_{\Lambda_1} \to E_{\Lambda_2}$ eine Abbildung

$$\begin{array}{llll} \mathbb{C}/\Lambda_1 \to & E_{\Lambda_1} \to & E_{\Lambda_2} \to & \mathbb{C}/\Lambda_2, \\ z \mapsto & (\wp_{\Lambda_1}(z), \wp'_{\Lambda_1}(z)) \mapsto & \varphi(\wp_{\Lambda_1}(z), \wp'_{\Lambda_1}(z)) \mapsto & z', \end{array}$$

wobei die letzte Abbildung die Umkehrabbildung von $z \mapsto (\wp_{\Lambda_2}(z), \wp'_{\Lambda_2}(z))$ ist. Genauer gilt folgender

4.10 Satz. *Seien $\Lambda_1, \Lambda_2 \subset \mathbb{C}$ zwei Gitter. Wir bezeichnen mit $H(\Lambda_1, \Lambda_2)$ die Menge der holomorphen Abbildungen $\varphi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ mit $\varphi(0) = 0$. Dann gelten*

(a) Die Abbildung

$$\begin{array}{rcl} \{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subseteq \Lambda_2\} & \to & H(\Lambda_1, \Lambda_2) \\ \alpha & \mapsto & \varphi_\alpha \end{array}$$

ist eine Bijektion.

(b) Seien E_1 und E_2 elliptische Kurven mit zugehörigen Gittern Λ_1 und Λ_2. Dann ist die natürliche Einbettung

$$\{\textit{Isogenien } \varphi : E_1 \to E_2\} \quad \to \quad H(\Lambda_1, \Lambda_2)$$

eine Bijektion.

Beweis. Siehe [Sil86],VI.4.1. □

Haben wir also zwei Gitter Λ_1 und Λ_2 und ein $\alpha \in \mathbb{C}$ mit $\alpha\Lambda_1 \subseteq \Lambda_2$ gegeben, dann finden wir auch eine Isogenie, welche nach Umwandlung in eine holomorphe Abbildung dieselbe Abbildung liefert wie α. Andersherum stammt jede Isogenie $\varphi : E_{\Lambda_1} \to E_{\Lambda_2}$ von einer solchen Multiplikationsabbildung. Das folgende Diagramm kommutiert also:

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\alpha} & \mathbb{C} \\ \downarrow & & \downarrow \\ \mathbb{C}/\Lambda_1 & \xrightarrow{\varphi_\alpha} & \mathbb{C}/\Lambda_2 \\ {\scriptstyle z \mapsto (\wp_{\Lambda_1}(z), \wp'_{\Lambda_1}(z))}\downarrow & & \downarrow{\scriptstyle z \mapsto (\wp_{\Lambda_2}(z), \wp'_{\Lambda_2}(z))} \\ E_{\Lambda_1} & \xrightarrow[\varphi]{} & E_{\Lambda_2} \end{array}$$

Abbildung 4.1: Isogenien und Multiplikationsabbildungen von Gittern

Als Korollar aus Satz 4.10 folgt eine bedeutende Aussage über homothetische Gitter:

4.11 Korollar. *Für zwei Gitter $\Lambda, \Lambda' \subset \mathbb{C}$ gilt:*

$$\mathbb{C}/\Lambda \cong \mathbb{C}/\Lambda' \Leftrightarrow \exists \alpha \in \mathbb{C} : \alpha\Lambda = \Lambda'$$

Beweis. „⇒“ Sei $\mathbb{C}/\Lambda \cong \mathbb{C}/\Lambda'$. Dann gibt es nach Satz 4.10(a) Elemente $\alpha, \alpha' \in \mathbb{C}$ mit $\alpha\Lambda \subset \Lambda'$ und $\alpha'\Lambda' \subset \Lambda$, welche Isomorphismen

$$\varphi_\alpha : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda',\ z \bmod \Lambda \mapsto \alpha z \bmod \Lambda'$$

bzw.

$$\varphi_{\alpha'} : \mathbb{C}/\Lambda' \to \mathbb{C}/\Lambda, z \bmod \Lambda' \mapsto \alpha' z \bmod \Lambda$$

definieren. Da diese Abbildungen invers zueinander sind, muss $\alpha' = \frac{1}{\alpha}$ gelten und somit $\alpha\Lambda = \Lambda'$.
„⇐“ Gilt $\alpha\Lambda = \Lambda'$, dann definieren α und $\frac{1}{\alpha}$ wegen Satz 4.10(a) inverse Isomorphismen wie oben. Also gilt $\mathbb{C}/\Lambda \cong \mathbb{C}/\Lambda'$. □

Als Folgerung aus Korollar 4.11 ergibt sich eine wichtige Aussage über isomorphe elliptische Kurven:

4.12 Korollar. *Seien $\Lambda_1, \Lambda_2 \subseteq \mathbb{C}$ Gitter, E_{Λ_1} bzw. E_{Λ_2} die zugehörigen elliptischen Kurven. Dann gilt:*

$$E_{\Lambda_1} \cong E_{\Lambda_2} \Leftrightarrow \Lambda_1 \text{ und } \Lambda_2 \text{ homothetisch.}$$

Über die Endomorphismenringe elliptischer Kurven über $\mathbb{C}$ kann man folgende Aussage machen:

4.13 Satz. *Sei $E/\mathbb{C}$ eine elliptische Kurve und seien ω_1 und ω_2 Erzeuger für das zugehörige Gitter Λ. Dann gilt:*

(i) $\mathrm{End}(E) \cong \mathbb{Z}$ *oder*

(ii) $\mathbb{Q}(\omega_1/\omega_2)$ *ist ein imaginärquadratischer Zahlkörper und* $\mathrm{End}(E)$ *ist eine Ordnung in* $\mathbb{Q}(\omega_1/\omega_2)$.

Beweis. [Sil86],VI.5.5 □

Falls $\mathbb{Z} \subsetneq \mathrm{End}(E) = \mathcal{O}$, so sagen wir E hat *komplexe Multiplikation* mit $\mathcal{O}$.
Der Beweis des obigen Satzes benutzt die Tatsache, dass nach Satz 4.10 gilt:

$$\mathrm{End}(E_\Lambda) = \{\gamma \in \mathbb{C} \mid \gamma\Lambda \subseteq \Lambda\} \tag{4.14}$$

Das zu einer elliptischen Kurve gehörige Gitter Λ ist zwar nur bis auf Homothetie eindeutig, allerdings gilt für homothetische Gitter Λ_1, Λ_2 mit $\alpha\Lambda_1 = \Lambda_2$:

$$\mathrm{End}_1(E) := \{\gamma \in \mathbb{C} \mid \gamma\Lambda_1 \subseteq \Lambda_1\} = \{\gamma \in \mathbb{C} \mid \gamma\Lambda_2 \subseteq \Lambda_2\} =: \mathrm{End}_2(E)$$

denn:

$$\gamma \in \mathrm{End}_1(E) \Leftrightarrow \gamma\Lambda_1 \subseteq \Lambda_1 \Leftrightarrow \alpha\gamma\Lambda_1 \subseteq \alpha\Lambda_1 = \Lambda_2 \Leftrightarrow \gamma \in \mathrm{End}_2(E).$$

Der mithilfe von (4.14) bestimmte Endomorphismenring ist also unabhängig von der Wahl von Λ.
Haben wir eine elliptische Kurve $E/\mathbb{C}$ mit Endomorphismenring $\mathcal{O}$ und $\mathrm{Quot}(\mathcal{O}) = F$ gegeben, so kann man folgendermassen zu E isogene Kurven mit demselben Endomorphismenring „konstruieren“: Sei $\mathfrak{a} \subset F$ ein invertierbares gebrochenes Ideal von $\mathcal{O}$. Dann ist $\mathfrak{a}$ auch ein Gitter. Es gibt also eine elliptische Kurve $E_\mathfrak{a}$ und

$$\begin{aligned} \mathrm{End}(E_\mathfrak{a}) &= \{\gamma \in \mathbb{C} \mid \gamma\mathfrak{a} \subseteq \mathfrak{a}\} \\ &= \{\gamma \in F \mid \gamma\mathfrak{a} \subseteq \mathfrak{a}\} \qquad (4.15) \\ &= \mathcal{O} \qquad (4.16) \end{aligned}$$

Hierbei gilt die Gleichheit in (4.15), da $\mathfrak{a} \subseteq F$, und in (4.16), da $\mathfrak{a}$ ein invertierbares Ideal von $\mathcal{O}$ ist und somit $[\mathfrak{a}/\mathfrak{a}] = \mathcal{O}$ nach Lemma 3.28.
Wenn $\mathfrak{a}$ nicht invertierbar ist, dann ist

$$\{\gamma \in F \mid \gamma\mathfrak{a} \subseteq \mathfrak{a}\} \supsetneq \mathcal{O}, \qquad (4.17)$$

siehe Kapitel 3. Jedes invertierbare Ideal $\mathfrak{a} \subset F$ von $\mathcal{O}$ definiert also eine zu E isogene Kurve mit gleichem Endomorphismenring. Da aber homothetische Gitter isomorphe Kurven definieren, also $E_{c\mathfrak{a}} \cong E_\mathfrak{a}\ \forall c \in F$, genügt es, die Menge der invertierbaren Ideale modulo den Hauptidealen zu betrachten. Diese Menge ist aber gerade die Picardgruppe $Pic(\mathcal{O})$. Setzen wir also

$$\mathcal{ELL}(\mathcal{O}) := \frac{\{\text{elliptische Kurven } E/\mathbb{C} \text{ mit } \mathrm{End}(E) = \mathcal{O}\}}{\text{Isomorphismen über } \mathbb{C}},$$

dann gilt folgender

4.18 Satz.

$$\#Pic(\mathcal{O}) = \#\mathcal{ELL}(\mathcal{O})$$

Für ein gebrochenes Ideal $\mathfrak{a} \subset F$ von $\mathcal{O}$ bezeichnet $\overline{\mathfrak{a}}$ die Klasse von $\mathfrak{a}$ in $Pic(\mathcal{O})$. Zusammenfassend gilt dann folgende

4.19 Proposition. *(a) Sei Λ ein Gitter mit $E_\Lambda \in \mathcal{ELL}(\mathcal{O})$, seien $\mathfrak{a}, \mathfrak{b}$ invertierbare gebrochene Ideale von $\mathcal{O}$. Dann gilt:*

(i) $\mathfrak{a}\Lambda$ ist ein Gitter in $\mathbb{C}$.

(ii) Für die elliptische Kurve $E_{\mathfrak{a}\Lambda}$ gilt: $End(E_{\mathfrak{a}\Lambda}) = \mathcal{O}$.

(iii) $E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda} \Leftrightarrow \overline{\mathfrak{a}} = \overline{\mathfrak{b}}$.

Die Abbildung

$$Pic(\mathcal{O}) \times \mathcal{ELL}(\mathcal{O}) \to \mathcal{ELL}(\mathcal{O}),\ \overline{\mathfrak{a}} * E_\Lambda = E_{\mathfrak{a}^{-1}\Lambda} \tag{4.20}$$

ist also wohldefiniert.
(b) Die durch 4.20 beschriebene Operation ist transitiv und frei, d.h.
$\forall E_1, E_2 \in \mathcal{ELL}(\mathcal{O})$ *gibt es genau ein* $\overline{a} \in Pic(\mathcal{O})$, *so dass* $\overline{a} * E_1 = E_2$.

Beweis. Der Satz ist entnommen aus [Sil94], Proposition II.1.2. Dort wird zwar $\mathrm{End}(E) = \mathcal{O}_F$ vorausgesetzt, die einzige Voraussetzung an die verwendeten Ideale ist aber die Invertierbarkeit, der Satz gilt demnach auch für Kurven mit beliebigen Endomorphismenringen. □

Wir werden später einen Algorithmus angeben, der die oben definierte Abbildung für bestimmte Ideale berechnet. Zu bemerken bleibt noch, dass zwar für Ideale $\mathfrak{a}$ und $\mathfrak{b}$ mit $\overline{\mathfrak{a}} = \overline{\mathfrak{b}}$ wie oben erwähnt die Kurven $E_{\mathfrak{a}^{-1}\Lambda}$ und $E_{\mathfrak{b}^{-1}\Lambda}$ isomorph sind, aber trotzdem die Abbildungen, welche durch die Ideale definiert werden, unterschiedlich sind. Ausserdem gilt noch folgender Satz:

4.21 Satz. *Seien $\Lambda \subset \mathbb{C}$ ein Gitter $E_\Lambda \in \mathcal{ELL}(\mathcal{O})$ und $\mathfrak{a} \subset \mathcal{O}$ ein echtes Ideal. Dann hat die natürliche Abbildung $\overline{\mathfrak{a}} * E_\Lambda$ den Grad $\mathcal{N}(\mathfrak{a})$.*

Beweis. Siehe [Sil94], Corollary II.1.5. □

Können wir nun diese Ergebnisse über elliptische Kurven über $\mathbb{C}$ auch für elliptische Kurven über endlichen Körpern anwenden?

Seien M ein Zahlkörper mit Maximalordnung $\mathcal{O}$ und $\mathfrak{p} \in \mathcal{O}$ ein Primideal. Die *Lokalisierung* von $\mathcal{O}$ an $\mathfrak{p}$ bezeichnen wir mit $\mathcal{O}_\mathfrak{p} := \{\frac{x}{y} \mid x \in \mathcal{O}, y \in \mathcal{O}\backslash\mathfrak{p}\} \subset M$. Dann ist $\mathfrak{p}\mathcal{O}_\mathfrak{p}$ das einzige maximale Ideal von $\mathcal{O}_\mathfrak{p}$ und somit $\mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p}$ ein Körper. Es ist sogar ein endlicher Körper: Es gibt einen kanonischen Isomorphismus $\mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p} \leftrightarrow \mathcal{O}/\mathfrak{p}$([Lan70], p.37). Sei $p \in \mathbb{Z}$ so, dass $\mathfrak{p}$ über $p\mathbb{Z}$ liegt. Dann ist erstens $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$ und andererseits $[\mathcal{O}/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}] \leq [M : \mathbb{Z}]$ ([Jan96],I.6.5). Somit ist $\mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p}$ ein endlicher Körper der Charakteristik p.
Sei nun E eine elliptische Kurve, definiert durch eine Gleichung $f(x, y) = 0$,
$f \in \mathcal{O}_\mathfrak{p}[x, y] \subset M(x, y)$. Man sagt E hat *nicht-degenerierte Reduktion* an $\mathfrak{p}\mathcal{O}_\mathfrak{p}$, wenn die Gleichung $f(x, y) = 0$, deren Koeffizienten mod $\mathfrak{p}\mathcal{O}_\mathfrak{p}$ reduziert wurden, eine ordinäre elliptische Kurve über $\mathbb{F}_{p^k} := \mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p}$, definiert. Die Reduktion von E mod $\mathfrak{p}\mathcal{O}_\mathfrak{p}$ nennen wir $\overline{E}$.

Seien nun E_1 und E_2 über $\mathcal{O}_\mathfrak{p}$ definierte elliptische Kurven mit guten Reduktionen $\overline{E_i}$ an $\mathfrak{p}\mathcal{O}_\mathfrak{p}$, sei $\varphi : E_1 \to E_2$ eine Isogenie. Dann bezeichnen wir die koeffizientenweise Reduktion von φ mod $\mathfrak{p}\mathcal{O}_\mathfrak{p}$ mit $\overline{\varphi} : \overline{E_1} \to \overline{E_2}$ (vergleiche [Lan73], 9.2). Mithilfe dieser Begriffe können wir nun die folgenden zwei Sätze formulieren:

4.22 Satz. *Sei E eine elliptische Kurve über einem Zahlkörper M mit $\mathcal{O} := Cl(\mathbb{Z}, M)$, sei $End(E) = \mathcal{O}_E$ eine Ordnung in einem imaginärquadratischen Zahlkörper mit Führer c. Sei $\mathfrak{p}$ ein Ideal in $\mathcal{O}_E$ über einer zerlegten Primzahl p, so dass E an $\mathfrak{p}\mathcal{O}_\mathfrak{p}$ gute Reduktion hat. Dann gilt:*

- *$End(\overline{E}) = \mathbb{Z} + c_0\mathcal{O}$ mit $c = p^r c_0,\ p \nmid c_0$*

- *wenn $p \nmid c$, dann $End(\overline{E}) \cong End(E)$*

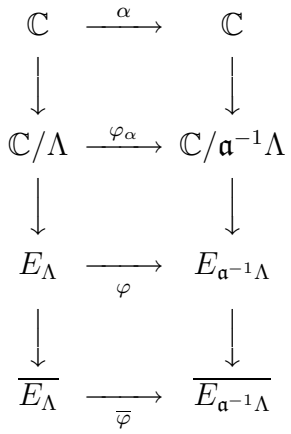
Beweis. [Lan73], Theorem 13.4.12. □

Es geht auch andersherum:

4.23 Satz. ***(Deuring-Lift)***
Seien $\widetilde{E}/\mathbb{F}_{p^r}$ eine elliptische Kurve und φ ein nicht-trivialer Endomorphismus von $\widetilde{E}$. Dann gibt es eine über einem Zahlkörper M definierte elliptische Kurve E, $\alpha \in End(E)$ und ein über p liegendes Primideal $\mathfrak{p} \in Cl(\mathbb{Z}, M)$, an dem E gute Reduktion hat, so dass es einen Isomorphismus $\psi : \overline{E} \to \widetilde{E}$ gibt mit $\varphi = \psi\overline{\alpha}\psi^{-1}$.

Beweis. [Lan73],13.5, Theorem 14 □

Nun können wir die obigen Ergebnisse über isogene Kurven über $\mathbb{C}$ auf Kurven über endlichen Körpern übertragen:
Sei $\widetilde{E}/\mathbb{F}_{p^r}$ eine elliptische Kurve. Dann gibt es eine elliptische Kurve E/M über einem Zahlkörper $M \subset \mathbb{C}$, so dass $\widetilde{E} \cong \overline{E}$ für ein passendes Primideal $\mathfrak{p} \subset \mathcal{O}_M$, welches über $p\mathbb{Z}$ liegt. Sei $\mathfrak{a} \subset \mathrm{End}(E) =: \mathcal{O}$ ein gebrochenes Ideal von $\mathcal{O}$ mit $[\mathfrak{a}/\mathfrak{a}] = \mathcal{O}$ und $E_\mathfrak{a}$ die zum Gitter $\mathfrak{a}$ gehörige Kurve. Dann gibt es auch eine Isogenie $\varphi : E \to E_\mathfrak{a}$. Es hat nun auch $E_\mathfrak{a}$ gute Reduktion an $\mathfrak{p}$ (siehe [ST68], Corollary 2). Also gibt es eine Isogenie $\overline{\varphi} : \widetilde{E} \to \overline{E_\mathfrak{a}}$. Wir können daher in Diagramm 4.1 noch eine Ebene hinzufügen:



Später werden wir einen Algorithmus angeben, der eine solche Isogenie berechnet.

Kapitel 5

Endomorphismenringe elliptischer Kurven

In diesem Kapitel stellen wir den Algorithmus von Kohel zur Berechnung des Endomorphismenrings elliptischer Kurven über endlichen Körpern vor. Während des gesamten Kapitels sei E/K eine über dem endlichen Körper K der Charakteristik p definierte ordinäre elliptische Kurve in Weierstrass-Form.
Eine weitere Charakterisierung für ordinäre Kurven, die wir später benötigen werden, ist $\mathrm{ggT}(t, p) = 1$ (vgl. [Koh96], Chapter 4), wobei t die Spur des Frobeniusendomorphismus der Kurve bezeichnet.
Zunächst gilt für den Ring $\mathrm{End}(E)$ der Endomorphismen von E folgender

5.1 Satz. *End(E) ist eine Ordnung in einem imaginärquadratischen Zahlkörper.*

Beweis. Siehe [Sil86], Theorem V.3.1 (b). □

Dies kann man sich wie folgt vorstellen: Es ist immer $\mathbb{Z} \subseteq \mathrm{End}(E)$, dies sind die Multiplikation-mit-m-Abbildungen. Ausserdem ist der Frobenius-Endomorphismus π ein Element von $\mathrm{End}(E)$, dieser hat als charakteristisches Polynom die quadratische Gleichung $\pi^2 - t\pi + q$, deren Lösungen sind $\frac{t}{2} \pm \sqrt{\frac{t^2}{4} - q}$. Nach dem Satz von Hasse ist $|t| \leqslant 2\sqrt{q}$, also ist der Term unter der Wurzel $\leqslant 0$. Falls aber $|t| = 2\sqrt{q}$, dann ist E supersingulär. Da wir hier nur ordinäre Kurven betrachten, gilt also immer $\pi \in \mathbb{C}\backslash\mathbb{R}$.
Sei nun E eine elliptische Kurve und $\mathcal{O}_F$ die Maximalordnung zur charakteristischen Gleichung von π. Das Ziel dieses Kapitels ist es, $c \in \mathbb{Z}$ zu bestimmen, so dass $\mathcal{O} := \mathrm{End}(E) = \mathbb{Z} + c\mathcal{O}_F$, also den Führer von $\mathcal{O}$ zu berechnen. Damit ist $\mathcal{O}$ eindeutig bestimmt.
Wir wissen auf jeden Fall immer, dass $\mathbb{Z}[\pi] \subseteq \mathcal{O}$. Falls $\mathbb{Z}[\pi]$ schon die Maximalordnung ist, dann gilt $c = 1$ und $\mathcal{O} = \mathbb{Z}[\pi] = \mathcal{O}_F$.

