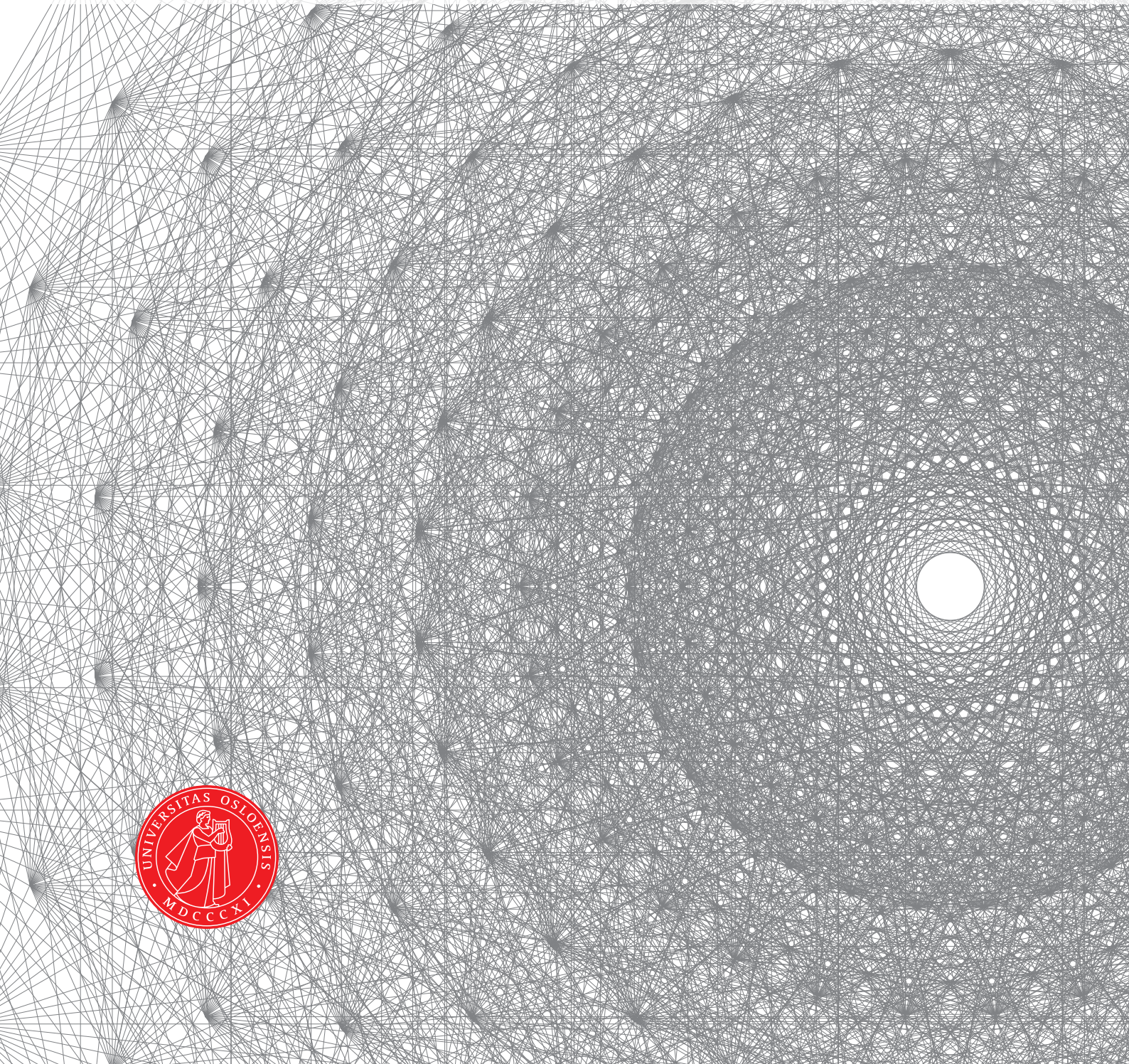
UiO : Department of Mathematics
University of Oslo

Isogenies between Hessian curves

Ella Wolff Kristensen

Master's Thesis, Spring 2022



This master's thesis is submitted under the master's programme *Mathematics*, with programme option *Mathematics*, at the Department of Mathematics, University of Oslo. The scope of the thesis is 60 credits.

The front page depicts a section of the root system of the exceptional Lie group E_8, projected into the plane. Lie groups were invented by the Norwegian mathematician Sophus Lie (1842–1899) to express symmetries in differential equations and today they play a central role in various parts of mathematics.