Sei nun $D := \mathrm{disc}(\mathcal{O}_F)$, $d_\pi := \mathrm{disc}(\mathbb{Z}[\pi]) = t^2 - 4q$, denn: Sei $\mathcal{O}_\pi = \mathbb{Z}[\pi]$ und $f_\pi(x) = x^2 - tx + q$ das Minimalpolynom für π. Dann ist

$$\mathrm{disc}(\mathbb{Z}[\pi]) = \mathrm{disc}(f_\pi) = (x^{(1)} - x^{(2)})^2,$$

wobei $x^{(i)}$ die Nullstellen von f sind. Dies ist nach der p-q-Formel

$$\left(\frac{t}{2} + \sqrt{\frac{t^2}{4} - q} - \frac{t}{2} + \sqrt{\frac{t^2}{4} - q}\right)^2 = \left(2\sqrt{\frac{t^2}{4} - q}\right)^2 = 4\left(\frac{t^2}{4} - q\right) = t^2 - 4q.$$

Den Führer von $\mathbb{Z}[\pi]$ nennen wir $m := \sqrt{\frac{d_\pi}{D}}$. Zwischen $\mathbb{Z}[\pi]$ und $\mathcal{O}_F$ liegen dann noch die Ringe $\mathbb{Z} + c\mathcal{O}_F$ für alle Teiler c von m, die Möglichkeiten für $\mathcal{O}$ sind also durch die Teiler von m beschränkt.
Weiterhin gilt: Falls $\#E_1(K) = \#E_2(K)$, dann ist auch die charakteristische Gleichung des Frobenius-Endomorphismus von E_1 gleich der des Frobenius-Endomorphismus von E_2, somit ist die Maximalordnung zu $\mathrm{End}(E_1)$ gleich der zu $\mathrm{End}(E_2)$, die Endomorphismenringe können also in denselben Ring eingebettet werden.
Eine Schlüsselrolle bei der Bestimmung des Führers des Endomorphismenrings spielt folgender

5.2 Satz. *([Koh96], Proposition 21) Sei $\varphi : E \to E'$ eine Isogenie von primem Grad ℓ zwischen ordinären elliptischen Kurven über $\mathbb{F}_{p^r}$. Sei $\ell \neq p$ und seien $\mathcal{O}$ bzw. $\mathcal{O}'$ die Endomorphismenringe von E bzw. E'. Dann gilt einer der folgenden drei Fälle:*

(i) $\mathcal{O} \subsetneq \mathcal{O}'$ *und* $\mathcal{O} = \mathbb{Z} + \ell\mathcal{O}'$

(ii) $\mathcal{O}' \subsetneq \mathcal{O}$ *und* $\mathcal{O}' = \mathbb{Z} + \ell\mathcal{O}$

(iii) $\mathcal{O} = \mathcal{O}'$.

Beweis. Wir geben hier den etwas ausführlicheren Beweis aus [Hen02], Satz 5.1.5, wieder.
Es gilt:

$$\mathbb{Z} + \ell^2\mathcal{O} \overset{(i)}{\subseteq} \mathbb{Z} + \widehat{\varphi}\mathcal{O}'\varphi \overset{(ii)}{\subseteq} \mathcal{O},$$

denn: Die Mengeninklusion (ii) gilt wegen $\mathbb{Z} \subset \mathcal{O}$ und $\widehat{\varphi}\psi\varphi : E \to E$ für alle $\psi \in \mathcal{O}'$, somit $\widehat{\varphi}\mathcal{O}'\varphi \subset \mathcal{O}$. Für (i) schreiben wir $\mathbb{Z}+\ell^2\mathcal{O} = \mathbb{Z}+\widehat{\varphi}\varphi\mathcal{O}\widehat{\varphi}\varphi \subset \mathbb{Z}+\widehat{\varphi}\mathcal{O}'\varphi$ wegen $\varphi\psi\widehat{\varphi} : E' \to E'$ für alle $\psi \in \mathcal{O}$.
Desweiteren ist $\mathbb{Z} + \widehat{\varphi}\mathcal{O}'\varphi \cong \mathbb{Z} + \ell\mathcal{O}'$ mittels $\widehat{\varphi}\psi\varphi \mapsto \varphi\widehat{\varphi}\psi = \ell\psi$.
Falls weder bei (i) noch bei (ii) Gleichheit gilt, so ist $\mathcal{O} = \mathcal{O}'$, denn $\mathcal{O}$ enthält dann $\mathbb{Z}+\widehat{\varphi}\mathcal{O}'\varphi \cong \mathbb{Z}+\ell\mathcal{O}'$ mit Index ℓ. Gilt Gleichheit in (i), dann ist $\mathbb{Z}+\ell^2\mathcal{O} = \mathbb{Z}+\ell\mathcal{O}'$, somit enthält $\mathcal{O}$ den Endomorphismenring $\mathcal{O}'$ mit Index ℓ. Bei Gleichheit in (ii) ist $\mathcal{O} = \mathbb{Z} + \ell\mathcal{O}'$, also $\mathcal{O}'$ enthält $\mathcal{O}$ mit Index ℓ. □

Ist E/K gegeben und sind $j(E)$, $\mathbb{Z}[\pi]$, $\mathcal{O}_F$ und der Führer m von $\mathbb{Z}[\pi]$ berechnet, so ist die Grundidee des Algorithmus, für alle Primteiler ℓ von m zu testen, ob das Modulpolynom $\Psi_\ell(j(E), x)$ vom Grad ℓ Nullstellen in K besitzt. Ist $\tilde{j}$ eine solche Nullstelle, dann wissen wir, dass es eine über K definierte Isogenie $\varphi : E \to E'$ mit $j(E') = \tilde{j}$ vom Grad ℓ gibt. Da $\mathrm{ggT}(t, p) = 1$ gilt, sind alle Teiler des Führers prim zu p, somit sind die Voraussetzungen von Satz 5.2 immer erfüllt. Allerdings ist noch nicht klar, wie die Beziehung zwischen $\mathrm{End}(E)$ und $\mathrm{End}(E')$, für die es nach Satz 5.2 nur 3 Möglichkeiten gibt, aussieht.
Um mögliche Beziehungen zu beschreiben, benötigen wir noch einige Definitionen:

5.3 Definition. Wir sagen, eine Isogenie $\varphi : E \to E'$ vom Grad ℓ

- geht *nach oben*, wenn $[\mathrm{End}(E') : \mathrm{End}(E)] = \ell$
- geht *nach unten*, wenn $[\mathrm{End}(E) : \mathrm{End}(E')] = \ell$
- verläuft *horizontal*, wenn $\mathrm{End}(E) = \mathrm{End}(E')$.

Wir nennen $\mathrm{End}(E)$ *maximal bei* ℓ, falls ℓ den Führer von $\mathrm{End}(E)$ nicht teilt.

Wenn wir also den Endomorphismenring einer Kurve E/K betrachten und eine K-Isogenie vom Grad ℓ nach oben finden, dann wissen wir, dass ℓ den Führer von $\mathrm{End}(E)$ teilt. Ob es ℓ-Isogenien gibt, können wir über die Nullstellen des Modulpolynoms $\Psi_\ell(j(E), x)$ herausfinden. Woher wissen wir aber, ob diese nach oben, nach unten oder horizontal verlaufen? Dabei hilft uns folgender

5.4 Satz. *Sei $E/\mathbb{F}_q$ eine elliptische Kurve mit Endomorphismenring $\mathcal{O}$, π der Frobenius-Endomorphismus von E, $\mathcal{O}_F$ die Maximalordnung von $\mathbb{Z}[\pi]$, D die Diskriminante von $\mathcal{O}$, ℓ eine Primzahl und $(\frac{D}{\ell})$ das Legendresymbol. Dann gilt:*

(i) Falls $\ell \nmid [\mathcal{O}_F : \mathcal{O}]$, dann gibt es $(1 + (\frac{D}{\ell}))$ $\mathbb{F}_q$-Isogenien vom Grad ℓ zu elliptischen Kurven mit gleichem Endomorphismenring.

(ii) Falls $\ell \mid [\mathcal{O}_F : \mathcal{O}]$, dann gibt es genau eine $\mathbb{F}_q$-Isogenie vom Grad ℓ nach oben.

(iii) Falls $\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$ und $\ell \mid [\mathcal{O}_F : \mathcal{O}]$, dann gibt es ℓ $\mathbb{F}_q$-Isogenien vom Grad ℓ nach unten.

(iv) Falls $\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$ und $\ell \nmid [\mathcal{O}_F : \mathcal{O}]$, dann gibt es $\ell - (\frac{D}{\ell})$ $\mathbb{F}_q$-Isogenien vom Grad ℓ nach unten.

Beweis. Siehe [Hen02], 5.2.2. □

Fall		Typ	$\#\mathcal{N}_\ell$	
$\ell \nmid [\mathcal{O}_F : \mathcal{O}]$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + (\frac{D}{\ell}) \rightarrow$	$1 + (\frac{D}{\ell})$	(a)
	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$	$\begin{cases} 1 + (\frac{D}{\ell}) \rightarrow \\ \ell - (\frac{D}{\ell}) \downarrow \end{cases}$	$\ell + 1$	(b)
$\ell \mid [\mathcal{O}_F : \mathcal{O}]$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 \uparrow$	1	(c)
	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$	$\begin{cases} 1 \uparrow \\ \ell \downarrow \end{cases}$	$\ell + 1$	(d)

Tabelle 5.1: Typen und Anzahl von Isogenien vom Grad ℓ

Die Tabelle 5.1 stammt aus [FM02] und enthält eine sehr übersichtliche Version von Satz 5.4. Hierbei ist $\mathcal{N}_\ell$ die Menge der Nullstellen von $\Psi_\ell(j(E), x)$ in $\mathbb{F}_q$. Die Richtung des Pfeils in der Typ-Spalte gibt die Richtung der Isogenien an.
Wie benutzen wir nun diese Erkenntnisse zur Bestimmung von $\mathcal{O}$? Sei als einfaches Beispiel E so, dass $[\mathcal{O}_F : \mathbb{Z}[\pi]] = \ell$ eine Primzahl ist. Dann gibt es nur zwei Möglichkeiten für $\mathcal{O}$: Entweder $\mathcal{O} = \mathcal{O}_F$ oder $\mathcal{O} = \mathbb{Z}[\pi]$. Falls $\mathcal{O} = \mathcal{O}_F$, dann befinden wir uns in Zeile (b) der Tabelle, das Modulpolynom $\Psi_\ell(j(E), x)$ muss also $\ell + 1$ Nullstellen in $\mathbb{F}_q$ haben. Im anderen Fall ist (c) die passende Tabellenspalte, das Modulpolynom $\Psi_\ell(j(E), x)$ hat also nur eine Nullstelle in $\mathbb{F}_q$.
Fall (a) spielt für den folgenden Algorithmus keine Rolle, denn wir wollen aus den Teilern des Führers von $\mathbb{Z}[\pi]$ den Führer von $\mathcal{O}$ ermitteln. Wenn aber $\ell \nmid [\mathcal{O}_F : \mathcal{O}]$ und $\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$, dann ist ℓ kein Teiler des Führers von $\mathbb{Z}[\pi]$.

Wir stellen nun den Algorithmus von Kohel zur Berechnung von Endomorphismenringen ordinärer elliptischer Kurven über endlichen Körpern vor, wie er auch in [Hen02] beschrieben wird:
Seien $\mathrm{End}(E) = \mathcal{O}$ und $c = \ell_1^{e_1} \cdot \ldots \cdot \ell_r^{e_r}$ der Führer von $\mathbb{Z}[\pi]$. Unser Ziel ist die Berechnung von $m \in \mathbb{Z}$ mit $\mathcal{O} = \mathbb{Z} + \frac{c}{m}\mathcal{O}_F$. Zu Beginn setzen wir $m := 1$. Für jedes $i \in \{1 \ldots r\}$ werden nun zwei verschiedene Folgen von isogenen elliptischen Kurven bzw. deren j-Invarianten erzeugt, jeweils ausgehend von der Kurve, deren Endomorphismenring wir bestimmen wollen. Sei ℓ^e ein Teiler von c mit passendem Exponenten. Eine Folge von j-Invarianten wird immer dann beendet, wenn wir schon e Schritte gelaufen sind oder wenn $\#\mathcal{N}_\ell = 1$ für die aktuelle j-Invariante gilt. Letzteres ist immer nur dann der Fall, wenn die aktuelle j-Invariante zu einer elliptischen Kurve E' mit $\ell \nmid [\mathrm{End}(E') : \mathbb{Z}[\pi]]$ gehört. Die Längen der beiden Folgen merken wir uns. Falls nun $\ell \mid [\mathcal{O}_F : \mathcal{O}]$ und $\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$, dann gilt gleich

$\#\mathcal{N}_\ell = 1$, wir wissen also sofort, dass ℓ^e den Führer von $\mathcal{O}$ teilt. In diesem Fall verändern wir m nicht.
Falls $\ell \mid [\mathcal{O}_F : \mathcal{O}]$ und $\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$, dann gibt es nur eine ℓ-Isogenie nach oben, d.h. eine der beiden Folgen wird, da wir mit unterschiedlichen Nullstellen beginnen, „nach unten gehen“. Die elliptische Kurve zu der entsprechenden j-Invariante wird also mit der Ausgangskurve durch eine ℓ-Isogenie nach unten verbunden sein. Dann ist aber die gesamte Folge absteigend, denn es gibt von einer solchen j-Invariante immer nur eine Isogenie nach oben, der Rest führt nach unten. Da wir von oben gekommen sind und uns immer die vorherige j-Invariante merken und eine andere als diese als neue j-Invariante auswählen, gehen wir zwangsläufig nach unten. Sind wir dann bei einer j-Invariante j^* „ganz unten“ angekommen, dann hat $\Psi_\ell(j^*, x)$ nur noch eine Nullstelle in $\mathbb{F}_q$ und der richtige Faktor des Führers wird durch die gespeicherte Anzahl der Schritte ermittelt: Wir setzen $m := m\ell^s$, wobei s das Minimum der Längen der beiden Folgen ist. Die Folge, die nicht nach unten geht, wird zwangsläufig immer länger sein als die, die nach unten geht, siehe Tabelle 5.1.
Falls $\ell \nmid [\mathcal{O}_F : \mathcal{O}]$, dann laufen wir entweder horizontal oder nach unten. Hat das Modulpolynom an der aktuellen j-Invariante nur eine Nullstelle, dann sind wir ganz unten angekommen, allerdings sind wir dann auch schon e Schritte gelaufen, so dass also auch hier mit $m := m\ell^e$ der richtige Faktor ermittelt wird.

5.5 Algorithmus. ***Berechung des Endomorphismenrings***
Input: *ordinäre elliptische Kurve* $E/\mathbb{F}_q$
Output: *Führer* m *von* $End_{\mathbb{F}_q}(E)$ *oder ERROR, falls einer der Teiler von* $m > 60$

- $\pi :=$ *Frobenius-Endomorphismus von* E, $j := j(E)$, $m := 1$
- $c :=$ *Führer von* $\mathbb{Z}[\pi]$, $L :=$*Faktorisierung von* c [1]
- *IF* $L[\#L][1] > 60$ *THEN RETURN ERROR*
- *FOR* $i \in \{1 \dots \#L\}$ *DO*
  - $\ell := L[i][1]$, $e := L[i][2]$, $r_1 := 0$, $r_2 := 0$
  - $\Psi_\ell :=$ ℓ*-tes Modulpolynom,* $\mathcal{N}_\ell :=$ *Nullstellen von* $\Psi_\ell(j, x)$ *in* $\mathbb{F}_q$
  - *IF* $\#\mathcal{N}_\ell = 1$ *THEN* $i := i + 1$
  - *ELSE*
    - $j_{r_1} := \mathcal{N}_\ell[1]$, $j_{r_2} := \mathcal{N}_\ell[2]$, $j_{alt} := j$, $r_1 := 1$, $r_2 := 1$
    - *FOR* $k \in \{1, 2\}$ *DO*
      - *WHILE* $r_k \leqslant e$ *DO*
        - $\mathcal{N}_\ell :=$ *Nullstellen von* $\Psi_\ell(j_{r_k}, x)$
        - *IF* $\#\mathcal{N}_\ell = 1$ *THEN* $k := k + 1, j_{alt} := j$
        - *ELSE*
          - *IF* $\mathcal{N}_\ell[1] = j_{alt}$ *THEN* $j_{r'_k} := \mathcal{N}_\ell[2]$
          - *ELSE* $j_{r'_k} := \mathcal{N}_\ell[1]$
          - *END IF*
          - $j_{alt} := j_{r_k}$, $j_{r_k} := j_{r'_k}$, $r_k := r_k + 1$
        - *END IF*
      - *END WHILE*
    - *END FOR*
    - *IF* $r_1 > e$ *AND* $r_2 > e$ *THEN* $m := m \cdot \ell^e$
    - *ELSE* $m := m \cdot \ell^{min(r_1, r_2)}$
    - *END IF*
  - *END IF*
- *END FOR*
- *RETURN* $\frac{c}{m}$

In KASH3 erzeugen wir die resultierende Ordnung $\mathcal{O}$, indem wir zunächst mithilfe von Algorithmus 5.5 den Führer c von $\mathcal{O}$ berechnen. Ist $\mathcal{O}_F$ die Maximalordnung mit Basis $(1, \omega)$, dann setzen wir $\mathcal{O}$ auf die Gleichungsordnung des Minimalpolynoms von $c\omega$. Somit erhalten isogene elliptische Kurven, deren Endomorphismenring denselben Führer hat, tatsächlich dieselbe Ordnung als Endomorphismenring.

[1] In KASH3 wird die Faktorisierung einer ganzen Zahl als Liste wiedergegeben: Für $c = p_1^{e_1} \cdot \ldots \cdot p_r^{e^r}$ ist Factorization(c) $= [[[p_1][e_1]], \ldots, [[p_r][e_r]]]$. So werden wir das hier auch behandeln.

Kapitel 6

Berechnung von Isogenien

In diesem Kapitel stellen wir verschiedene Bausteine zur Isogenieberechnung vor, die wir dann später zu einem vollständigen Algorithmus zusammensetzen. Alle Kurven, die wir hier betrachten, sind ordinär.

6.1 Der Algorithmus von Vélu

Nach 2.13 gibt es zu jeder Untergruppe G einer elliptischen Kurve E eine separable Isogenie $\varphi : E \to E/G$. Wie sieht diese aus?
Jacques Vélu konstruiert in [Vél71] aus einer elliptischen Kurve E/K und einer Untergruppe $G \subseteq E$ eine Isogenie $\varphi : E \to E'$ mit $\ker(\varphi) = G$. Dabei ist E' eine sich aus der Berechnung von φ ergebende zu E isogene Kurve, welche auch mit E/G bezeichnet wird. Die Konstruktion von φ funktioniert folgendermassen:
Wir setzen für $P \in E$

$$\varphi(P) := \begin{cases} O & \text{falls } P = O \\ (\varphi_x(P), \varphi_y(P)) & \text{sonst} \end{cases}$$

mit

$$\varphi_x(P) = X(P) + \sum_{Q \in G \setminus \{O\}} (X(P+Q) - X(Q))$$

und

$$\varphi_y(P) = Y(P) + \sum_{Q \in G \setminus \{O\}} (Y(P+Q) - Y(Q))$$

Dann wissen wir noch nicht, wie E' aussieht, aber $\ker(\varphi) = G$ ist erfüllt.
Um dies zu zeigen, erweitern wir die Koordinatenfunktionen $X, Y : E \to \overline{K}$ symbolisch auf $X, Y : E \to \overline{K} \cup \{\infty\}$, so dass $X(O) = Y(O) = \infty$ definiert sind.
Dann gilt zunächst: $P \in G \Rightarrow \varphi_x(P) = X(\mathcal{O})$, denn für $P \neq \mathcal{O}$ ist

(*i*) $-P \in G \Rightarrow \varphi_x(P) = a + X(\mathcal{O}),\ a \in \overline{K}$ noch zu bestimmen

(*ii*) $P \in G \Rightarrow X(P)$ vor der Summe kürzt sich weg

(*iii*) für $Q \in G \backslash \{O, -P\}$ gilt: $P + Q = Q' \in G \backslash \{O, P\}$. Andererseits wird bei jedem dieser Q' an anderer Stelle in der Summe die x-Koordinate wieder abgezogen.

Somit folgt insgesamt: $\varphi_x(P) = X(O) + 0$.
Die Argumentation für φ_y funktioniert analog, also:

$$P \in G \Rightarrow \varphi(P) = O \Rightarrow G \subseteq \ker(\varphi).$$

Ausserdem gilt: $P \in E \backslash G \Rightarrow \varphi(P) \neq O$, denn $P \notin G \Rightarrow -P \notin G$, also wird $\varphi_x(P)$ nicht zu $X(O)$ ausgewertet. Also $\ker(\varphi) = G$. Die Formeln für φ_x und φ_y kann man mithilfe der Additionsformeln für elliptische Kurven in rationale Funktionen $\varphi_x, \varphi_y \in \overline{K}(E)$ umwandeln.
Die Gleichung der Zielkurve ergibt sich dann aus der Betrachtung der Beziehung zwischen φ_x und φ_y (siehe [Vél71] für eine ausführliche Berechnung).
Da φ eine separable Isogenie ist (siehe [BSME06], Abschnitt 4.1), gilt
$\deg(\varphi) = \#\ker(\varphi)$ und somit $\deg(\varphi) = \#G$.
Für den nächsten Satz benötigen wir noch zwei weitere Definitionen:

6.1 Definition. Sei K'/K eine Körpererweiterung. Die Galoisgruppe von K'/K bezeichnen wir mit $G_{K'/K}$.

6.2 Definition. Sei $E/\mathbb{F}_q$ eine elliptische Kurve und $G \subset E(\mathbb{F}_{q^r})$ eine Untergruppe von E. G heisst galois-invariant, wenn gilt:

$$P = (x_P, y_P) \in G \Rightarrow (\sigma(x_P), \sigma(y_P)) \in G \text{ für alle } P \in G, \sigma \in G_{\mathbb{F}_{q^r}/\mathbb{F}_q}.$$

6.3 Bemerkung. Für die Galois-Invarianz einer solchen Untergruppe genügt es zu zeigen, dass für alle $P = (x_P, y_P) \in G$ gilt: $(x_P^q, y_P^q) \in G$, da der Frobenius-Endomorphismus $x \mapsto x^q$ die Galois-Gruppe von $\mathbb{F}_{q^r}/\mathbb{F}_q$ erzeugt.

Dann können wir folgende strengere Version von Satz 2.13 angeben:

6.4 Satz. *([BSS99], Theorem III.11)*
Sei E/K eine elliptische Kurve, G eine endliche, galois-invariante Untergruppe von E. Dann gibt es eine elliptische Kurve E'/K und eine eindeutig bestimmte, separable, über K definierte Isogenie $\varphi : E \to E'$ mit $ker(\varphi) = G$.

Ist eine solche galois-invariante Untergruppe $G \subset E(\widetilde{K})$ gegeben, dann ist die aus den Vélu-Formeln entstehende Isogenie also über K definiert. Siehe zum Beweis zum Beispiel [Koh96], Abschnitt 2.4: Hier wird gezeigt, dass eine durch die Vélu-Formeln erhaltene Isogenie von ungeradem Grad von der Form $\left(\frac{f(x)}{h(x)^2}, \frac{g(x,y)}{h(x)^3}\right)$ ist, wobei $f(x)$ und $g(x,y)$ Polynome sind, die von $h(x)$ bzw. den Koeffizienten von $h(x)$ und den Koeffizienten der Kurve abhängen. Da aber $h(x)$ als Nullstellen gerade die x-Koordinaten der galoisinvarianten Untergruppe hat, gilt
$h(x)^\sigma = h(x)$ für alle $\sigma \in G_{\widetilde{K}/K}$. Hierbei ist

$$(x^n + a_{n-1}x^{n-1} + ... + a_0)^\sigma = x^n + \sigma(a_{n-1})x^{n-1} + ... + \sigma(a_0),$$

σ wird also koeffizientenweise angewendet. Daher gilt $h(x) \in K(x)$ und somit ist die ganze Isogenie über K definiert.
Wir halten noch folgende Aussage über die Grade der in der Vélu-Isogenie vorkommenden Polynome fest:

6.5 Proposition. *Die aus einer galois-invarianten Untergruppe G von E berechnete separable Isogenie $\varphi : E \to E/G$ vom Grad $\ell > 2$ hat folgende Form:*

$$\varphi(x,y) = \left(\frac{f(x)}{h(x)^2}, \frac{g(x,y)}{h(x)^3}\right),$$

wobei $f(x)$ vom Grad ℓ ist, $h(x)$ vom Grad $\frac{\ell-1}{2}$ und $g(x,y)$ ein Polynom vom Grad 1 in y ist.

Beweis. siehe [LM98], Proposition 4.1. □

6.6 Korollar. *Mit den Bezeichnungen in Proposition 6.5 gilt, falls die Charakteristik des Grundkörpers > 3: $g(x,y) = g_1(x)y$.*

Beweis. Wir wissen aus Proposition 6.5, dass $g(x,y)$ ein Polynom vom Grad 1 in y ist, es bleiben also nur die beiden Möglichkeiten $g(x,y) = g_1(x)y + g_2(x)$ oder $g(x,y) = g_1(x)y$. Haben wir zwei Punkte $P, Q \in E$ mit $P = -Q$, welche nicht im Kern von φ liegen, dann gilt wegen $\varphi(P) = -\varphi(Q)$ auch $X(\varphi(P)) = X(\varphi(Q))$ und daher $Y(\varphi(P))^2 = Y(\varphi(Q))^2 = X(\varphi(P))^3 + aX(\varphi(P)) + b$ für die Koeffizienten a, b der Gleichung der Zielkurve. Also muss $g(X(P),Y(P))^2 = g(X(Q),Y(Q))^2$ gelten. Ist nun $g(x,y) = g_1(x)y + g_2(x)$, dann ist

$$g(x,y)^2 = g_1(x)^2y^2 + g_2(x)^2 + 2g_1(x)yg_2(x)$$

Dann ist $g(X(P),Y(P))^2 \neq g(X(Q),Y(Q))^2$. Also folgt $g(x,y) = g_1(x)y$. □

Also ergibt sich insgesamt, dass

$$\varphi(x,y) = \left(\frac{f(x)}{h(x)^2}, \frac{g_1(x)y}{h(x)^3}\right). \tag{6.7}$$

6.2 Zur Berechnung der dualen Isogenie

Nun können wir den Algorithmus zur Berechnung der dualen Abbildung einer separablen Isogenie vorstellen, jedoch geben wir vorher einige Anmerkungen zur Erläuterung des Algorithmus.
Zunächst gilt:

6.8 Lemma. *Sei $\varphi : E/\mathbb{F}_q \to E'/\mathbb{F}_q$ eine separable Isogenie vom Grad m mit $ggT(m,q) = 1$. Dann ist auch $\widehat{\varphi}$ separabel.*

Beweis. Es gilt $\#E[m] = m^2$ und $\#\ker(\varphi) = m$, daher ist $\#\ker(\widehat{\varphi}) = m$. Dann folgt wegen $\deg(\widehat{\varphi})$ und $\#\widehat{\varphi}^{-1}(O) = \deg_s(\widehat{\varphi})$ (siehe [Sil86], Theorem 4.10 (a)), dass $\widehat{\varphi}$ separabel ist. □

Sei nun $\varphi : E_1 \to E_2$ eine über K definierte separable Isogenie vom Grad m, deren duale Isogenie $\widehat{\varphi}$ wir berechnen wollen. Laut Definition ist $\widehat{\varphi} \circ \varphi = [m]$. Aber $[m]$ können wir mithilfe der Rekusionsformeln in Definition 2.1 berechnen. Sei $[m] = (m_x, m_y)$ und $\varphi = (\frac{\varphi_{x_1}}{\varphi_{x_2}}, \frac{\varphi_{y_1}}{\varphi_{y_2}})$. Die duale Isogenie hat folgende Gestalt: $\widehat{\varphi} = (\frac{\widehat{\varphi}_{x_1}}{\widehat{\varphi}_{x_2}}, \frac{\widehat{\varphi}_{y_1}}{\widehat{\varphi}_{y_2}})$. Wenn wir nun $\widehat{\varphi}_{x_2}$ ermitteln können, dann können wir mithilfe des Vélu-Algorithmus $\widehat{\varphi}$ berechnen: Sei $P \in E_2$ mit $\widehat{\varphi_{x_2}}(X(P)) = 0$ und $G := \langle P \rangle$. Berechnen wir nun wie in Abschnitt 6.1 beschrieben $\widetilde{\varphi} : E_2 \to E_2/G$, dann ist entweder $\widetilde{\varphi} = \widehat{\varphi}$ oder $-\widetilde{\varphi} = \widehat{\varphi}$. Es gibt nur diese zwei Möglichkeiten, da Kern und Zielkurve der Abbildung schon feststehen, wir müssen also nur noch testen, welche von beiden Möglichkeiten zutrifft. Dafür bilden wir $f := \widetilde{\varphi} \circ \varphi$ und testen für einen zufälligen Punkt $Q \in E \backslash E[2]$, ob $f(P) = mP$. Trifft das zu, dann gilt $\widehat{\varphi} = \widetilde{\varphi}$, sonst ist $\widehat{\varphi} = -\widetilde{\varphi}$. Es reicht auch aus, einen Punkt Q zu testen, denn entweder ist ja $f(Q) = mQ$ oder $f(Q) = -mQ$. Aber $mQ = -mQ$ gilt nur dann, falls $Q \in E[2]$.
Wie berechnen wir nun $\widehat{\varphi}_{x_2}$? Wir wissen, dass

$$\widehat{\varphi}_x = \frac{a_m x^m + a_{m-1}x^{m-1} + ... + a_0}{b_{m-1}x^{m-1} + b_{m-2}x^{m-2} + ... + b_0}, a_i, b_i \in K$$

und $\widehat{\varphi}_x(\varphi_x) = m_x$, dass also

$$a_m\varphi_x^m + a_{m-1}\varphi_x^{m-1} + ... + a_0 = m_x(b_{m-1}\varphi_x^{m-1} + b_{m-2}\varphi_x^{m-2} + ... + b_0) \qquad (6.9)$$

gelten muss. Diese Gleichung hat (wegen Existenz und Eindeutigkeit der dualen Isogenie) eine bis auf Vielfache eindeutige Lösung, welche wir mithilfe der KASH3-Funktion Relations finden. Somit haben wir $\hat{\varphi}_{x_2}$ berechnet.

6.10 Algorithmus. ***Berechnung der dualen Isogenie***
*-**Input**: $\varphi : E_1 \to E_2$ über $\mathbb{F}_q$ definierte seperable Isogenie vom Grad m mit $ggT(m,q) = 1$*
*-**Output**: die zu φ duale Isogenie $\widehat{\varphi}$ mit $\widehat{\varphi} \circ \varphi = [m]$*

- $[m]$:= *Multiplikation-mit-m-Abbildung auf* E_1, $[m] = (m_x, m_y)$
- φ *hat die Gestalt* $(\frac{\varphi_{x_1}}{\varphi_{x_2}}, \frac{\varphi_{y_1}}{\varphi_{y_2}})$
- *Finde eine Lösung* $(a_m, ..., a_0, b_{m-1}, ..., b_0) \in \mathbb{F}_q^{2m+1}$ *der Gleichung 6.9*
- $\overline{\mathbb{F}_q} \ni r :=$ *eine Nullstelle von* $b_m x^m + ... + b_0$
- $E_2 \ni P := (r, y_P)$ *ein Punkt mit x-Koordinate r*
- $\widetilde{\varphi} : E_2 \to E_2/\langle P \rangle$ *die mit Vélu berechnete Isogenie*
- *IF* $E_2/\langle P \rangle = E_1$ [1] *THEN* $\psi := \widetilde{\varphi}$
- *ELSE Berechne Isomorphismus* $f : E_2/\langle P \rangle \to E_1$, $\psi := f \circ \widetilde{\varphi}$
- *END IF*
- $Q \in E(K) \backslash E[2]$ *zufälliger Punkt*
- *IF* $\psi \circ \varphi(Q) = mQ$ *THEN RETURN* ψ
- *ELSE RETURN* $-\psi$
- *END IF*

6.3 Isogenien im SEA-Algorithmus

Im SEA-Algorithmus zur Berechnung der Anzahl der Punkte einer elliptischen Kurve über einem endlichen Körper spielen Isogenien primen Grades bzw. deren Kern eine wichtige Rolle. Der SEA-Algorithmus berechnet zu $E/\mathbb{F}_q$ die Spur t des Frobenius-Endomorphismus von E. Dann ist $\#E(\mathbb{F}_q) = q+1-t$. Wir haben aber in den von uns betrachteten Fällen $\#E(\mathbb{F}_q)$ und somit t immer schon gegeben.

Zunächst benötigen wir folgende

6.11 Definition. Sei $E/\mathbb{F}_{p^r}$ eine elliptische Kurve. Eine Primzahl $\ell \in \mathbb{N} \backslash \{p\}$ heisst *Elkies-Primzahl* von E, wenn $f_\pi(x) \equiv (x-\lambda)(x-\mu) \bmod \ell$ mit $\lambda, \mu \in \mathbb{Z}$.

6.12 Bemerkung. (Elkies-Primzahlen und Eigenräume des Frobenius-Endomorphismus)
Sei ℓ eine Elkies-Primzahl von $E/\mathbb{F}_q$, also

$$x^2 - tx + q \equiv (x-\lambda)(x-\mu) \bmod \ell.$$

Wenn wir $E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ als zweidimensionalen $\mathbb{Z}/\ell\mathbb{Z}$-Vektorraum mit Basis (P_1, P_2) betrachten, so dass alle $R \in E[\ell]$ eindeutig darstellbar sind als

[1] Die Kurve $E_2/\langle P \rangle$ ist nur bis auf Isomorphie eindeutig bestimmt

$R = a_1P_1 + a_2P_2,\ a_i \in \mathbb{Z}/\ell\mathbb{Z}$, dann gilt zunächst ganz allgemein, dass alle Endomorphismen $\varphi : E \to E$ eingeschränkt auf $E[\ell]$ als 2×2-Matrix darstellbar sind. Aus der Linearen Algebra wissen wir: Wenn das charakteristische Polynom von $\varphi \mod \ell$ zerfällt, dann gibt es eine Basis von $E[\ell]$ aus Eigenvektoren von φ. Konkret in unserem Fall der Elkies-Primzahlen gilt: Es gibt $P, Q \in E[\ell]$ mit $\pi(P) = \lambda P, \pi(Q) = \mu Q$ und $E[\ell] = \langle P \rangle \times \langle Q \rangle$. Andererseits bedeutet $\pi(P) = \lambda P \in \langle P \rangle$, dass die von P erzeugte Untergruppe $C \subseteq E[\ell]$ galois-invariant ist, es gibt also eine über $\mathbb{F}_q$ definierte Isogenie $\varphi : E \to E/C$.

Wir könnten diese Eigenräume theoretisch durch Berechnung der kompletten ℓ-Torsion und Testen der Nullstellen der charakteristischen Gleichung bestimmen. Allerdings ist $\#E[\ell] = \ell^2$, so dass uns diese Herangehensweise komplexitäts- und speichertechnisch vor ein Problem stellt. Es geht auch schneller:
Basierend auf folgendem Satz wird in [Sch95] ein Algorithmus zur Bestimmung dieser Eigenräume entwickelt, welchen wir im nächsten Abschnitt vorstellen.

6.13 Satz. *([Sch95],Proposition 6.1)*
Sei $E/\mathbb{F}_q$ eine ordinäre elliptische Kurve mit j-Invariante $j \neq 0, 1728$. Dann gilt: Das ℓ-te Modulpolynom $\Psi_\ell(j, x)$ hat eine Nullstelle $\tilde{j} \in \mathbb{F}_q \Leftrightarrow$ Der Kern C der korrespondierenden Isogenie $\psi : E \to E'$ (mit $j(E') = \tilde{j}$) ist ein 1-dimensionaler Eigenraum des Frobenius-Endomorphismus π.

Die Eigenräume von π in $E[\ell]$ korrespondieren also zu den Nullstellen des Modulpolynoms $\Psi_\ell(j, x)$. Aus einer solchen Nullstelle $\tilde{j}$ und den Koeffizienten von E wird nun in [Sch95] (siehe auch [BSS99], VII.4 für ungerade Charakteristik, VII.5 für Charakteristik 2) ein Faktor $F(x) \in \mathbb{F}_q[x]$ des Divisionspolynoms $\overline{f_\ell}$ berechnet, sodass die Nullstellen von $F(x)$ gerade die x-Koordinaten der Punkte eines der beiden Eigenräume des Frobenius-Endomorphismus sind. Diesen Algorithmus stellen wir im nächsten Abschnitt vor.

6.14 Bemerkung. Es gilt natürlich immer: ℓ Elkies-Primzahl von $E/\mathbb{F}_q \Rightarrow \ell$ Elkies-Primzahl aller zu E $\mathbb{F}_q$-isogener Kurven.

6.4 Berechnung der Isogenie

Alle Berechnungen werden theoretisch für elliptische Kurven über $\mathbb{C}$ bzw. über Zahlkörpern durchgeführt, welche mithilfe des Deuring-Lift aus unserer ursprünglichen Kurve entstanden sind und reduziert wieder diese ergeben. Die Berechnungen bleiben jedoch richtig, wenn man sie alle sofort in dem endlichen Körper ausführt.

Ziel des Algorithmus ist es, zu einer elliptischen Kurve $E/\mathbb{F}_q$ und einer Elkies-Primzahl $\ell > 2$ eine $\mathbb{F}_q$-Isogenie $\varphi : E \to E'$ vom Grad ℓ zu berechnen. Hierzu wird eine Nullstelle j' von $\Psi_\ell(j(E), x)$ ermittelt. Mithilfe dieser Daten erhält man dann ein Polynom $F_\ell(x)$ vom Grad $\frac{(\ell-1)}{2}$, welches das Divisionspolynom $\overline{f_\ell}(x)$ teilt, wobei die Nullstellen von $F_\ell(x)$ die x-Koordinaten einer galois-invarianten Untergruppe von $E(\overline{\mathbb{F}_q})$ sind. Dann kann man mithilfe der Vélu-Formeln (siehe 6.1) bzw. in grosser Charakteristik mithilfe eines schnelleren Algorithmus, der auch in MAGMA zur Isogenieberechnung verwendet wird und den wir im nächsten Unterabschnitt ansprechen, die Isogenie berechnen, welche dann zu einer Kurve führt, deren j-Invariante j' ist. Allerdings unterscheidet sich die Berechnung von $F_\ell(x)$ im Fall von Charakteristik 2 erheblich von der für grosse Charakteristik, weshalb wir sie hier getrennt behandeln.
Auf den Fall $\ell = 2$ gehen wir danach ein.

6.4.1 Grosse Charakteristik

Wir geben hier nur den Algorithmus an, wobei wir ihn [BSS99], VII.4, entnommen haben. Wir bezeichnen für ein Polynom $f \in K[x, y]$ die partiellen Ableitungen von f nach x bzw. y mit f_x bzw. f_y. Desweiteren werden wir in dem Algorithmus einige Potenzreihen in x definieren. Ist $A(x)$ eine solche, dann meinen wir mit $[A(x)]_i$ den Koeffizienten vor x^i. Das Modulpolynom $\Psi_\ell(x, y)$ wird dabei immer als Element von $\mathbb{F}_q[x, y]$ verstanden.