Abstract

Elliptic curves are used in post-quantum cryptography, where two parties can use compositions of low-degree isogenies to establish a shared secret. There are several forms for representing elliptic curves, and different forms require different isogeny formulas. This thesis is concerned with the Hessian form of elliptic curves, and explicit formulas for isogenies between these. A formula for n-isogenies between Hessian curves has recently been found for $n \neq 0 \mod 3$ [Bro+21]. We derive a new formula for 3-isogenies between Hessian curves. We also derive new formulas for 2- and 4-isogenies that results in a simpler formula for the latter case, compared to [Bro+21]. We find that any representative for 2-isogenies must have indeterminacies. We give a globally defined formula for morphisms that are 2-isogenies followed by translation with a 2-torsion point. In addition we describe how such morphisms can be used to construct isogenies of degree 2^e for some positive integer e, similar to how 2-isogenies are used in cryptography to construct isogenies of degree 2^e.

Acknowledgements

I thank my supervisors, Kristian Ranestad and Martin Strand, for introducing me to isogeny-based cryptography and Hessian curves. I also thank Simen Westbye Moe for support while working with this thesis.

Contents

CHAPTER 1

Introduction

The research on quantum computers poses a threat to public key cryptosystems currently in use. Factoring large numbers and solving the discrete log problem is considered practically impossible for classical computers. Therefore these problems are widely used as primitives for public key cryptography today. In 1994 Peter Shor showed that a quantum computer could solve these problems efficiently. Since it is possible that a full scale quantum computer will exist in a few decades, it is necessary to prepare the digital communication systems worldwide to be secure against quantum computing. In 2016 the National Institute of Standards and Technology (NIST) initiated a process to standardize public key cryptography that is secure against attacks from both classical and quantum computers.

The candidate schemes in the NIST standardization process are based on different mathematical primitives. After three rounds in the "competition", the finalist public key encryption schemes are *lattice-based* (Kyber, NTRU and SABER) and *code-based* (Classic McEliece). An alternative finalist is the *isogeny-based* scheme SIKE. SIKE has small key and ciphertext sizes but is slower than the other finalists. In a summer project at FFI (the Norwegian Defence Research Establishment) we tested the performance of the NIST candidates on microcontrollers, and registered key sizes and time consumption for different levels of security [KES20]. It was clear that SIKE stood out as slow compared to the other candidate schemes.

The SIKE scheme uses elliptic curves on Montgomery form and computes isogenies, which are special morphisms, between such curves. In particular, one computes high-degree isogenies as a composition of isogenies of degree 2, 3 and 4. Isogeny computations make up a large part of the SIKE algorithm. It is therefore interesting to look at other alternatives for representing elliptic curves, and possibly find more efficient isogeny formulas.

We will mainly focus on the Hessian form of elliptic curves in this thesis. Hessian curves are closely related to the representation theory of a special group, namely the Heisenberg group H_3. Explicit formulas for the multiplication-by-n isogeny on elliptic curves on Hessian form was found in [Fri02]. When $n \neq 0 \mod 3$ this isogeny can be viewed as a representation of H_3. When $n = 0 \mod 3$ the representations of H_3 also play an important role. The kernel of the isogeny is the group $E[n]$ of n-torsion points on the curve E. For cryptographic purposes, we are interested in isogenies that has a *subgroup* of $E[n]$ as kernel. Inspired by [Fri02], we started our search for such isogenies by looking at Hessian curves in the light of representation theory.

Our main contribution is new formulas for isogenies of degree 2, 3 and 4 between Hessian curves. More precicely, these are isogenies between Hessian curves where the kernels are cyclic subgroups of 2-, 3-, and 4-torsion points. In addition, we derive formulas for special morphisms of degree 2 and 3 between Hessian curves that are isogenies followed by a translation with a 2-torsion point or a 3-torsion point, respectively. We also give a description of how such morphisms can be used to construct isogenies with a specified kernel of order 2^e for some positive integer e.

In Chapter 2 we give a brief introduction to algebraic geometry. We define affine and projective varieties, and focus on varieties of dimension 1, namely curves. We include some useful results about curves and maps between them.

In Chapter 3 we introduce elliptic curves, and describe important properties of these, including the group structure on an elliptic curve. Furthermore we introduce isogenies, which are morphisms between elliptic curves preserving the group structure. At the end we present the Hesse pencil, and the Hessian form of elliptic curves.