6.15 Algorithmus. ***Berechnung eines Faktors des Divisionspolynoms***
Input*: $E/\mathbb{F}_q : y^2 = x^3 + ax + b$ mit $j(E) \notin \{0, 1728\}$, ℓ Elkies-Primzahl von E*
Output*: Faktor $F_\ell(x) \mid \overline{f_\ell}(x)$ oder ERROR*

- $j := j(E),\ \tilde{j} :=$ *Nullstelle von* $\Psi_\ell(j, x),\ d := \frac{\ell-1}{2}$
- *IF* $(d-2)(2d+3) \geq char(\mathbb{F}_q)$ *THEN RETURN ERROR*
- *IF* $\tilde{j} \in \{0, 1728\}$ *OR* $\Psi_y(j, \tilde{j}) = 0$ *THEN*
  wähle andere Nullstelle von $\Psi_\ell(j, x)$
  falls nicht möglich: RETURN ERROR
- *END IF*
- $j' := -j \cdot \dfrac{\overline{E_6}}{\overline{E_4}},\ \tilde{j}' := -\dfrac{j'\Psi_x(j,\tilde{j})}{\ell\Psi_y(j,\tilde{j})}$ $(*)$
- $\widetilde{a} := -\dfrac{1}{48}\dfrac{\tilde{j}'^2}{\tilde{j}(\tilde{j}-1728)},\ \widetilde{b} := -\dfrac{1}{864}\dfrac{\tilde{j}'^3}{\tilde{j}^2(\tilde{j}-1728)}$ $(**)$
- $\overline{E4} := -48 \cdot a,\ \overline{E6} := 864 \cdot b,\ \overline{E_4}' := -\widetilde{a} \cdot 48,\ \overline{E_6}' := \widetilde{b} \cdot 864$
- $jj := -\dfrac{j'^2\Psi_{xx}(j,\tilde{j}) + 2\ell j'\tilde{j}'\Psi_{xy}(j,\tilde{j}) + \ell^2\tilde{j}'^2\Psi_{yy}(j,\tilde{j})}{j'\Psi_x(j,\tilde{j})}$
- $p_1 := \dfrac{\ell}{2} \cdot jj + \dfrac{\ell}{4}\left(\dfrac{\overline{E_4}^2}{\overline{E}_6} - \ell\dfrac{\overline{E_4}'^2}{\overline{E_6}'}\right) + \dfrac{\ell}{3}\left(\dfrac{\overline{E_6}}{\overline{E}_4} - \ell\dfrac{\overline{E_6}'}{\overline{E_4}'}\right)$
- $c_1 := -\dfrac{a}{5},\ c_2 := -\dfrac{b}{7},\ \tilde{c}_1 := -\dfrac{\ell^4\tilde{a}}{5},\ \tilde{c}_2 := -\dfrac{\ell^6\tilde{b}}{7}$
- *FOR* $k = 3 \ldots d$ *DO* $(***)$

$$c_k := \frac{3}{(k-2)(2k+3)} \sum_{j=1}^{k-2} c_j c_{k-1-j}$$

$$\tilde{c}_k := \frac{3}{(k-2)(2k+3)} \sum_{j=1}^{k-2} \tilde{c}_j \tilde{c}_{k-1-j}$$

- *END FOR*
- $F_{\ell,d} := 1,\ F_{\ell,d-1} := -\dfrac{p_1}{2}$
- $A(x) := exp\left(-\dfrac{1}{2}p_1 x - \displaystyle\sum_{k=1}^{\infty} \frac{\tilde{c}_k - \ell c_k}{(2k+1)(2k+2)} x^{k+1}\right)$
- $C(x) := \displaystyle\sum_{k=1}^{\infty} c_k x^k$
- *FOR* $i = 2 \ldots d$ *DO*

$$F_{\ell,d-i} := [A(x)]_i - \sum_{k=1}^{i} \left(\sum_{j=0}^{k} \binom{d-i+k}{k-j} [C(x)^{k-j}]_j \right) F_{\ell,d-i+k}$$

- *END FOR*
- *RETURN* $F_\ell(x) := \displaystyle\sum_{k=0}^{d} F_{\ell,k} x^k$

In 6.15 kann man ein paar Fälle erkennen, für die der Algorithmus nicht funktioniert:
Wenn $\Psi_y(j,\tilde{j}) = 0$, dann kann man die Ausdrücke in $(*)$ nicht zu berechnen (siehe [Sch95], am Ende von 7. gibt es eine kurze Erläuterung zu diesen Fällen). Wenn $\tilde{j} \in \{0, 1728\}$, so schlägt die Berechnung bei $(**)$ fehl. An den Formeln bei $(***)$ sieht man, dass $\mathrm{char}(\mathbb{F}_q) > \frac{l^2-3\ell-10}{2}$ gelten muss.
Obiger Algorithmus funktioniert nur, falls $\ell > 2$. Nun gehen wir auf die schon angesprochene Beschleunigung der Isogenieberechnung ein, für die man die Untergruppe im Kern nicht berechnen braucht:
Betrachten wir die obige Situation für elliptische Kurven über $\mathbb{C}$, so ergibt sich folgendes:
Seien $E/\mathbb{C}, F/\mathbb{C}$ zwei isogene elliptische Kurven. Ist ψ eine Funktion, deren Nullstellen die x-Koordinaten der Punkte im Kern der separablen Isogenie $\varphi : E \to F$ sind, so können wir mithilfe der Weierstrass-Funktionen $\wp_E$ und $\wp_F$ der zu den Kurven assoziierten Gitter die komplette Isogenie berechnen: Wir wissen wegen Gleichung 6.7, dass

$$\varphi(x,y) = \left(\frac{\alpha(x)}{\psi(x)^2}, \frac{\omega(x)y}{\psi(x)^3}\right).$$

Es muss also gelten

$$\begin{aligned} \alpha(\wp_E) &= \psi(\wp_E)^2\wp_F \text{ und} \\ \omega(\wp_E) &= \frac{\psi(\wp_E)^3\wp'_F}{\wp'_E}, \end{aligned}$$

denn $\wp_E$ und $\wp'_E$ bzw. $\wp_F$ und $\wp'_F$ parametrisieren die Kurve, d.h. für alle Punkte $P \in E(\mathbb{C})$ gilt $X(P) = \wp_E(z)$ für ein $z \in \mathbb{C} \Rightarrow Y(P) = \wp'_E(z)$, genauso für die Kurve F. In Magma gibt es eine Funktion, welche zu zwei gegebenen Potenzreihen r_1 und r_2 ein Polynom f berechnet, so dass $f(r_1) = r_2$, diese haben wir in KASH übertragen und hierfür verwendet. Die Weierstrass-Funktion $\wp_E$ ergibt sich für eine Kurve E der Form $y^2 = x^3 + ax + b$ rekursiv aus a und b (siehe [Mül95], Lemma 6.2):

$$\wp_E(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} c_k x^{2k} \quad \text{mit}$$

$$c_1 = -\frac{a}{5}, c_2 = -\frac{b}{7},\ c_k = \frac{k}{(k-2)(2k+3)} \sum_{h=1}^{k-2} c_h c_{k-1-h} \text{ für } k \geq 3$$

Da die Grade von α und ω bekannt sind, genügt es, endlich viele Koeffizienten der Potenzreihen zu berechnen.
Sind $a, b \in \mathbb{Z}$ und ist für ein $p \in \mathbb{P}$ die Reduktion modulo p sinnvoll, d.h. ist

$\overline{E} : y^2 = x^3 + \overline{a}x + \overline{b},\ \overline{a} \equiv a \mod p,\ \overline{b} \equiv b \mod p$ eine ordinäre elliptische Kurve, dann kann man die Koeffizienten der Weierstrass-Funktion als Elemente von $\mathbb{F}_p$ betrachten. Es gilt weiterhin für alle $P \in \overline{E} : X(P) = \wp_E(z)$ für ein $z \in \mathbb{F}_p \Rightarrow Y(P) = \wp'(z)$. Die obigen Überlegungen sind also auch für diesen Fall anwendbar. Sind die Kurven, zwischen denen wir eine solche Isogenie berechnen wollen, über $\mathbb{F}_{p^r}$ definiert, so wird die Argumentation schwieriger, denn dann muss man wieder elliptische Kurven über Zahlkörpern (bzw. lokalen Ringen) betrachten, das Ergebnis ist aber dasselbe.
Die Berechnung der Isogenie aus ψ geht dann deutlich schneller als die Berechnung über eine Untergruppe mit Nullstellen von ψ als x-Koordinaten. Man muss zum Beispiel ψ hierfür nicht faktorisieren und spart sich die Berechnung der Punktgruppe C im Kern von φ, denn da C zwar galois-invariant, aber nicht $\mathbb{F}_q$-rational sein muss, kann es vorkommen, dass ψ über einem Erweiterungskörper von $\mathbb{F}_q$ vom Grad $\frac{\ell-1}{2}$ zerfällt und die Punkte in C über einem Erweiterungskörper von $\mathbb{F}_q$ vom Grad $\ell - 1$ definiert sind.

6.4.2 Charakteristik 2

Hier folgen wir [Ler96] und [Ver99], 4.4.2. Hierbei wird die eigentliche Isogenie nicht über den Vélu-Algorithmus bestimmt, sondern lässt sich direkt berechnen. Mit E_a bezeichnen wir hier eine über $\mathbb{F}_{2^n}$ definierte Kurve $y^2 + xy = x^3 + a$. Da in Charakteristik 2 gilt: E supersingulär $\Leftrightarrow j(E) = 0$ (vgl. [BSS99], p.45), sind alle hier betrachteten Kurven ordinär.
Der Algorithmus basiert auf folgenden Sätzen aus [Ler96]:

6.16 Satz. *([Ler96], Theorem 4)*
Seien E_a und E_b zwei elliptische Kurven, die über $\mathbb{F}_{2^n}$ definiert sind, sei ℓ eine ungerade Zahl und $d = \frac{\ell-1}{2}$. Sei φ eine Isogenie vom Grad ℓ zwischen E_a und E_b, welche durch

$$(x, y) \mapsto \left(\frac{g(x)}{q^2(x)}, \frac{h(x) + yk(x)}{q^3(x)} \right)$$

gegeben ist, wobei $q(x), g(x), h(x), k(x) \in \mathbb{F}_{2^n}[x]$ mit Graden jeweils $\leq d, \ell, 3d$ und $2d$. Dann gilt:

- *$g(x) = xp^2(x)$, wobei $p(x)$ ein Polynom vom Grad d ist, so dass $ggT(p(x), q(x)) = 1$ und*

$$x^d q(\frac{\sqrt{a}}{x}) = \frac{\sqrt[8]{a}}{\sqrt[8]{b}}(\sqrt[4]{a})^d p(x) \overset{(x \mapsto \frac{x}{\sqrt{a}})}{\Longrightarrow} x^d p(\frac{\sqrt{a}}{x}) = \frac{\sqrt[8]{b}}{\sqrt[8]{a}}(\sqrt[4]{a})^d q(x) \qquad (6.17)$$

- *$k(x) = p^2(x)q(x)$*

- $h(x) = xr(x)p(x) + \sqrt{b}q^3(x) + \sqrt{a}p^2(x)q(x)$ *mit*
  $r(x) = x((pq)'(x))$ *oder* $r(x) = (xpq)'(x)$

Hier sieht man, dass alle in der Isogenie vorkommenden Polynome aus den zwei Polynomen $q(x)$ und $p(x)$ und den Koeffizienten der Kurven berechnet werden können. Diese müssen auch noch eine bestimmte Beziehung erfüllen (siehe Gleichung 6.17). Daraus wird dann gefolgert:

6.18 Korollar. *([Ler96], Corollary 5) Es müssen folgende Beziehungen zwischen $p(x)$ und $q(x)$ gelten:*

$$x^d \hat{q}(x + \frac{\sqrt{a}}{x}) = q(x)p(x)$$
$$\text{und } (x + \sqrt[4]{a})x^d \hat{p}(x + \frac{\sqrt{a}}{x}) = xp^2(x) + \sqrt[4]{b}q^2(x),$$

wobei $\hat{p}(x) = \sqrt{p(x^2)}$ *und* $\hat{q}(x) = \sqrt{q(x^2)}$

Desweitern gilt noch

6.19 Korollar. *([Ler96], Corollary 6)*
Seien $p(x) = \sum_{i=0}^{d} p_i^2 x^i, q(x) = x^d + \sum_{i=0}^{d-1} q_i^2 x^i, \alpha = \sqrt[4]{a}$ *und* $\beta = \sqrt[4]{b}$. *Dann gilt*

$$q_i = \frac{\sqrt[4]{\alpha}}{\sqrt[4]{\beta}} \sqrt{\alpha}^{d-2i} p_{d-i} \tag{6.20}$$

und

$$\begin{aligned} p_0 &= \sqrt[4]{\alpha^{2d} + \alpha^{2d-1} p_{d-1}},\ p_d = 1,\ p_{d-1} = \alpha + \beta, \\ p_{d-2} &= \begin{cases} p_{d-1}^4 + \alpha p_{d-1} + \alpha^2 & \text{für } d \text{ ungerade} \\ p_{d-1}^4 + \alpha p_{d-1} & \text{für } d \text{ gerade} \end{cases} \end{aligned}$$

Aus Korollar 6.18 leitet Lercier dann (siehe [Ler96], 4.1) folgende Gleichungen ab:

$$\begin{aligned} \forall k = 0, \ldots, \left\lfloor \frac{d-1}{2} \right\rfloor : p_k^4 &= \alpha^{2d-4k-1} \sum_{i=0}^{k} p_{d-2k-1+2i} \epsilon_{d-2k-1+2i,i} \alpha^{2i} \\ &+ \alpha^{2d-4k} \sum_{i=0}^{k} p_{d-2k+2i} \epsilon_{d-2k+2i,i} \alpha^{2i}, \end{aligned} \tag{6.21}$$

$$\begin{aligned} \forall k = 1, \ldots, \left\lfloor \frac{d}{2} \right\rfloor : p_{d-k}^4 &= \alpha \sum_{i=0}^{k-1} p_{d+1-2k+2i} \epsilon_{d+1-2k+2i,i} \alpha^{2i} \\ &+ \sum_{i=0}^{k} p_{d-2k+2i} \epsilon_{d-2k+2i,i} \alpha^{2i} \end{aligned} \tag{6.22}$$

wobei $\epsilon_{i,j} := \frac{i!}{j!(i-j)!} \mod 2$ für alle $0 \leq i \leq j \in \mathbb{Z}$. Dies ergibt ein nichtlineares Gleichungssystem mit d Gleichungen für $d-4$ Unbekannte. Wie kann man es geschickt lösen? Zunächst kann man es in ein lineares Gleichungssystem umwandeln: Sei ω ein erzeugendes Element von $\mathbb{F}_{2^n}^*$. Dann ist jedes p_i als
$p_i = p_{i,0} + p_{i,1}\omega + p_{i,2}\omega^2 + ... + p_{i,n-1}\omega^{n-1}$ darstellbar. Wenn wir diese Darstellung in obigem Gleichungssystem benutzen, dann wird es linear, denn

$$\begin{aligned} p_i^4 &= (p_{i,0} + p_{i,1}\omega + p_{i,2}\omega^2 + ... + p_{i,n-1}\omega^{n-1})^4 \\ &\overset{\forall a,b\in\mathbb{F}_2:\ (a+b)^{2^n}=a^{2^n}+b^{2^n}}{=} p_{i,0}^4 + p_{i,1}^4\omega^4 + p_{i,2}^4(\omega^2)^4 + ... + p_{i,n-1}^4(\omega^{n-1})^4 \\ &\overset{\forall a\in\mathbb{F}_2:\ a^2=a}{=} p_{i,0} + p_{i,1}\omega^4 + p_{i,2}(\omega^2)^4 + ... + p_{i,n-1}(\omega^{n-1})^4 \end{aligned}$$

Dies ergibt dann also ein lineares Gleichungssystem mit nd Gleichungen (jede Gleichung wird zusätzlich nach ω-Potenz aufgesplittet) und $n(d-4)$ Unbekannten. Das wird natürlich schnell sehr gross, deshalb gibt es noch einige Verbesserungen: Es gilt (siehe [Ler96],4.2)

$$\forall k = 0, \ldots, d : \sqrt[4]{\alpha} \sum_{i=0}^{k} p_i^2 p_{d-k+i}^2 \alpha^{2i} = \sqrt[4]{\beta}\sqrt{\alpha}^{d+2k} \sum_{i=0}^{\lfloor \frac{k}{2} \rfloor} p_{k-2i}\epsilon_{d-k+2i,i} \qquad (6.23)$$

Somit ist jedes p_i die Lösung einer quadratischen Gleichung
$p_i^2 + cp_i + d = 0$. Eine solche Gleichung hat aber nur dann eine Lösung, wenn $Tr(\frac{d}{c^2}) = 0$, dies ist also eine zusätzliche Bedingung, welche wir an die Koeffizienten stellen können. Dann hat sie aber auch zwei Lösungen, denn ist x_0 eine solche, dann auch $x_0 + c$, die Lösungen haben daher die Form $x_0 + \pi c$, wobei $\pi \in \mathbb{F}_2$. Bei der Berechnung der Koeffizienten p_i gehen wir nun folgendermassen vor: Zu Beginn sind p_0, p_{d-2}, p_{d-1} und p_d gegeben. Mithilfe von 6.23 erhalten wir p_1 als Lösung einer quadratischen Gleichung, die darin eingehenden Koeffizienten sind p_0, p_d und p_{d-1}. Dann hat p_1 die Form $p_1 = x_0 + \pi_0 a_0$, wobei wir $\pi_0 \in \mathbb{F}_2$ als binäre Variable betrachten. Wir erhalten dann mit $k = 1$ durch Einsetzen in die Gleichung 6.21 p_{d-3} als Funktion in π_0 und mit $k = 2$ durch Einsetzen in die Gleichung 6.22 p_{d-4}, ebenfalls als Funktion in π_0. Dann erhalten wir p_2 als Lösung von Gleichung 6.23 mithilfe von 2 binären Variablen π_0 und π_1, da p_2 auch von p_1 abhängt. Dann wieder Einsetzen in die Gleichungen 6.21 und 6.22, bis nach $K \leq \frac{d+1}{3}$ Schritten $p_0, ..., p_d$ als multivariate Polynome in höchstens $K-1$ binären Variablen gegeben sind. Wir erhalten aus den Gleichungen 6.21 und 6.22 dann noch K zusätzliche Gleichungen, welche wir verwenden, um die π_i zu bestimmen. Trivialerweise gilt für alle binären Variablen $\pi_i : \pi_i^n = \pi_i$.

6.24 Algorithmus. ***Berechnung eines Faktors des Divisionspolynoms***
Input:$E/\mathbb{F}_{2^n} : y^2 + xy = x^3 + a, \ell$ *Elkies-Primzahl*
Output: *Faktor* $F_\ell(x) \mid \overline{f_\ell}(x)$

- $j := j(E), \tilde{j} :=$ *Nullstelle von* $\Psi_\ell(j, x), b := \frac{1}{\tilde{j}}$
- $d := \frac{\ell-1}{2}, K := 1, \alpha := \sqrt[4]{a}, \beta := \sqrt[4]{b}$
- *WHILE* $K \leq d - 2K + 1$ *DO*
  - *(*)(gegeben sind hier schon* $p_0, ..., p_{K-1}, p_{d-2K}, ..., p_d$ *als Funktion in* $\pi_0, ..., \pi_{K-2}$*.)*
    Aus Gleichung 6.23 erhalten wir $p_K^2 + b_K p_K + c_K = 0$ *mit*

$$c_K = \left(\sum_{i=0}^{K-1} p_i^2 p_{d-K+i}^2 \alpha^{2i} + \sqrt[4]{\beta}\sqrt{\alpha}^{d+2K} \sum_{i=1}^{\lfloor \frac{K}{2} \rfloor} p_{K-2i} \epsilon_{d-K+2i,i} \right) / (\alpha^{2K} \sqrt[4]{\alpha})$$

    und $b_K = \sqrt[4]{\beta}\sqrt{\alpha}^{d+2K}/(\alpha^{2K}\sqrt[4]{\alpha})$.
    Sei $c_K/b_K^2 = \sum_{(\mu_0,...,\mu_{K-2}) \in \{0,1\}^{K-1}} C_\mu \pi_0^{\mu_0} \cdot ... \cdot \pi_{K-2}^{\mu_{K-2}}$ *(nach Produkten in den binären Variablen geordnet aufgeschrieben). Wir wissen, dass* $Tr(c_K/b_K) = 0$ *gelten muss und betrachten nun* $T := \sum_{(\mu_0,...,\mu_{K-2}) \in \{0,1\}^{K-1}, Tr(C_\mu)=1} \pi_0^{\mu_0} \cdot ... \cdot \pi_{K-2}^{\mu_{K-2}}$.
  - *IF* $T \neq 0$ *THEN*
    Stelle T *nach einem der vorkommenden* π_i *um, dieses kann dann in allen schon berechneten* p_i *eliminiert werden. Gehe wieder zu (*). (Bei der erneuten Berechnung von* c_K *und* b_K *gilt dann* $T = 0$*.)*
  - *ELSE*
    Setze $p_K = b_K \pi_{K-1} + b_K \sum_{(\mu_0,...,\mu_{K-2}) \in \{0,1\}^{K-1}} P_\mu \pi_0^{\mu_0} \cdot ... \cdot \pi_{K-2}^{\mu_{K-2}}$ *mit* $\pi_{K-1} \in \mathbb{F}_2$ *und* P_μ *Lösung von* $x^2 + x + C_\mu$, $K := K + 1$
  - *END IF*
- *IF* $K \leq d - 2K + 1$ *THEN*
  berechne p_{d-2K+1} *aus Gleichung 6.21 mit* $k = K$
  END IF
- *IF* $K \leq d - 2K$ *THEN*
  berechne p_{d-2K} *aus Gleichung 6.22 mit* $k = K - 1$
  END IF

END WHILE

- *die noch nicht verwendeten Gleichungen aus 6.21 und 6.22 berechnen, alle* p_i *(als multivariate Polynome in binären Variablen gegeben) einsetzen, Gleichungssystem lösen.*
- *aus Gleichung 6.20 alle* q_i *berechnen*
- *return* $q(x) = x^d + \sum_{i=0}^{d-1} q_i^2 x^i$

Mithilfe des durch den Algorithmus 6.24 ermittelten Faktors des Divisionspolynoms kann nun die konkrete Isogenie entweder durch den Vélu-Algorithmus oder mithilfe der Formeln in Satz 6.16 berechnet werden.

Der Algorithmus 6.24 ist, wie man bei der Inputforderung sieht, nur für elliptische Kurven in der dort angegebenen Form anwendbar. Allerdings sind zum Beispiel die Kurven aus dem ANSI-Standard von der Form

$$E/\mathbb{F}_{2^n} : y^2 + xy = x^3 + ax^2 + b, \tag{6.25}$$

und wegen $Tr(a) \neq 0$ auch nicht in diese Form zu bringen (siehe [Sil86]). Allerdings können wir dann mit einem quadratischen Twist E^t arbeiten, denn

6.26 Lemma. *Seien $\mathbb{F}_q$ ein endlicher Körper der Charakteristik 2, $E/\mathbb{F}_q : y^2 + xy = x^3 + a$ eine elliptische Kurve und $E^t/\mathbb{F}_q : y^2 + xy = x^3 + bx^2 + a$ ihr quadratischer Twist. Dann gilt für alle Primzahlen ℓ:*

(i) ℓ Elkies-Primzahl von $E \Leftrightarrow \ell$ Elkies-Primzahl von E^t

(ii) Ist $\langle P \rangle \subset E$ eine mit 6.24 ermittelte galois-invariante Untergruppe und $\psi : E \to E^t$ ein $\mathbb{F}_{q^2}$-Isomorphismus zwischen E und E^t, dann ist $\langle \psi(P) \rangle$ eine galois-invariante Untergruppe von E^t.

Beweis. (*i*) „⇒“ Es gilt folgende Beziehung zwischen der Grösse der Punktgruppen der beiden Kurven: $\#E(\mathbb{F}_q) + \#E^t(\mathbb{F}_q) = 2q + 2$. Sei t die Spur des Frobenius-Endomorphismus von E, dann ist $\#E(\mathbb{F}_q) = q + 1 - t$ und somit $\#E(\mathbb{F}_q) + \#E^t(\mathbb{F}_q) = 2q + 2 = q + 1 - t + q + 1 - t^t$, wobei t^t die Spur der getwisteten Kurve ist. Also muss $t = -t^t$ gelten. Sei ℓ eine Elkies-Primzahl von E, also

$$x^2 - t + q \equiv (x - \lambda)(x - \mu) \equiv x^2 - (\lambda + \mu)x + \lambda\mu \bmod \ell.$$

Also $t \equiv \lambda + \mu \mod \ell$, somit $-t \equiv -\lambda - \mu \mod \ell$ und daher ℓ auch Elkies-Primzahl von E^t.
„⇐“: analog

(*ii*) Seien $\pi_E : E \to E$ bzw. $\pi_{E^t} : E^t \to E^t$ die Frobenius-Endomorphismen von E bzw. E^t. Zunächst zeigen wir, dass $\psi(\pi_E(Q)) = -\pi_{E^t}(\psi(Q))$ für alle $Q \in E$ gilt: Es ist $\psi(x, y) = (x, y + sx)$, wobei $s \in \mathbb{F}_{q^2}$ eine Nullstelle von $x^2 + x + b$ ist (siehe Seite 20). Daher ist

$$\begin{aligned} \psi(\pi_E(x, y)) &= \psi(x^q, y^q) \\ &= (x^q, y^q + sx^q) \\ \text{und } \pi_{E^t}(\psi(x, y)) &= \pi(x, y + sx) \\ &= (x^q, y^q + s^q x^q) \end{aligned}$$

Da aber $s \notin \mathbb{F}_q$, denn sonst wären E und E^t schon $\mathbb{F}_q$-isomorph, ist $s^q \neq s$. Somit ist $X(\psi(\pi_E(Q))) = X(\pi_{E^t}(\psi(Q)))$, aber $Y(\psi(\pi_E(Q))) \neq Y(\pi_{E^t}(\psi(Q)))$. Also muss $\psi(\pi_E(Q)) = -\pi_{E^t}(\psi(Q))$ gelten.
Sei nun $\langle P \rangle \subset E$ eine mit 6.24 zur Elkies-Primzahl ℓ ermittelte galois-invariante Untergruppe. Es gilt dann für ein $\lambda \in \mathbb{Z}/\ell\mathbb{Z} : \lambda P = \pi_E(P)$. Wegen $-\psi(\pi_E(P)) = \pi_{E^t}(\psi(P))$ gilt:

$$\pi_{E^t}(\psi(P)) = -\psi(\pi_E(P)) = -\psi(\lambda P) = -\lambda\psi(P).$$

Daher erzeugt $\psi(P)$ eine galois-invariante Untergruppe zum Eigenwert $-\lambda$. □

Für elliptische Kurven der Form 6.25 berechnen wir also eine Isogenie wie folgt:

6.27 Algorithmus. ***Isogenieberechnung für Kurven der Form 6.25***
Input*: $E/\mathbb{F}_{2^n} : y^2 + xy = x^3 + ax^2 + b$ mit $Tr(a) = 1, \ell$ Elkies-Primzahl von E*
Output*: über $\mathbb{F}_{2^n}$ definierte Isogenie $\varphi : E \to E'$ vom Grad ℓ*

- $E^t :=$ *quadratischer Twist von* E
- $\psi : E^t \to E$ *ein* $\mathbb{F}_{2^{2n}}$*-Isomorphismus*
- $Q :=$ *mithilfe von Algorithmus 6.24 berechnetes Kernpolynom*
- $P \in E^t$ *ein Punkt der galois-invarianten Untergruppe mit* $\lambda P = \pi(P)$
- $G := \langle \psi(P) \rangle$
- $\varphi : E \to E'$ *mithilfe der Vélu-Formel (Abschnitt 6.1) berechnete Isogenie*
- *RETURN* φ

6.4.3 Der Fall $\ell = 2$

Für $\ell = 2$ funktioniert die Berechnung einer Isogenie folgendermassen:

6.28 Algorithmus. ***Berechnung einer Isogenie vom Grad 2***
Input: *E/K elliptische Kurve, für die 2 eine Elkies-Primzahl ist*
Output: *$\varphi : E \to E'$ Isogenie vom Grad 2*

- $\widetilde{j}$ = *Nullstelle von* $\Psi_2(j(E), x)$
- *IF* $char(K) = 2$ *AND* $\widetilde{j} = j(E)^2$ *THEN*
  - $E' := E^{(2)}$
  - *RETURN* $\varphi : E \to E', (x, y) \mapsto (x^2, y^2)$
- *END IF*
- *FOR* $P \in E[2]$ *DO*
  - $\widetilde{\varphi} : E \to E'$ = *mit Vélu berechnete Isogenie mit Kern* $\{P, \mathcal{O}\}$
  - *IF* $j(E') = \widetilde{j}$ *THEN*
    - *RETURN* $\widetilde{\varphi}$
  - *END IF*
- *END FOR*

6.29 Bemerkung. Frobenius-Isogenien
Im Algorithmus zur Berechnung einer Isogenie vom Grad 2 kann im Fall der Charakteristik 2 eine *Frobenius-Isogenie* die passende Abbildung sein. Die Gleichung der Zielkurve $E' = E^{(2)}$ entsteht aus der Gleichung der Ausgangskurve durch Quadrieren der Koeffizienten. Es gilt dann $j(E') = j(E)^2$. Eine solche Frobenius-Isogenie kann in unserem Algorithmus allerdings nur im Fall $\ell = 2$ vorkommen, da die Charakteristik des Grundkörpers für die Berechnung von Isogenien mit Algorithmus 6.15 voraussetzt, dass die Charakteristik deutlich grösser als der Grad der Isogenie ist.

6.30 Bemerkung. Die j-Invariante benötigen wir eigentlich nicht zum Berechnen einer Isogenie vom Grad 2. Allerdings werden wir später diesen Algorithmus so anwenden, dass wir eine j-Invariante vorgeben, welche die Zielkurve haben soll.

6.5 Berechnung von isogenen Kurven mit gleichem Endomorphismenring

Seien wieder E/K eine ordinäre elliptische Kurve über einem endlichen Körper, $\pi : E \to E$ der Frobenius-Endomorphismus von E und $\mathcal{O} := \mathrm{End}(E)$. Mit den Sätzen 3.34 und 3.35 folgt, dass alle Primzahlen ℓ, welche die Diskriminante von

$\mathbb{Z}[\pi]$ teilen, Elkies-Primzahlen von E sind, denn für ein solches ℓ gilt: $f_\pi \equiv (x-\lambda)^2 \mod \ell$. Also sind auch alle Teiler des Führers von $\mathbb{Z}[\pi]$ Elkies-Primzahlen. Wir können somit zu einer Primzahl ℓ mit $\ell \mid [\mathcal{O}_F : \mathcal{O}]$ mithilfe von Algorithmus 6.15 bzw. 6.24 eine K-Isogenie nach oben vom Grad ℓ berechnen: Wir testen für alle Nullstellen $j' \in K$ von $\Psi_\ell(j(E), x)$, ob $\ell = [\mathrm{End}(E') : \mathcal{O}]$ für eine Kurve E' mit j-Invariante j' und gleicher Punktanzahl über K wie E. Wenn wir die passende Nullstelle gefunden haben, dann berechnen wir die Isogenie hierzu. Im folgenden Algorithmus berechnen wir zu zwei isogenen elliptischen Kurven E_1 und E_2 zwei Kurven E_1' und E_2' und Isogenien $\varphi_1 : E_1 \to E_1'$ und $\varphi_2 : E_2 \to E_2'$ mit $\mathrm{End}(E_1')$ =$\mathrm{End}(E_2')$. Dies werden wir später benötigen. Hierbei ist $\varphi(E, \ell, k)$ eine mit Algorithmus 6.15 bzw. 6.24 berechnete Isogenie $\varphi : E \to E'$, so dass $j(E') = k$-te Nullstelle von $\Psi_\ell(j(E), x)$ gilt. (Wir nehmen hier an, dass wir die Nullstellen eines Polynoms als Liste gegeben haben, wie es z.B. in KASH3 der Fall ist.)

6.31 Algorithmus. ***Berechnung von isogenen Kurven mit gleichem Endomorphismenring***

Input: *$E_1/\mathbb{F}_q, E_2/\mathbb{F}_q$ isogene elliptische Kurven*

Output: *E_1', E_2' mit $End(E_1') = End(E_2'), \varphi_1 : E_1 \to E_1', \varphi_2 : E_2 \to E_2'$.*

- *c_1 := Füher von $End(E_1)$, c_2 := Füher von $End(E_2)$*
- *$g := ggT(c_1, c_2), f_i := \frac{c_i}{g}$*
- *f_i :=Factorization$(f_i), \varphi_i := id_{E_i}$*
- *FOR $i \in \{1, 2\}$ DO*
  - *$E := E_i, \mathcal{O}$:=$End(E_i)$*
  - *FOR $k \in \{1, ..., \#f_i\}$ DO*
    - *$\ell := f_i[k][1]$, berechne Ψ_ℓ*
    - *FOR $l \in \{1, ..., f_i[k][2]\}$ DO*
      - *ro:=Nullstellen von $\Psi_\ell(j(E), x)$*
      - *IF #ro = 1 THEN*
        - *$\varphi := \varphi(E, \ell, 1) \circ \varphi$*
      - *ELSE*
        - *finde in ro j-Invariante einer isogenen elliptischen Kurve E' mit $End(E') \supsetneq \mathcal{O}$, n:=Index von j(E') in ro*
        - *$\varphi := \varphi(E, \ell, n) \circ \varphi, E := E', \mathcal{O}$:=$End(E)$*
      - *END IF*
    - *END FOR*
  - *END FOR*
  - *$E_i' := E, \varphi_i := \varphi$*
- *END FOR*
- *RETURN $E_1', E_2', \varphi_1, \varphi_2$*

6.32 Bemerkung. Erläuterung von Algorithmus 6.31
Wir berechnen in dem Algorithmus zwei elliptische Kurven mit isomorphem Endomorphismenring. Dabei legen wir fest, dass dieser über den ursprünglichen Endomorphismenringen liegt, wir müssen also passende Isogenien finden, welche nach oben gehen. Sei $p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ die Faktorisierung von f_1. Sei $\ell := p_1$. Hat nun $\Psi_\ell(j(E_1), x)$ nur eine Nullstelle j', dann wissen wir mit Tabelle 5.1, dass die Isogenie vom Grad ℓ, welche von E_1 zu einer elliptischen Kurve E' mit j-Invariante j' führt, nach oben geht, d.h. $\mathrm{End}(E') \supsetneq \mathrm{End}(E_1)$ und $[\mathrm{End}(E') \colon \mathrm{End}(E_1)] = p_1$. Falls es mehr als eine Nullstelle gibt, müssen wir die Nullstellen so lange durchprobieren, also Kurven mit den entsprechenden j-Invarianten erzeugen und den Endomorphismenring berechnen, bis wir eine Kurve gefunden haben, die auf einem höheren Level liegt. Von E' aus gehen wir mit dem nächsten Faktor weiter nach oben, bis wir alle Faktoren abgearbeitet haben.
Unser eigentliches Ziel ist es, eine Isogenie zwischen E_1 und E_2 zu finden. Die Situation wird durch folgendes Diagramm verdeutlicht. Die Isogenie φ ist dabei noch unbekannt. Rechts neben den Pfeilen stehen jeweils die Grade der Isogenien.

$$\begin{array}{ccc} E_1' & \xrightarrow[?]{\varphi} & E_2' \\ {\scriptstyle\varphi_1}\uparrow{\scriptstyle\frac{c_1}{c}} & & \widehat{\varphi_2}\downarrow{\scriptstyle\frac{c_2}{c}} \\ E_1 & & E_2 \end{array}$$

Sind wir dann auf demselben Level, so haben wir unser Problem auf das Finden einer Isogenie mit demselben Endomorphismenring beschränkt. Dann suchen wir noch eine passende Verkettung von Isogenien mit Primzahlgraden ℓ, die den Führer von $\mathbb{Z}[\pi]$ nicht teilen, denn wir brauchen, auf der Endomorphismenringseite gesehen, nicht mehr hinauf oder herab zu gehen, wir betrachten nun nur noch horizontale Isogenien. Für Elkies-Primzahlen wissen wir schon, wie man eine solche Isogenie berechnet. Wir wissen allerdings noch nicht, ob wir auch jede zu einer Kurve E isogene Kurve auf demselben Level durch Verkettung solcher aus Elkies-Primzahlen entstehenden Isogenien erreichen können. Mit dieser Fragestellung werden wir uns später beschäftigen.

6.6 Erster Algorithmus

Aus den letzten beiden Abschnitten ergibt sich schon ein erster Algorithmus zur Lösung unseres Problems: Seien E_1/K und E_2/K zwei ordinäre, isogene elliptische Kurven, d.h. $\#E_1(K) = \#E_2(K)$. Gesucht ist eine konkrete, über K definierte Isogenie $\varphi : E_1 \to E_2$. Wir können annehmen, dass $\mathrm{End}(E_1) = \mathrm{End}(E_2)$. Trifft das nicht zu, kann man mit Algorithmus 6.31 diese Situation herbeiführen. Ab

jetzt heisst eine Primzahl ℓ nur noch dann Elkies-Primzahl, wenn sie nicht den Führer von $\mathbb{Z}[\pi]$ teilt.

6.33 Algorithmus.
Input: *E_1, E_2 elliptische Kurven mit obigen Eigenschaften*
Output: *Isogenie $\varphi : E_1 \to E_2$*

- *L:= Elkies-Primzahlen von E_1*
- *$E := E_1,\ j := j(E_1)$*
- *$\varphi := id_{E_1}$*
- *WHILE NOT $(j = j(E_2))$ DO*
  - *wähle zufällig $\ell \in L$*
  - *$\tilde{j}$:= eine der beiden Nullstellen von $\Psi_\ell(j, x)$*
  - *berechne mit Algorithmus aus 6.3 eine galois-invariante Untergruppe C von $E[\ell]$*
  - *berechne mit Algorithmus aus 6.1 die Isogenie $\psi : E \to E/C$*
  - *$E := E/C,\ j := \tilde{j},\ \varphi := \psi \circ \varphi$*

  END WHILE
- *RETURN φ*

Wir wissen noch nicht, ob dieser Algorithmus terminiert. Und es gibt noch ein weiteres Problem: Die Grade der durch Komposition entstehenden Isogenien werden sehr schnell sehr gross, denn es gilt nach Korollar 2.26:
Sind $\varphi_1 : E_1 \to E_2,\ \varphi_2 : E_2 \to E_3$ zwei separable Isogenien vom Grad ℓ_1 bzw. ℓ_2, dann ist $\deg(\varphi_2 \circ \varphi_1) = \ell_1 \cdot \ell_2$. Um den Grad der resultierenden Isogenie deutlich zu verringern und um auch die Frage der Terminierung des obigen Algorithmus zu klären, erläutern wir im übernächsten Abschnitt den Zusammenhang zwischen Isogenien und Picardgruppen des Endomorphismenrings. Zunächst benötigen wir jedoch noch einige zahlentheoretische Betrachtungen.

6.7 Quadratische Formen und die Picardgruppe

Wir haben schon in Kapitel 4 gesehen, dass es bestimmte Beziehungen zwischen Idealklassen der Picardgruppe des Endomorphismenrings einer elliptischen Kurve und den von dieser Kurve ausgehenden Isogenien gibt. Wie man diese Beziehung in unserem Algorithmus verwenden kann, werden wir später noch genauer ausführen.
Um effizient mit den Idealen einer Ordnung zu rechnen, vor allem um einen eindeutigen Vertreter einer Klasse von Idealen bestimmen zu können, welcher „kleine“ Koeffizienten hat, führen wir hier binäre quadratische Formen ein.

6.34 Definition. Eine *binäre quadratische Form* ist eine Funktion

$$f(x,y) = \alpha x^2 + \beta xy + \gamma y^2.$$

Dies schreiben wir abgekürzt als $f = (\alpha, \beta, \gamma)$. Die binäre quadratische Form f heisst *primitiv*, wenn $ggT(\alpha, \beta, \gamma) = 1$, und *ganz*, wenn $\alpha, \beta, \gamma \in \mathbb{Z}$. Wir bezeichnen $D = \beta^2 - 4\alpha\gamma$ als *Diskriminante* der quadratischen Form (α, β, γ). Eine binäre quadratische Form $f(x,y)$ heisst *positiv definit*, wenn $f(x,y) > 0$ für alle $(0,0) \neq (x,y) \in \mathbb{Z} \times \mathbb{Z}$.
Sind f und g zwei binäre quadratische Formen, dann heissen sie *äquivalent*, wenn es eine Matrix $M = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}$ mit ganzen Einträgen und $det(M) = 1$ gibt, so dass $g(x,y) = f(m_{11}x + m_{12}y, m_{21}x + m_{22}y)$. Wir bezeichnen mit $\mathcal{F}^+(D)$ die Menge der Äquivalenzklassen positiv definiter binärer quadratischer Formen der Diskriminante D.

6.35 Bemerkung. Wir schreiben auch manchmal zur Abkürzung nur quadratische Form und meinen dann aber hier immer eine positiv definite binäre quadratische Form.

Sei nun F ein imaginärquadratischer Zahlkörper und $\mathcal{O} = \mathbb{Z}[\omega]$ eine Ordnung von F. Wir können nun Ideale von $\mathcal{O}$ mit positiv-definiten binären quadratischen Formen der Diskriminante $disc(\mathcal{O})$ identifizieren:
Wir setzen

$$\phi_{IF}(\mathfrak{a}) := \frac{\mathcal{N}(ax - (b+\omega)y)}{\mathcal{N}(\mathfrak{a})}$$

Dann gilt folgendes

6.36 Lemma. *Die Abbildung ϕ_{IF} bildet gebrochene Ideale von $\mathcal{O}$ auf ganze, positiv definite quadratische Formen der Diskriminante $disc(\mathcal{O})$ ab.*

Beweis. Das Lemma ist ein Teil von Theorem 5.2.4 aus [Coh96], allerdings gestalten wir den Beweis deutlich ausführlicher.
Zunächst betrachten wir Ideale der Form $\mathfrak{a} = a\mathbb{Z} + (b + \omega\mathbb{Z}),\ a, b \in \mathbb{Z}^{\geq 0}, b < a$ in Hermite-Normal-Form (siehe Proposition 3.19). Es ist dann

$$\begin{aligned}
\phi_{IF}(\mathfrak{a}) &= \frac{\mathcal{N}(ax - (b+\omega)y)}{\mathcal{N}(\mathfrak{a})} \\
&= \frac{(ax - (b+\omega)y)\sigma(ax - (b+\omega)y)}{\mathcal{N}(\mathfrak{a})} \\
&= \frac{a^2x^2 - a(2b + Tr(\omega))xy + \mathcal{N}(b+\omega)y^2}{a} \text{ (da } \sigma \text{ Ringhomomorphismus)} \\
&= ax^2 - (2b + Tr(\omega))xy + \frac{\mathcal{N}(b+\omega)}{a}y^2
\end{aligned}$$

Auch $\frac{\mathcal{N}(b+\omega)}{a} \in \mathbb{Z}$, da $\mathcal{N}(b+\omega) = (b+\omega)\sigma(b+\omega) \in \mathfrak{a}$. Andererseits $\mathcal{N}(b+\omega) \in \mathbb{Z}$, also $\mathcal{N}(b+\omega) \in \mathfrak{a} \cap \mathbb{Z} = a\mathbb{Z}$. Somit ist $\phi_{IF}(\mathfrak{a}) = \left(a, -2b - Tr(\omega), \frac{\mathcal{N}(b+\omega)}{a}\right)$ eine ganze binäre quadratische Form.
Ist nun $\mathfrak{b} = \widetilde{a}\mathbb{Z} + (\widetilde{b} + c\omega)\mathbb{Z}, \widetilde{a}, \widetilde{b} \in \mathbb{Z}$, ein Ideal in Hermite-Normal-Form, dann können wir es, wegen $c|\widetilde{a}$ und $c|\widetilde{b}$ auch als $\mathfrak{b} = ca\mathbb{Z} + (cb + c\omega)\mathbb{Z}$ schreiben. Dann ist

$$\begin{aligned}
\phi_{IF}(\mathfrak{b}) &= \frac{\mathcal{N}(cax - (cb + c\omega)y)}{\mathcal{N}(\mathfrak{b})} \\
&= \frac{\mathcal{N}(c(ax - (b+\omega)y))}{ac^2} \\
&= \frac{c^2\mathcal{N}(ax - (b+\omega)y)}{ac^2} \\
&= \left(a, -(2b + Tr(\omega)), \frac{\mathcal{N}(b+\omega)}{a}\right) \\
&= \phi_{IF}(a\mathbb{Z} + (b+\omega)\mathbb{Z})
\end{aligned}$$

Nun fehlen noch Ideale der Form $\mathfrak{c} = \frac{\mathfrak{a}}{d}$, mit $\mathfrak{a} = a\mathbb{Z} + (b + c\omega)\mathbb{Z}$ ein ganzes Ideal von $\mathcal{O}, d \in \mathbb{Z}$. Aber

$$\begin{aligned}
\phi_{IF}(\mathfrak{c}) &= \phi_{IF}\left(\frac{a\mathbb{Z} + (b + c\omega)\mathbb{Z}}{d}\right) \\
&= \frac{\mathcal{N}(\frac{1}{d}(a\mathbb{Z} + (b + c\omega)\mathbb{Z}))}{\mathcal{N}(\mathfrak{c})} \\
&= \frac{\frac{1}{d^2}\mathcal{N}(a\mathbb{Z} + (b + c\omega)\mathbb{Z})}{\frac{1}{d^2}\mathcal{N}(\mathfrak{a})} \\
&= \phi_{IF}(\mathfrak{a})
\end{aligned}$$

Weiter gilt für $(\alpha, \beta, \gamma) = \phi_{IF}(a\mathbb{Z} + (b+\omega)\mathbb{Z})$, dass

$$\beta^2 - 4\alpha\gamma = disc(\mathcal{O}) = Tr(\omega)^2 - 4\mathcal{N}(\omega),$$

denn

$$\begin{aligned}
\beta^2 - 4\alpha\gamma &= (2b + Tr(\omega))^2 - 4a\left(\frac{\mathcal{N}(b+\omega)}{a}\right) \\
&= 4b^2 + 4bTr(\omega) + Tr(\omega)^2 - 4(b^2 + bTr(\omega) + \mathcal{N}(\omega)) \\
&= Tr(\omega)^2 - 4\mathcal{N}(\omega) = disc(\mathcal{O})
\end{aligned}$$

Jetzt bleibt nur noch die positive Definitheit zu zeigen: Wir können die binäre quadratische Form $f(x,y) = \alpha x^2 + \beta xy + \gamma y^2$ auch durch eine symmetrische Matrix M_f darstellen:

$$f(x,y) = (x,y)\begin{pmatrix}\alpha & \frac{\beta}{2}\\ \frac{\beta}{2} & \gamma\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix}$$

Somit ist $f(x,y)$ genau dann positiv definit, wenn M_f positiv definit ist, das ist der Fall, wenn alle Unterdeterminanten von M_f positiv sind, also muss hier (i) $\alpha = a > 0$ und (ii) $\alpha\gamma - \frac{\beta^2}{4} > 0$ gelten. (i) ist trivialerweise erfüllt. Auch Bedingung (ii) ist erfüllt, da $\alpha\gamma - \frac{\beta^2}{4} = -\frac{D}{4} > 0$. □

Damit das Ganze Sinn macht, brauchen wir natürlich auch noch eine Abbildung, welche quadratische Formen der Diskriminante D auf Ideale von $\mathcal{O}$ in Hermite-Normalform abbildet. Da unsere Basisdarstellung für $\mathcal{O}$ im Allgemeinen von der in [Coh96], 5.2, verwendeten abweicht, sieht auch unsere Umkehrabbildung ein bisschen anders aus: Wir definieren

$$\phi_{FI}(\alpha,\beta,\gamma) = \alpha\mathbb{Z} + \left(\frac{-\beta - Tr(\omega)}{2} + \omega\right)\mathbb{Z}.$$

Setzen wir nun eine mittels ϕ_{IF} erhaltene quadratische Form

$$\phi_{IF}\left(\frac{a\mathbb{Z} + (b+c\omega)\mathbb{Z}}{d}\right) = \left(a, -2b - Tr(\omega), \frac{N(b+\omega)}{a}\right)$$

in diese Funktion ein, so ergibt sich

$$\begin{aligned}\phi_{FI}\left(a, -2b - Tr(\omega), \frac{N(b+\omega)}{a}\right) &= a\mathbb{Z} + \left(\frac{2b + Tr(\omega) - Tr(\omega)}{2} + \omega\right)\mathbb{Z}\\ &= a\mathbb{Z} + (b+\omega)\mathbb{Z}\end{aligned}$$

Wir haben also gezeigt, dass

$$\phi_{FI}\left(\phi_{IF}\left(\frac{ca\mathbb{Z} + (cb+c\omega)\mathbb{Z}}{d}\right)\right) = a\mathbb{Z} + (b+\omega)\mathbb{Z},$$

also

6.37 Satz. *([Coh96], Theorem 5.2.8.)*
Sei $D < 0$ mit $D \equiv 0, 1 \mod 4$ und $\mathcal{O}$ eine Ordnung in einem imaginärquadratischen Zahlkörper mit disc$(\mathcal{O}) = D$. Dann induzieren die Abbildungen ϕ_{IF} und ϕ_{FI} inverse Bijektionen von $\mathcal{F}^+(D)$ und Pic$(\mathcal{O})$.

Dies bedeutet folgendes: Starten wir mit einem gebrochenen Ideal $\mathfrak{a}$ von $\mathcal{O}$, so erhalten wir eine binäre quadratische Form $(\alpha,\beta,\gamma) = \phi_{IF}(\mathfrak{a})$. Dann ist $\phi_{FI}(\alpha,\beta,\gamma) = \xi\mathfrak{a}, \xi \in F$ und daher $\phi_{FI}(\phi_{IF}(\mathfrak{a})) \sim \mathfrak{a}$. Wenden wir ϕ_{IF} auf ein Ideal $\mathfrak{b} \sim \mathfrak{a}$ an, so erhalten wir eine binäre quadratische Form (α',β',γ') mit

$(\alpha, \beta, \gamma) \sim (\alpha', \beta', \gamma')$.
Nun wollen wir noch erläutern, wie man mithilfe binärer quadratischer Formen einen eindeutigen Vertreter einer Klasse von $Pic(\mathcal{O})$ definieren kann. Dies geschieht mit *reduzierten* binären quadratischen Formen:

6.38 Definition. Eine positiv definite binäre quadratische Form (a, b, c) heisst *reduziert*, wenn $\mid b \mid \leq a \leq c$ und, falls $\mid b \mid = a$ oder $a = c$, dann $b > 0$.

Dann gilt folgender Satz:

6.39 Proposition. *In jeder Äquivalenzklasse positiv definiter quadratischer Formen mit Diskriminante $D < 0$ gibt es genau eine reduzierte Form.*

Beweis. siehe [Coh96], Proposition 5.3.3. □

Ist $\mathfrak{a}$ ein gebrochenes Ideal von $\mathcal{O}$, so erhalten wir einen eindeutigen Repräsentanten der Idealklasse von $\mathfrak{a}$, indem wir $\phi_{IF}(\mathfrak{a}) = (\alpha, \beta, \gamma)$ bilden und die reduzierte Form $(\alpha', \beta', \gamma') \sim (\alpha, \beta, \gamma)$ berechnen. Dann ist $\phi_{FI}(\alpha', \beta', \gamma')$ ein eindeutiger Vertreter der Idealklasse von $\mathfrak{a}$. Weiterhin gilt noch:

6.40 Korollar. *Sei f eine reduzierte binäre quadratische Form und sei $\mathfrak{a} := \phi_{FI}(f)$. Dann ist*

$$\mathcal{N}(\mathfrak{a}) \leq \mathcal{N}(\mathfrak{b}) \text{ für alle ganzen Ideale } \mathfrak{b} \sim \mathfrak{a} \text{ von } \mathcal{O}$$

Beweis. Aus dem Beweis zu [Coh96], Proposition 5.3.3, geht hervor, dass für binäre quadratische Formen gilt:

$$(\alpha, \beta, \gamma) \text{ ist reduziert } \Leftrightarrow \text{ für alle } (\alpha', \beta', \gamma') \sim (\alpha, \beta, \gamma) \text{ gilt } \alpha \leq \alpha'.$$

Aber

$$\begin{aligned} \phi_{IF}(\alpha, \beta, \gamma) &= \alpha\mathbb{Z} + \left(\frac{-\beta - Tr(\omega)}{2} + \omega\right)\mathbb{Z} \\ &= a\mathbb{Z} + (b + \omega)\mathbb{Z} \\ &=: \mathfrak{a}. \end{aligned}$$

Da $\mathcal{N}(\mathfrak{a}) = a = \alpha$, gibt es in der Klasse von $\mathfrak{a}$ kein Ideal $\mathfrak{a}' := a'\mathbb{Z} + (b' + \omega)\mathbb{Z}$ mit $\mathcal{N}(\mathfrak{a}') < \mathcal{N}(\mathfrak{a})$, denn das würde im Widerspruch zu f reduziert stehen. Nun nehmen wir an, dass $\widetilde{\mathfrak{a}} := c\widetilde{a}\mathbb{Z} + (c\widetilde{b} + c\omega)\mathbb{Z}$ ein zu $\mathfrak{a}$ äquivalentes Ideal mit $\mathcal{N}(\widetilde{\mathfrak{a}}) = c^2\widetilde{a} < \mathcal{N}(\mathfrak{a}) = a$. Dann gäbe es ein zu $\widetilde{\mathfrak{a}}$ und somit zu $\mathfrak{a}$ äquivalentes Ideal mit noch kleinerer Norm, nämlich $\widetilde{a}\mathbb{Z} + (\widetilde{b} + \omega)\mathbb{Z}$. Das haben wir aber oben schon ausgeschlossen. □

Um diese Erkenntnisse anwenden zu können, fehlt uns noch ein effizienter Algorithmus zur Berechnung einer reduzierten binären quadratischen Form, welchen wir aus [Coh96] (Algorithm 5.4.2) entnehmen:

6.41 Algorithmus. ***Reduktion einer positiv definiten quadratischen Form***
*-**Input:** f= (a,b,c) eine positiv definite quadratische Form*
*-**Output:** f' = (a',b',c') reduzierte quadratische Form mit $f \sim f'$*

1. *IF* $-a < b \leq a$ *THEN*
   GO TO 3.
   END IF
2. $r := b \mod 2a, q := \lfloor \frac{b}{2a} \rfloor$
   IF $r > a$ *THEN*
   $r := r - 2a, q := q + 1$
   END IF
   $c := c - \frac{1}{2}(b + r)q, b := r$
3. *IF* $a > c$ *THEN*
   $b := -b, tmp := a, a := c, c := tmp$
   GO TO 2.
   ELSE IF $a = c$ *AND* $b < 0$ *THEN*
   $b := -b$
   END IF
   RETURN (a,b,c)

Ausserdem gilt noch, dass reduzierte binäre quadratische Formen Idealen kleiner Norm entsprechen, genauer

6.42 Lemma. *Sei $f = (\alpha, \beta, \gamma)$ eine positiv definite reduzierte quadratische Form mit Diskriminante $D = \beta^2 - 4\alpha\gamma < 0$. Dann ist $\alpha \leq \sqrt{|D|/3}$.*

Beweis. [Coh96], Lemma 5.3.4 (1). □

Nun führen wir noch den Begriff der reduzierten Ideale ein:

6.43 Definition. Ein Ideal $\mathfrak{a} \subset \mathcal{O}$ heisst *reduziert*, wenn es eine reduzierte binäre quadratische Form f gibt mit $det(f) = det(\mathcal{O})$ und $\mathfrak{a} = \phi_{FI}(f)$.

Wir halten noch folgende Schlussfolgerung fest:

6.44 Lemma. *Sei $\mathfrak{a} \subset \mathcal{O}$ ein reduziertes, zum Führer von $\mathcal{O}$ teilerfremdes Ideal und sei $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_r^{e_r}$ die mithilfe von Satz 3.25 gewonnene Primidealfaktorisierung von $\mathfrak{a}$. Dann sind die $\mathfrak{p}_i$ reduzierte Ideale.*

Beweis. Sei oBdA $\mathfrak{p}_1$ nicht reduziert, also $\mathfrak{p}_1 \sim \mathfrak{b}$ mit $\mathcal{N}(\mathfrak{b}) < \mathcal{N}(\mathfrak{p}_1)$. Da alle vorkommenden Ideale invertierbar sind, ist die Norm nach Lemma 3.20(*ii*) multiplikativ: $\mathcal{N}(\mathfrak{a}) = \mathcal{N}(\mathfrak{p}_1)^{e_1} \cdot \ldots \cdot \mathcal{N}(\mathfrak{p}_r)^{e_r}$. Dann ist aber auch $\mathfrak{a} \sim \mathfrak{a}' := \mathfrak{b}^{e_1} \cdot \mathfrak{p}_2^{e_r} \cdot \ldots \cdot \mathfrak{p}_r^{e_r}$ und $\mathcal{N}(\mathfrak{a}') < \mathcal{N}(\mathfrak{a})$. Dies ist wegen Korollar 6.40 ein Widerspruch dazu, dass $\mathfrak{a}$ ein reduziertes Ideal ist. □

6.8 Isogenien und Ideale

Wie können wir nun unsere Isogenien in Ideale des Endomorphismenrings umwandeln?
Zunächst betrachten wir die Torsionsgruppe eines Ideals des Endomorphismenrings $\mathcal{O}$ einer elliptischen Kurve E/K.

6.45 Definition. Für ein ganzes Ideal $\mathfrak{a}$ von O ist

$$E[\mathfrak{a}] := \{P \in E \mid \alpha(P) = 0 \text{ für alle } \alpha \in \mathfrak{a}\}.$$

Dann gilt:

6.46 Proposition. *$E[\mathfrak{a}]$ ist der Kern der Abbildung $E \to \overline{\mathfrak{a}} * E$.*

Beweis. [Sil94], Proposition II.1.4 (a) □

Sei wieder $E/\mathbb{F}_q$ eine elliptische Kurve mit $\mathrm{End}(E) = \mathcal{O}$, sei φ die durch einen der Algorithmen aus Abschnitt 6.4 berechnete Isogenie $\varphi : E \to E_2$ vom Grad ℓ. Den Kern dieser Abbildung φ kennen wir aber: Es ist die Menge

$$C := \{P \in E[\ell] \mid \pi(P) = \lambda P\},$$

wobei λ der passende Eigenwert des Frobenius-Endomorphismus ist. Für das entsprechende Ideal $\mathfrak{a}$ muss also gelten: $\ell \equiv 0 \mod \mathfrak{a}$ und $\pi - \lambda \equiv 0 \mod \mathfrak{a}$, also $\mathfrak{a} = \ell\mathbb{Z} + (\pi - \lambda)\mathbb{Z}$.
Andersherum können wir aus einem auf diese Weise gewonnenen Ideal
$\mathfrak{a} = a\mathbb{Z} + (b + c\omega)\mathbb{Z}$ wieder die zur Isogenieberechnung nötigen Informationen herausfinden: Der Grad der zugehörigen Isogenie φ ist a, der Eigenwert des Frobenius-Endomorphismus auf dem Kern von φ ist $\pi \bmod \mathfrak{a}$.

6.47 Bemerkung. Im Fall der in Bemerkung 6.29 angesprochenen Frobenius-Isogenie setzen wir den Eigenwert des Frobenius auf der Untergruppe auf 0. Erhalten wir andersherum ein Ideal $\mathfrak{a}$ mit $\pi \mod \mathfrak{a} = 0$, dann müssen wir als passende Isogenie dazu eine Frobenius-Isogenie berechnen.

Wenn wir eine Isogenie $\varphi : E_1 \to E_2$ vom Grad ℓ und mit Eigenwert λ des Frobenius-Endomorphismus auf dem Kern als $\varphi_{(\ell,\lambda)}(E_1)$ schreiben, dann gibt es also Bijektionen

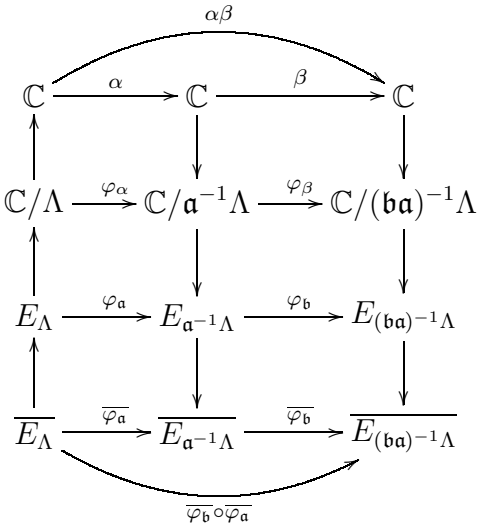
$$\psi_1 : H_E \to P(\mathrm{End}(E)), \quad \varphi_{(\ell,\lambda)}(E) \mapsto \ell\mathbb{Z} + (\pi - \lambda\omega)\mathbb{Z}$$
$$\psi_2 : P(\mathrm{End}(E)) \to H_E, \quad a\mathbb{Z} + (b + c\omega)\mathbb{Z} \mapsto \varphi_{(a,\pi \bmod \mathfrak{a})}(E).$$

Hierbei bezeichnen wir für eine Ordnung $\mathcal{O}$ in einem imaginärquadratischen Zahlkörper F mit $P(\mathcal{O})$ die Menge der ganzen Primideale von $\mathcal{O}$, welche über in F zerlegten Primzahlen liegen. H_E sind die von E startenden horizontalen Isogenien, die mithilfe einer Elkies-Primzahl berechnet wurden. Die Abbildung $\psi_2(\mathfrak{a})$ entspricht hier der oben definierten Abbildung $E \to \overline{\mathfrak{a}} * E$.
Betrachten wir nun die folgende Situation:

Seien E_1, E_2, E_3 elliptische Kurven über K mit $\mathrm{End}(E_i) = \mathcal{O}$. Seien $\mathfrak{a}, \mathfrak{b} \in P(\mathcal{O})$ und seien $\varphi_1 : E_1 \to E_2$ und $\varphi_2 : E_2 \to E_3$ Isogenien, welche aus $\mathfrak{a}$ und $\mathfrak{b}$ errechnet wurden, also $\psi_2(\mathfrak{a}) = \varphi_1$ und $\psi_2(\mathfrak{b}) = \varphi_2$. Dann entspricht das Ideal $\mathfrak{ab}$ der Hintereinanderausführung der Isogenien, denn wir können es mithilfe von Satz 3.25 eindeutig faktorisieren, da laut Voraussetzung die Normen der Ideale Elkies-Primzahlen sind und somit, nach der Konvention in Abschnitt 6.6, $\mathfrak{ab}$ koprim zum Führer von $\mathbb{Z}[\pi]$ ist. Ausserdem ist es für unsere Zwecke egal, ob wir

$$\varphi_1 := \psi_2(\mathfrak{a}) \circ \psi_2(\mathfrak{b}) \text{ oder } \varphi_2 := \psi_2(\mathfrak{b}) \circ \psi_2(\mathfrak{a})$$

berechnen, denn beide Isogenien gehen von E_1 nach E_3. Das folgende Bild verdeutlicht die Situation:



Wegen der Ausführungen auf Seite 36 gilt, dass wir, wenn wir von einer Kurve E_Λ mit Endomorphismenring $\mathcal{O}$ ausgehen, alle Kurven mit Endomorphismenring $\mathcal{O}$ durch eine Abbildung $E_\Lambda \to E_{\mathfrak{a}^{-1}\Lambda}$ erreichen können, wobei $\mathfrak{a}$ ein Produkt von Idealen über zerlegten bzw. verzweigten Primzahlen ist. Mithilfe der im vorigen Abschnitt vorgestellten Reduktion von Idealen durch quadratische Formen können wir möglicherweise sogar, wenn wir ein Ideal $\mathfrak{a}$ gefunden haben, das eine Isogenie zwischen zwei Kurven beschreibt, den Grad dieser Isogenie deutlich verringern: Wir reduzieren $\mathfrak{a}$ und erhalten ein reduziertes Ideal $\mathfrak{b}$ mit $\mathfrak{b} \sim \mathfrak{a}$. Dann gilt wegen Lemma 6.40 $\mathcal{N}(\mathfrak{b}) \leq \mathcal{N}(\mathfrak{a})$ und daher $\deg(\psi_2(\mathfrak{b})) \leq \deg(\psi_2(\mathfrak{a}))$ mit Satz 4.21.
Falls $\mathfrak{b}$ koprim zum Führer von $\mathcal{O}$ ist, so können wir $\mathfrak{b}$ faktorisieren und dann die zugehörige Isogenie durch Verkettung der aus den Primidealen berechneten Isogenien erhalten.
Der Fall $\mathfrak{b}$ nicht koprim zum Führer sollte eigentlich nicht vorkommen, da wir ja, nachdem wir Kurven auf demselben Level erhalten haben, alle Primzahlen, welche den Führer von $\mathbb{Z}[\pi]$ teilen, als Grad einer Isogenie ausgeschlossen haben, denn wir wissen, dass wir uns nur noch horizontal, also mit Isogenien, deren Grad koprim zum Führer ist, bewegen müssen. Allerdings kannn es passieren, dass ein Ideal, welches eigentlich koprim zum Führer war, zu einem nicht zum Führer koprimen Ideal reduziert wird, dazu aber später mehr.

Wir gehen also im Algorithmus zur Berechnung einer Isogenie zwischen zwei elliptischen Kurven E_1, E_2 mit $\mathrm{End}(E_1) = \mathrm{End}(E_2) = \mathcal{O}$ folgendermassen vor:

6.9 Ein Random-Walk auf der Picardgruppe

Aus den obigen Ausführungen wird ersichtlich: Sind $E_1/\mathbb{F}_q$ und $E_2/\mathbb{F}_q$ zwei isogene elliptische Kurven mit $\mathrm{End}(E_1) = \mathrm{End}(E_2) = \mathcal{O}$, dann gibt es ein ganzes Ideal $\mathfrak{a} \subset \mathcal{O}$ von $\mathcal{O}$, sodass $\overline{\mathfrak{a}} * E_1 = E_2$. Dieses gilt es zu finden, um eine Isogenie $\varphi : E_1 \to E_2$ zu berechnen. Dabei gehen wir folgendermassen vor: Wir definieren uns eine pseudozufällige Funktion f, die uns einen „Random-Walk“ auf den möglichen, mit E_1 und E_2 durch eine horizontale Isogenie verbundenen Kurven vorgeben soll. Hierbei hat f als Eingabewert die j-Invariante j einer elliptischen Kurve E und als Ausgabewert eine Elkies-Primzahl ℓ von E und $i \in \{1, 2\}$. Das bedeutet, dass die nächste j-Invariante auf unserem Random-Walk die i-te Nullstelle von $\Psi_\ell(j, x)$ sein soll. Mithilfe von Algorithmus 6.15 bzw. 6.24 berechnen wir einen Faktor F des Divisionspolynoms $\overline{f_\ell}$, aus dem wir folgendermassen den Eigenwert des Frobenius-Endomorphismus auf der Untergruppe im Kern der zugehörigen Isogenie ermitteln:

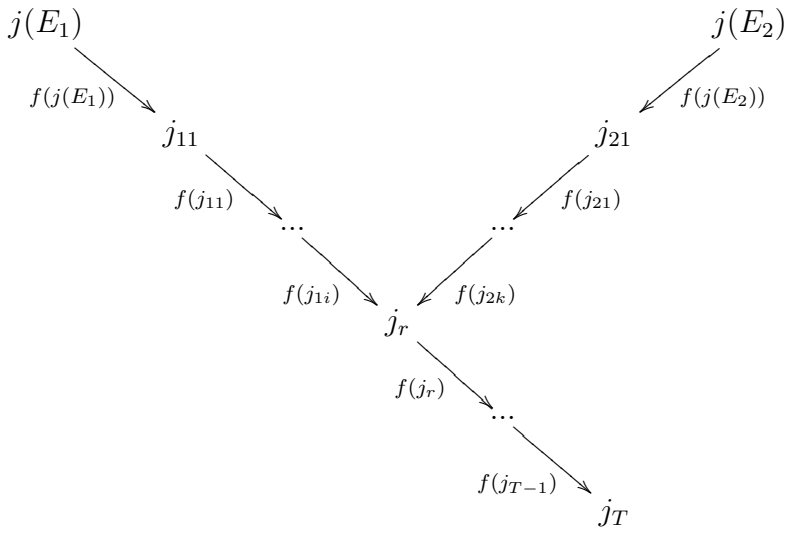
6.48 Algorithmus. ***Berechnung des Eigenwerts von*** π
Input: *$E/\mathbb{F}_q$ elliptische Kurve, F Faktor von $\overline{f_\ell}$*
Output: *Eigenwert des Frobenius-Endormorphismus auf der durch F definierten Untergruppe von E*

- $\{\lambda, \mu\}$*:= Nullstellen von f_π mod ℓ*
- *IF $\lambda = \mu$ THEN RETURN λ*
- *IF $\lambda = -\mu$ THEN*
  - *berechne eine Nullstelle r von F über seinem Zerfällungskörper, $P := (r, s) \in E$ Punkt mit r als x-Koordinate*
  - *IF $\pi(P) = \lambda P$ THEN RETURN λ*
  - *ELSE RETURN μ*
  - *END IF*
- $[\lambda]$:= *Multiplikation-mit-λ-Abbildung von E*
- *IF $\lambda_x \equiv \pi_x$ mod F THEN RETURN λ*
- *ELSE RETURN μ*
- *END IF*

Ist λ dieser Eigenwert, dann ist das passende Picardgruppen-Ideal $\ell\mathbb{Z} + (\pi - \lambda)\mathbb{Z}$. Die pseudozufällige Funktion f ist folgendermassen definiert: Sei L eine Liste der Elkies-Primzahlen≤ 59 von E_1, ω ein Erzeuger von $\mathbb{F}_q^* = \mathbb{F}_{p^n}^*$. Sei $m := \#L$. Wir schreiben j als Summe von Potenzen von ω : $j = a_0 + a_1\omega + ... + a_{n-1}\omega^{n-1}$ und definieren $a := \left(\sum_{k=0}^{n-1} a_k\right)$. Dann ist $f_0(j) := (L[(a \bmod m) + 1], (a \bmod 2) + 1)$. Die passende Isogenie führt zu einer elliptischen Kurve mit j-Invariante $\tilde{j}$, auf die wir wieder die Funktion f anwenden. Für den Pseudo-Random-Walk benutzen wir die *Pollard-Lambda-Methode*: Wir setzen $T := \sqrt{h_\mathcal{O}}$, wobei $h_\mathcal{O}$ die Picardzahl von $\mathcal{O}$ ist. Wir starten bei $j(E_1)$ und gehen T Schritte weit bis j_T. Dann starten wir neu bei $j(E_2)$ und gehen so weit, bis wir bei j_T angekommen sind, höchstens jedoch auch T Schritte. Falls es keine Kollision gibt, probieren wir eine andere pseudozufällige Funktion

$$f_i(j) := (L[(a + i \bmod m) + 1], (a \bmod 2) + 1),\ i \in \{1, \ldots, m-1\}.$$

Die Wahl der Weglänge T basiert auf dem *Geburtstagsparadoxon*: Wählen wir aus einer Menge von n Elementen zufällig $2\sqrt{n}$ Elemente aus, so haben wir mit Wahrscheinlichkeit $> \frac{1}{2}$ ein Element doppelt ausgewählt. Es ergibt sich also, da die pseudozufällige Funktion nur von der eingehenden j-Invariante abhängt, folgendes Bild:



Gibt es eine j-Invariante, in obigem Diagramm j_r, welche mithilfe der Funktion f von beiden Kurven aus erreicht wird, dann trennen sich die Wege auch nicht mehr. Gehen wir nun davon aus, dass unsere pseudozufällige Funktion gleichverteilt ist, das heisst mit gleicher Wahrscheinlichkeit jede j-Invariante einer zu E_1 und E_2 isogenen Kurve mit gleichem Endomorphismenring auswählt, dann ist die Wahrscheinlichkeit, dass sich die beiden Wege kreuzen und wir somit eine Verbindung zwischen E_1 und E_2 finden, grösser als $\frac{1}{2}$, denn die Anzahl der j-Invarianten von Kurven mit gleichem Endomorphismenring war $h_{\mathcal{O}}$, siehe Korollar 4.18.

6.49 Bemerkung. Da die oben definierten pseudozufälligen Funktionen in der Praxis nicht unbedingt gleichverteilt sind, verwenden wir im Algorithmus mehrere von ihnen, um die Wahrscheinlichkeit einer Kollision zu erhöhen.

6.10 Glatte Ideale

Nun betrachten wir noch einmal das reduzierte Ideal, welches eine Isogenie zwischen zwei elliptischen Kurven darstellt und überlegen, ob wir diese Isogenie berechnen können. Hierfür definieren wir zunächst, was ein glattes Ideal ist:

6.50 Definition. Sei $\mathfrak{a}$ ein Ideal einer Ordnung $\mathcal{O}$ und sei $\mathcal{F}$ eine Menge von Primidealen von $\mathcal{O}$. Das Ideal $\mathfrak{a}$ heisst $\mathcal{F}$-glatt, wenn in der Primfaktorisierung von $\mathfrak{a}$ nur Elemente aus $\mathcal{F}$ vorkommen.

Seien nun E_1 und E_2 elliptische Kurven mit demselben Endomorphismenring $\mathcal{O}$, sei $\mathfrak{a}$ das reduzierte Ideal, welches eine Isogenie zwischen E_1 und E_2 repräsentiert. Sei π der Frobenius-Endomorphismus von E_1. Sei $\mathcal{F}$ die Menge aller Primideale von $\mathcal{O}$, deren Norm eine Elkies-Primzahl kleiner als 60 und teilerfremd zum

Führer von $\mathbb{Z}[\pi]$ ist. Falls $\mathfrak{a}$ $\mathcal{F}$-glatt ist, dann können wir $\mathfrak{a}$ faktorisieren und die durch $\mathfrak{a}$ dargestellte Isogenie eindeutig berechnen. Ist dies nicht der Fall, dann können wir, wenn $\mathfrak{a}$ nicht teilerfremd zu $[\mathcal{O}_F : \mathcal{O}]$ ist, $\mathfrak{a}$ nicht faktorisieren bzw. falls $\mathfrak{a}$ nicht teilerfremd zu $[\mathcal{O} : \mathbb{Z}[\pi]]$, die zugehörige Isogenie nicht eindeutig berechnen, denn für einen solchen Primfaktor ℓ gibt es $\ell + 1$ in Frage kommende Nullstellen von Ψ_ℓ (siehe Tabelle 5.1).
Ist $\mathfrak{a}$ nicht $\mathcal{F}$-glatt, dann versuchen wir folgendermassen, das Ideal zu glätten:
Wir behandeln zunächst den Fall, dass $\mathcal{O} = \mathcal{O}_F$ gilt. In KASH3 liefert das Aufrufen der Funktion ClassGroup neben der Struktur und den Erzeugern $\mathfrak{g}_1, ..., \mathfrak{g}_r$ der Klassengruppe eines Zahlkörpers auch eine Funktion, welche jede Idealklasse als Produkt der Erzeuger darstellt. Die Erzeuger sind hierbei immer so gewählt, dass die Norm dieser Ideale möglichst klein ist. Wir berechnen also $\mathfrak{a} \sim \prod_{i=1}^{r} \mathfrak{g}_i^{e_i}$. Sind alle in diesem Produkt vorkommenden Ideale $\mathfrak{g}_i$ mit $e_i \neq 0$ $\mathcal{F}$-glatt, dann haben wir ein $\mathcal{F}$-glattes Ideal $\mathfrak{b} := \prod_{i=1}^{r} \mathfrak{g}_i^{e_i}$ mit $\mathfrak{b} \sim \mathfrak{a}$ gefunden.
Ist eines der $\mathfrak{g}_i$ nicht $\mathcal{F}$-glatt, dann wenden wir folgenden Trick an, der auch zur Berechnung von Erzeugern der Klassengruppe mit möglichst kleiner Norm verwendet wird:
Wir schreiben die ersten r Elemente von $\mathcal{F}$ als Produkt in $\mathfrak{g}_1, ..., \mathfrak{g}_r$:

$$\mathfrak{p}_j \sim \prod_{i=1}^{r} \mathfrak{g}_i^{e_{ij}}$$

Dann bilden wir die folgende Matrix $M \in \mathbb{Z}^{r \times 2r}$:

$$\begin{pmatrix} e_{11} & \dots & e_{1r} & 1 & 0 & 0 & \dots & 0 \\ e_{21} & \dots & e_{2r} & 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & & & & \ddots & & \\ \vdots & \vdots & & & & & \ddots & \\ e_{r1} & \dots & e_{rr} & 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

Aus der i-ten Spalte von M können wir dann ablesen, wie sich $\mathfrak{p}_i$ als Produkt der $\mathfrak{g}_i$ darstellen lässt. Dann bilden wir die Zeilen-Hermite-Normal-Form H von M:

$$\begin{pmatrix} h_{11} & h_{12} & \dots & h_{1r} & \dots & h_{1(2r)} \\ 0 & h_{22} & \dots & h_{2r} & \dots & h_{2(2r)} \\ 0 & & \ddots & \vdots & & \vdots \\ 0 & \dots & 0 & h_{rr} & \dots & h_{r(2r)} \end{pmatrix}$$

Falls nicht alle h_{ii} gleich 1 sind, dann nehmen wir noch weitere Ideale aus $\mathcal{F}$ dazu und wiederholen die Prozedur solange, bis diese Bedingung erfüllt ist bzw. bis alle

Ideale aus $\mathcal{F}$ aufgebraucht sind. Dann können wir die Ideale $\mathfrak{g}_i$ als Produkt von Idealen aus $\mathcal{F}$ darstellen und erhalten somit insgesamt ein $\mathcal{F}$-glattes Ideal $\mathfrak{b}$ mit $\mathfrak{b} \sim \mathfrak{a}$.
Nun besprechen wir den Fall $\mathcal{O} \neq \mathcal{O}_F$. Dies funktioniert in der Theorie genauso wie im Fall der Maximalordnung. Es gibt auch effiziente Algorithmen zur Berechnung der Picardgruppe einer beliebigen Ordnung, siehe [KP03]. Diese sind in KASH3 jedoch noch nicht implementiert. Daher können wir obige Prozedur in unserem Algorithmus nicht anwenden und geben in einem solchen Fall einen Fehler aus. Dass ein solcher Fall durchaus vorkommen kann, verdeutlicht das folgende

6.51 Beispiel. Hier wird ein Ideal, welches koprim zum Führer ist, reduziert zu einem Ideal, welches dies nicht mehr erfüllt.

```
kash% E:=EllipticCurve(101,[1,2]);
EllipticCurve over Finite field of size 101 defined by
 y^2 = x^3 + 1*x + 2
kash% L:=ElkiesPrimes(E);
[ 13, 17, 29, 37, 41, 53 ]
kash% Iso:=IsogenyFromJInvariant(E,13,1);;
kash% jInvariant(E) = jInvariant(Codomain(Iso));
FALSE
kash% O:=EndRing(E);;
kash% Conductor(O);
10
kash% Conductor(EquationOrder(CharacteristicFrobeniusPolynomial(E)));
10
kash% pi:=O.2;;
kash% fact:=IdealFactorization(13*O);;
kash% pi-FrobeniusEigenvalue(Iso) in fact[1][1];
TRUE
kash% I:=fact[1][1];
Ideal of O
Basis:
[ 13  0 ]
[  1  1 ]
kash% I:=IdReduction(I);
Ideal of O
Two element generators:
[8, 0]
[0, 1]
```

Kapitel 7

Algorithmus und Beispiele

Nun haben wir alle Bausteine, die wir zu unserem kompletten Algorithmus zusammenfügen wollen.

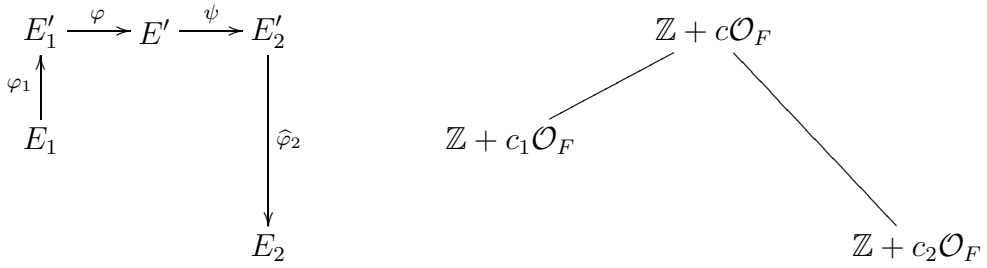
7.1 Der Algorithmus

7.1 Algorithmus. ***Berechnung einer Isogenie zwischen zwei isogenen Kurven***
Input: *$E_1/K, E_2/K$ zwei ordinäre elliptische Kurven mit $\#E_1(K) = \#E_2(K)$*
Output: *eine über K definierte Isogenie $\varphi : E_1 \to E_2$ oder ERROR*

- *$\pi :=$ Frobenius-Endormorphismus von E_1, $c :=$ Füher von $\mathbb{Z}[\pi]$, return ERROR, falls einer der Primfaktoren von $c > 60$ ist*
- *berechne mit Algorithmus 6.31 Kurven $E_1'/K, E_2'/K$ mit gleichem Endomorphismenring $\mathcal{O}$ und $\varphi_1 : E_1 \to E_1'$, $\varphi_2 : E_2 \to E_2'$, $m := \sqrt{h_\mathcal{O}}$*
- *berechne mithilfe einer pseudozufälligen Funktion f eine Verbindung zwischen $j(E_1')$ und $j(E_2')$ (über j_m), return ERROR, falls keine gefunden wird.*
- *starte von E_1', berechne bis j_m alle durch f bestimmten, zu Isogenien gehörigen Ideale, $I_1 :=$ reduziertes Produkt der Ideale, wiederhole den Schritt für E_2', erhalte I_2*
- *falls $I :=$ Reduktion$(I_1 I_2^{-1})$ nicht glatt bzgl. der Primideale von $\mathcal{O}$ mit Elkies-Primzahl-Norm < 60 ist:*
  - *falls $\mathcal{O} = \mathcal{O}_F$: glätte I*
  - *sonst return ERROR*
- *faktorisiere I und berechne die zugehörigen Isogenien, ausgehend von E_1', φ sei die Verkettung dieser Isogenien*
- *falls die Zielkurve E' von φ nicht E_2' ist, dann berechne einen Isomorphismus $\psi : E' \to E_2'$ und setze $\varphi := \psi \circ \varphi$*

- *return* $\widehat{\varphi}_2 \circ \varphi \circ \varphi_1$

Es ergibt sich folgendes Bild:



wobei auf der rechten Seite die Situation der Endormorphismenringe der Kurven auf dem jeweiligen Level zu sehen ist.
Zu Laufzeit und Speicherplatz des Algorithmus findet sich in [GHS02a] folgender Satz:

7.2 Satz. *([GHS02a], Theorem 3)*
Seien $E_1/\mathbb{F}_{q^n}$ und $E_2/\mathbb{F}_{q^n}$ zwei isogene elliptische Kurven. Der (in dieser Arbeit vorgestellte) Algorithmus, welcher $\varphi : E_1 \to E_2$ berechnet, benötigt im worst case $O(q^{\frac{3n}{2}+\epsilon})$ Operationen in $\mathbb{F}_{q^n}$ und $O(q^{n+\epsilon})$ Speicherplatz. Die durchschnittliche Komplexität beträgt $O(q^{\frac{n}{4}+\epsilon})$.

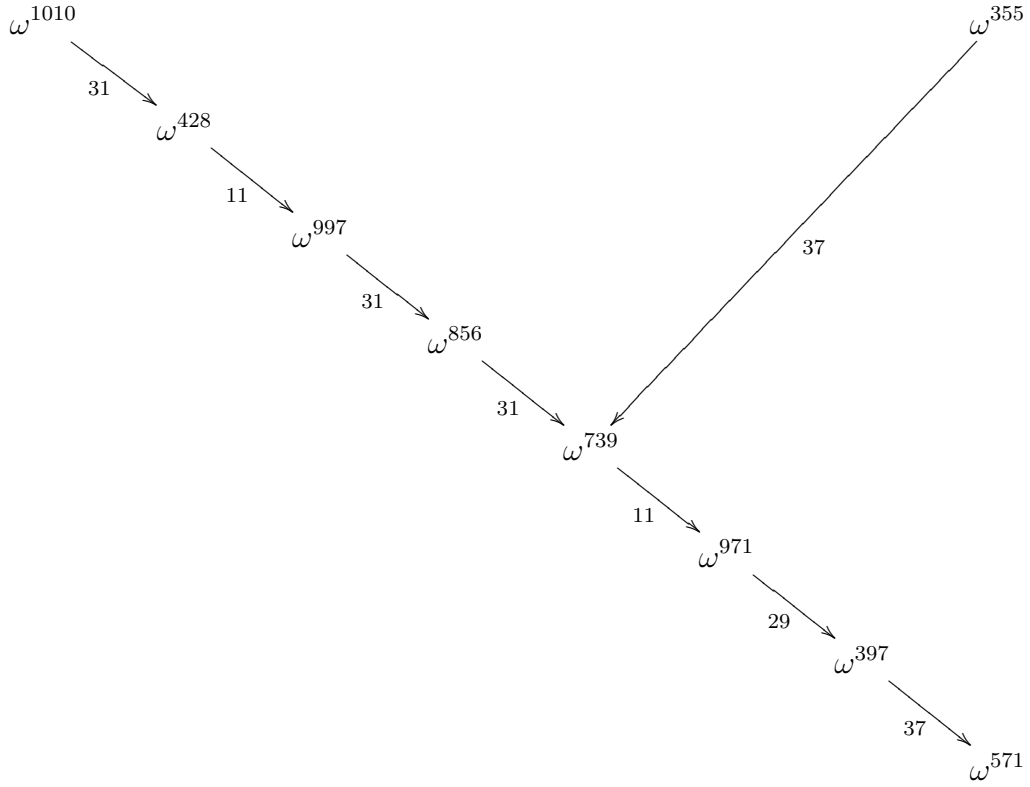
7.2 Beispiele

Wir geben noch zwei Beispiele an, um die Funktionsweise des Algorithmus zu verdeutlichen. Die Berechnungen fanden auf einem Prozessor des Typs AMD Athlon mit 1530 MHz statt.

7.3 Beispiel. Wir betrachten elliptische Kurven über $K = \mathbb{F}_{2^{10}}$, wobei K^* vom Element ω mit Minimalpolynom $x^{10} + x^6 + x^5 + x^3 + x^2 + x + 1$ erzeugt wird. Die verwendeten Kurven sind $E_1 : y^2 + xy = x^3 + \omega^{13}$ und $E_2 : y^2 + xy = x^3 + \omega^{668}$. Es gilt: $\#E_1(K) = \#E_2(K) = 998$, die beiden Kurven sind also K-isogen. Die Endomorphismenringe von E_1 und E_2 haben denselben Führer. Wir berechnen auch gleich noch die j-Invarianten der Kurven und die Picard-Zahl der Endomorphismenringe, um die Länge unseres Random-Walks auf der Picardgruppe zu erhalten.

```
kash% K:=GF(2,10);;
kash% w:=K.1;;
kash% E1:=EllipticCurve(K,[1,0,0,0,w^13]);
EllipticCurve over Finite field of size 2^10 defined by
 y^2 + 1*x*y  = x^3 + K.1^13
kash% E2:=EllipticCurve(K,[1,0,0,0,w^668]);
EllipticCurve over Finite field of size 2^10 defined by
 y^2 + 1*x*y  = x^3 + K.1^668
kash% Size(E1);
988
kash% Size(E2);
988
kash% O:= EndRing(E1);
Equation Order with defining polynomial X^2 - 39*X + 1062 over Z
kash% EndRing(E2);
Equation Order with defining polynomial X^2 - 39*X + 1062 over Z
kash% Conductor(O);
3
kash% jInvariant(E1);
K.1^1010
kash% jInvariant(E2);
K.1^355
kash% h:= PicardNumber(O);
40
kash% Ceiling(Sqrt(h));
7
```

Das Suchen nach einer pseudozufälligen Funktion auf den j-Invarianten in der Isogenieklasse von E_1 und E_2 ergibt folgenden Weg zwischen E_1 und E_2:



Die Zahl neben den Pfeilen gibt den Grad der entsprechenden Isogenie an. Die Grade auf dem gemeinsamen Weg sind dieselben, da die pseudozufällige Funktion auch den Grad der als nächstes zu berechnenden Isogenie vorgibt. Würden wir nun diese Isogenien berechnen und verketten, so würden sich die Grade multiplizieren. Das Resultat wäre also eine Isogenie vom Grad 1689134782544033. Mit der in 6.8 beschriebenen Methode wandeln wir jede Isogenie (welche auch nicht explizit berechnet, sondern nur durch Grad und Eigenwert des Frobenius auf dem Kern beschrieben wird) sofort in ein Ideal des Endomorphismenrings $\mathcal{O} = (1, \omega')$ um, welches wir dann mittels der in 6.7 beschriebenen Methode in ein reduziertes Ideal umwandeln. Die resultierenden Ideale werden multipliziert und am Ende noch einmal reduziert. In unserem Fall ergibt sich das Ideal

$$\begin{aligned} I &= 26\mathcal{O} + (15 + \omega')\mathcal{O} \\ &= (2\mathcal{O} + (1 + \omega')\mathcal{O}) \cdot (13\mathcal{O} + (2 + \omega')\mathcal{O}) \end{aligned}$$

Zwischen E_1 und E_2 gibt es also eine Isogenie vom Grad 26, welche eine Verkettung einer Isogenie vom Grad 2 (mit Eigenwert 1 des Frobenius auf dem Kern) und einer Isogenie vom Grad 13 (mit Eigenwert 2 des Frobenius auf dem Kern)

ist. Wir geben nur die x-Komponente explizit an: $\varphi : E_1 \to E_2, \varphi := (\varphi_x, \varphi_y)$ mit

$$\varphi_x = \frac{x^{26} + \omega^{1010}x^{22} + \omega^{991}x^{18} + \omega^{240}x^{14} + \omega^{655}x^{10} + \omega^{146}x^6 + \omega^{750}x^2}{x^{24} + \omega^{445}x^{20} + \omega^{980}x^{16} + \omega^{591}x^{12} + \omega^{345}x^8 + \omega^{390}x^4 + \omega^{429}}$$

Alle diese Schritte werden durch die KASH3-Funktion FindIso(E_1, E_2) hintereinander ausgeführt. Die Berechnung benötigte insgesamt 193 Sekunden.

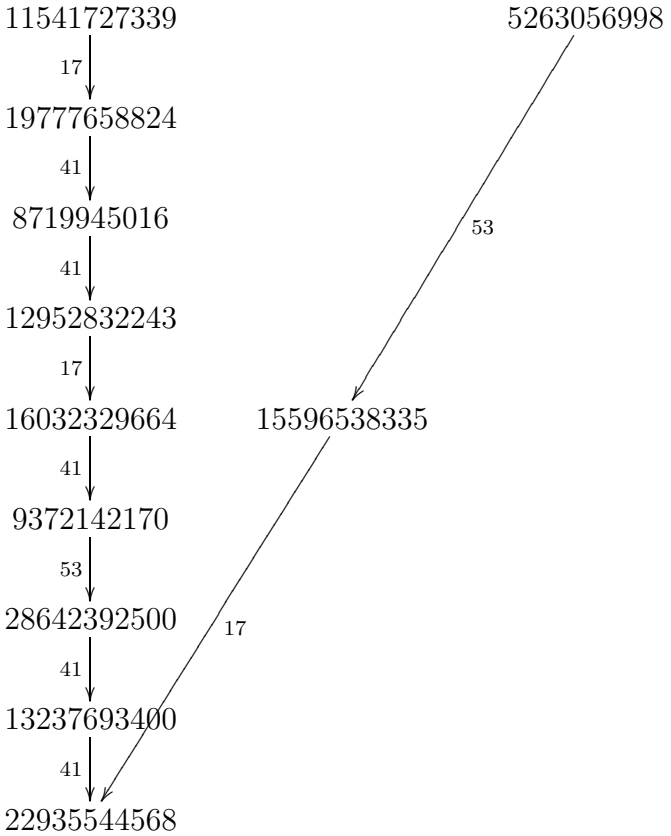
7.4 Beispiel. Als zweites Beispiel betrachten wir Kurven über $\mathbb{F}_p$ mit $p = 34463364647$. Es sind

$$E_1 : y^2 = x^3 + 235125x + 362$$

und

$$E_2 : y^2 = x^3 + 3349435905x + 3643865783$$

mit $\#E_1(\mathbb{F}_p) = \#E_2(\mathbb{F}_p) = 34463264753$ und $j(E_1) = 11541727339$, $j(E_2) = 5263056998$. Für beide Kurven ist der Endomorphismenring die Maximalordnung $\mathcal{O}_F$ mit Basis $(1, \omega)$. Die pseudozufällige Funktion ergibt folgenden Weg von E_1 nach E_2:



Das reduzierte Ideal, welches zur Verkettung dieser Isogenien gehört, ist

$697\mathbb{Z} + (122 + \omega)\mathbb{Z} = (17\mathbb{Z} + (3 + \omega)\mathbb{Z})(41\mathbb{Z} + (40 + \omega)\mathbb{Z})$, unser Algorithmus berechnet also eine Isogenie vom Grad 697 zwischen E_1 und E_2. Die Berechnung der Isogenie benötigte 342 Sekunden.

Dokumentation der verwendeten KASH3-Funktionen

Alle hier verwendeten elliptischen Kurven sind immer als elliptische Kurven über einem endlichen Körper zu verstehen.

- Ceiling(r)
  - Input: relle Zahl r
  - Output: $n \in \mathbb{N}$ mit $n \geq r$
- CharacteristicFrobeniusPolynomial(E)
  - Input: elliptische Kurve E über $\mathbb{F}_q$
  - Output: das charakteristische Polynom $x^2 - tx + q$ des Frobenius-Endomorphismus von E
- Codomain(f)
  - Input: Abbildung $f : A \to B$
  - Output: der Wertebereich B
- Conductor($\mathcal{O}$)
  - Input: Ordnung $\mathcal{O}$ in einem Zahlkörper F
  - Output: $k \in \mathbb{Z}$ mit $\mathcal{O} = \mathbb{Z} + k\mathcal{O}_F$
- ElkiesPrimes(E)
  - Input: E elliptische Kurve über einem endlichen Körper
  - Output: Liste der Elkies-Primzahlen von E
- EllipticCurve($K, [a, b]$)
  - Input: K endlicher Körper, $[a, b]$ Liste mit Elementen aus $\mathbb{Z}$ oder K
  - Output: elliptische Kurve $y^2 = x^3 + ax + b$ über K, falls diese Kurve nicht-singulär ist, sonst ERROR

- EllipticCurve($K, [a_1, a_3, a_2, a_4, a_6]$)
  - Input: K endlicher Körper, $[a_1, a_3, a_2, a_4, a_6]$ Liste mit Elementen aus $\mathbb{Z}$ oder K
  - Output: elliptische Kurve $y^2 + a_1y + a_3xy = x^3 + a_2x^2 + a_4x + a_6$ über K, falls diese Kurve nicht-singulär ist, sonst ERROR

- EndRing(E)
  - Input: elliptische Kurve E
  - Output: Endomorphismenring der elliptischen Kurve E als Ordnung in einem imaginärquadratischen Zahlkörper, falls der Führer von $\mathbb{Z}[\pi] < 60$, sonst ERROR

- EquationOrder(f)
  - Input: Polynom f über $\mathbb{Z}$
  - Output: Gleichungsordnung von f

- FindIso(E_1, E_2)
  - Input: E_1, E_2 isogene elliptische Kurven
  - Output: Isogenie $\varphi : E_1 \to E_2$ oder ERROR

- FrobeniusEigenvalue(f)
  - Input: Isogenie f, welche mithilfe der Funktion IsogenyFromJInvariant erzeugt wurde
  - Output: der Eigenwert λ des Frobenius der Ausgangskurve auf der Untergruppe im Kern von f

- GF(p, r)
  - Input: p Primzahl, $r \in \mathbb{N}$
  - Output: endlicher Körper mit p^r Elementen

- IdealFactorization(I)
  - Input: Ideal I einer Ordnung $\mathcal{O}$ eines Zahlkörpers
  - Output: Faktorisierung von I oder FAILURE, falls I nicht teilerfremd zum Führer von $\mathcal{O}$ ist

- IdReduction(I)
  - Input: ein Ideal I in einem imaginärquadratischen Zahlkörper
  - Output: ein mithilfe von binären quadratischen Formen reduziertes Ideal I' mit $I \sim I'$

- IsogenyFromJInvariant(E, ℓ, k)
  - Input: elliptische Kurve E, Elkies-Primzahl ℓ von E, $k \in \mathbb{Z}$
  - Output: Isogenie vom Grad ℓ von E nach E', berechnet mithilfe der Algorithmen aus 6.4. Die Zielkurve E' hat als j-Invariante die k-te Nullstelle von $\Psi_\ell(j(E), x)$.

- jInvariant(E)
  - Input: elliptische Kurve E
  - Output: j-Invariante von E

- PicardNumber($\mathcal{O}$)
  - Input: $\mathcal{O}$ Ordnung eines Zahlkörpers
  - Output: die Picardzahl $h_\mathcal{O}$

- Size(E)
  - Input: über dem endlichen Körper K definierte elliptische Kurve
  - Output: die Anzahl der Punkte in $E(K)$

- Sqrt(r)
  - Input: relle Zahl r
  - Output: die Wurzel aus r

Symbole

$\mathbb{A}^n(K)$	n-dimensionaler affiner Raum über K	1
V/K	über K definierte affine Varietät	1
$I(V)$	Ideal einer Varietät	1
$K[V]$	affiner Koordinatenring einer über K definierten Varietät	1
$K(V)$	Funktionenkörper einer über K definierten Varietät	1
$\overline{K}[V]_P$	lokaler Ring an einem Punkt $P \in V/K$	2
$\mathbb{P}^n$	n-dimensionaler projektiver Raum über K	2
$V_{(f)}$	durch homogenes Primpolynom f definierte projektive Varietät	2
$V \cap \mathbb{A}^n$	affine Varität zu projektiver Varität V	3
$\overline{V}$	projektiver Abschluss einer affinen Varietät V	3
F/K	algebraischer Funktionenkörper über K in einer Variablen	4
v	Bewertung eines Funktionenkörpers	5
$\mathbb{P}_F$	Menge der Stellen eines Funktionenkörpers F/K	6
$\mathcal{D}_F$	Divisorengruppe eines Funktionenkörpers F/K	6
$\mathcal{L}(\mathcal{A})$	Riemann-Roch-Raum eines Divisors $A \in \mathcal{D}_F$	6
O	Punkt im Unendlichen einer elliptischen Kurve	7
$E(\widetilde{K})$	Punktgruppe einer elliptischen Kurve E/K über Erweiterungskörper $\widetilde{K}$ von K	8
$E[m]$	m-Torsionsuntergruppe einer elliptischen Kurve E	8
X, Y	Koordinatenabbildungen einer elliptischen Kurve	8
$\triangle(E)$	Diskriminante einer elliptischen Kurve E	10
$j(E)$	j-Invariante einer elliptischen Kurve E	10
φ^*	induzierte Funktionenkörperabbildung zu einer Isogenie	13
$\mathrm{End}(E)$	Endomorphismenring einer elliptischen Kurve E	14
π	Frobenius-Endomorphismus einer elliptischen Kurve	14
t	Spur des Frobenius-Endomorphismus	15
f_π	charakteristisches Polynom des Frobenius	15

$[m]$	Multiplikation-mit-m-Abbildung	15
f_m	m-tes Divisionspolynom	16
$\widehat{\varphi}$	duale Isogenie zu einer Isogenie φ	17
E^t	quadratischer Twist einer elliptischen Kurve E	21
Ψ_n	n-tes modulares Polynom	24
F	Zahlkörper	25
$Cl(\mathbb{Z}, F)$	Ring der über $\mathbb{Z}$ ganzen Elemente von F	26
$\mathcal{O}_F$	Maximalordnung von F	26
$\mathcal{O}$	beliebige Ordnung eines Zahlkörpers	26
$\mathrm{Tr}(\alpha)$	Spur eines Zahlkörperelementes α	26
$\mathcal{N}(\alpha)$	Norm eines Zahlkörperelementes α	26
$\mathrm{disc}(\mathcal{O})$	Diskriminante der Ordnung $\mathcal{O}$	26
c	Führer einer Ordnung	28
$\mathfrak{F}$	Führerideal einer Ordnung	29
$[\mathfrak{a}/\mathfrak{a}]$	Multiplikatorring des Ideals $\mathfrak{a}$	29
$\mathcal{N}(\mathfrak{a})$	Norm des Ideal $\mathfrak{a}$	30
$I_F(c)$	ganze Ideale eines Zahlkörpers F, welche prim zu c sind	33
$I_{\mathcal{O}}(c)$	ganze Ideale einer Ordnung $\mathcal{O}$, welche prim zu c sind	33
$I_{\mathcal{O}}$	invertierbare Ideale einer Ordnung $\mathcal{O}$	34
$P_{\mathcal{O}}$	Hauptideale einer Ordnung $\mathcal{O}$	34
$Pic(\mathcal{O})$	Picardgruppe einer Ordnung $\mathcal{O}$	34
$Cl(F)$	Klassengruppe eines Zahlkörpers F	34
$h_{\mathcal{O}}$	Picardzahl einer Ordnung $\mathcal{O}$	34
h_F	Klassenzahl eines Zahlkörpers F	34
$M_{\mathcal{O}}$	Minkowski-Schranke einer Ordnung $\mathcal{O}$	35
Λ	Gitter in $\mathbb{C}$	37
$\wp$	Weierstrass-Funktion zu einem Gitter Λ	38
E_Λ	elliptische Kurve zu einem Gitter Λ	39
$\mathcal{ELL}(\mathcal{O})$	Isomorphieklassen elliptischer Kurven mit Endomorphismenring $\mathcal{O}$	42
$\mathcal{O}_{\mathfrak{p}}$	Lokalisierung von $\mathcal{O}$ an $\mathfrak{p}$	43
$\overline{E}$	Reduktion der elliptischen Kurve $E/\mathbb{C}$	43
$\overline{\varphi}$	Reduktion der Isogenie φ	44
(α, β, γ)	binäre quadratische Form	71
$\mathcal{F}^+(D)$	Äquivalenzklassen positiv definiter binärer quadratischer Formen der Diskriminante D	71
$\phi_{IF}(\mathfrak{a})$	Abbildung, welche Ideal $\mathfrak{a}$ in binäre quadratische Form umwandelt	72
$\phi_{FI}(\alpha, \beta, \gamma)$	Abbildung, welche binäre quadratische Form in ein Ideal umwandelt	74
$E[\mathfrak{a}]$	Torsionsgruppe der elliptischen Kurve E bezüglich eines Ideals $\mathfrak{a}$	77

Literaturverzeichnis

[Bos92] S. Bosch, *Algebra*, Springer-Verlag, Berlin-Heidelberg-New York, 1992.

[BSME06] A. Bostan, B. Salvy, F. Morain, and E.Schost, *Fast algorithms for computing isogenies between elliptic curves.*

[BSS99] I. Blake, G. Seroussi, and N. Smart, *Elliptic curves in cryptography*, LMS Lecture Notes Series 265, Cambridge University Press, Cambridge, 1999.

[Cha04] D. Charles, *The characteristic polynomial of frobenius and the isogeny class of an elliptic curve.*

[Coh96] H. Cohen, *A course in algebraic number theory*, 3rd corr. printing, GTM 138, Springer-Verlag, Berlin-Heidelberg-New York, 1996.

[FM02] M. Fouquet and F. Morain, *Isogeny volcanoes and the SEA algorithm*, Algorithmic number theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 276–291.

[Gal99] S. Galbraith, *Constructing isogenies between elliptic curves over finite fields*, LMS J. Comput. Math. **2** (1999), 118–138.

[GHS02a] S. Galbraith, F. Hess, and N. P. Smart, *Extending the GHS Weil descent attack*, Advances in Cryptology - EUROCRYPT 2002 (Amsterdam) (L. R. Knudsen, ed.), LNCS 2332, Springer-Verlag, Berlin-Heidelberg-New York, 2002, pp. 29–44.

[GHS02b] P. Gaudry, F. Hess, and N. P. Smart, *Constructive and destructive facets of Weil descent on elliptic curves*, J. Cryptology **15** (2002), no. 1, 19–46.

[Hen02] M. Henningsen, *Zur Berechnung von Endomorphismenringen von elliptischen Kurven über endlichen Körpern*, MSc Thesis, Technische Universität Berlin, 2002.

[Hes04] F. Hess, *Einführung in die Algebra Teil II*, 2004.

[Jan96] G. J. Janusz, *Algebraic number fields*, second ed., Graduate Studies in Mathematics, vol. 7, American Mathematical Society, Providence, RI, 1996.

[Koh96] D. R. Kohel, *Endomorphism rings of elliptic curves over finite fields*, PhD Thesis, University of California, Berkeley, 1996.

[KP03] J. Klüners and S. Pauli, *Computing residue class rings and Picard groups of arbitrary orders*, submitted to IMRN, 2003.

[Lan70] S. Lang, *Algebraic number theory*, Addison-Wesley Publishing Co., Inc., Reading, Mass.-London-Don Mills, Ont., 1970.

[Lan73] ———, *Elliptic functions*, Addison-Wesley Publishing Company, Reading, Massachusetts, 1973.

[Ler96] R. Lercier, *Computing isogenies in* $\mathbf{F}_{2^n}$, Algorithmic number theory (Talence, 1996), Lecture Notes in Comput. Sci., vol. 1122, Springer, Berlin, 1996, pp. 197–212.

[LM98] R. Lercier and F. Morain, *Algorithms for computing isogenies between elliptic curves*, Computational perspectives on number theory (Chicago, IL, 1995), AMS/IP Stud. Adv. Math., vol. 7, Amer. Math. Soc., Providence, RI, 1998, pp. 77–96.

[Mül95] V. Müller, *Ein Algorithmus zur Bestimmung der Punktanzahl elliptischer Kurven über endlichen Körpern der Charakteristik größer drei*, PhD Thesis, Universität des Saarlandes, Saarbrücken, 1995.

[Neu99] J. Neukirch, *Algebraic number theory*, Springer-Verlag, Berlin-Heidelberg-New York, 1999.

[Poh93] M. E. Pohst, *Computational algebraic number theory*, DMV-Seminar 21, Birkhäuser Verlag, Basel-Boston-Berlin, 1993.

[PZ97] M. E. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*, 1st paperback ed., Cambridge University Press, Cambridge, 1997.

[Sch95] R. Schoof, *Counting points on elliptic curves over finite fields*, J. Théor. Nombres Bordeaux **7** (1995), no. 1, 219–254, Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993).

[Sil86] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, Berlin-Heidelberg-New York, 1986.

[Sil94] ———, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR MR1312368 (96b:11074)

[ST68] J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517.

[Ste05] P. Stevenhagen, *Number rings*, 2005.

[Sti93] H. Stichtenoth, *Algebraic function fields and codes*, Springer-Verlag, Berlin-Heidelberg-New York, 1993.

[SZ03] S. Schmitt and H. G. Zimmer, *Elliptic curves*, de Gruyter Studies in Mathematics, vol. 31, Walter de Gruyter & Co., Berlin, 2003, A computational approach, With an appendix by Attila Pethö.

[Tat66] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144.

[Vél71] J. Vélu, *Isogénies entre courbes elliptiques*, C. R. Acad. Sci. Paris Sér. A-B **273** (1971), A238–A241.

[Ver99] F. Vercauteren, *Het aantal punten op elliptische krommen over eindige velden van karakteristiek 2*, MSc Thesis, K.U.Leuven, 1999.

[Wil93] K. Wildanger, *Konstruktive Zahlentheorie*, 1993.