In Chapter 4 we give a brief overview of how elliptic curves and isogenies are used in post-quantum cryptography. In cryptography we typically consider elliptic curves defined over a finite field. Elliptic curves over finite fields are either *ordinary* or *supersingular*. We describe some properties of supersingular curves that are useful for cryptographic purposes. We describe the SIDH (Supersingular Isogeny Diffie-Hellman) algorithm, and also how e isogenies of degree l can be used to construct an isogeny of degree l^e having a specific subgroup as kernel.

In Chapter 5 we introduce representation theory, and focus on the group action of the Heisenberg group H_3 and a particular action of the alternating group A_4 on the Hesse pencil. Given a Hessian curve, we describe how A_4 can be used to find all the other isomorphic curves on Hessian form. Furthermore, we find all the irreducible representations of H_3. We show that the multiplication-by-n isogeny from [Fri02] is a 3-dimensional representation of the Heisenberg group when $n \neq 0 \mod 3$. We will also see that the 1-dimensional representations of H_3 appear in the multiplication-by-3 isogeny.

In Chapter 6 we derive new formulas for isogenies of degree 2, 3 and 4 between Hessian curves. First we give the new formula for isogenies of degree 3, which we found using the 1-dimensional representations of H_3. Then we present a formula for isogenies of degree $n \neq 0 \mod 3$ between *twisted* Hessian curves found in [Bro+21]. This formula can be restricted to isogenies between Hessian curves, but we find that there are simpler representatives of these isogenies. In particular, we derive new formulas for isogenies of degree 2 and 4. These formulas give many representatives of the same isogeny, and results in simpler representatives when $n = 4$.

In Chapter 7 we derive a formula for morphisms between Hessian curves that are 2-isogenies followed by translation with a 2-torsion point. This morphism can be viewed as a 3-dimensional representation of H_3. Furthermore we describe how we think this formula can be generalized to all $n \neq 0 \mod 3$. We also give a formula for morphisms between Hessian curves that are 3-isogenies followed by a translation with a 3-torsion point. In addition we describe an algorithm to construct a 2^e-isogeny having a certain cyclic subgroup of order 2^e as kernel, using e morphisms of degree 2 and a single translation.

Many of the computations are done in [Macaulay2], which is a software system developed for algebraic geometry and commutative algebra. We will use [Macaulay2] as a tool for doing computations that are not suitable to do by hand. The [Macaulay2] code can be found in Appendix B.

PART I

Background

CHAPTER 2

Varieties

We begin with a brief overview of the theory that we need in order to study elliptic curves and isogenies. We first introduce affine and projective varieties. Then we focus on 1-dimensional varieties, namely curves, and we give some general properties about curves and maps between them.

2.1 Affine varieties

Let K be a field, and $\overline{K}$ an algebraic closure of K. The **affine n-space** is defined as $\mathbb{A}^n = \{(a_1, \ldots, a_n) : a_i \in \overline{K}\}$. Given an ideal $\mathfrak{a} \subseteq \overline{K}[x_1, \ldots, x_n]$ we define the **zero set** $Z(\mathfrak{a}) \subseteq \mathbb{A}^n$ by

$$Z(\mathfrak{a}) = \{(x_1, \ldots, x_n) \in \mathbb{A}^n \mid f(x_1, \ldots, x_n) = 0 \ \forall f \in \mathfrak{a}\}.$$

The zero sets satisfy the axioms for being the closed sets of a topology. This topology is called the **Zariski topology** on $\mathbb{A}^n$.

Definition 2.1.1. A set $V \subseteq \mathbb{A}^n$ is called an **affine variety** if there is an ideal $\mathfrak{a} \subseteq \overline{K}[x_1, \ldots, x_n]$ such that $V = Z(\mathfrak{a})$.

On the other hand, if $V \subseteq \mathbb{A}^n$ is an affine variety, we can define an ideal $I(V) \subseteq \overline{K}[x_1, \ldots, x_n]$ by

$$f \in I(V) \iff f(p) = 0 \ \forall p \in V.$$

By the Nullstellensatz we have that the ideal $I(Z(\mathfrak{a}))$ is equal to the radical ideal $\sqrt{\mathfrak{a}}$, hence we get a bijection

$$\{\text{Affine varieties } V \subseteq \mathbb{A}^n\} \leftrightarrow \{\text{Radical ideals } \mathfrak{a} \subseteq \overline{K}[x_1, \ldots, x_n]\}.$$

We say that V is **irreducible** if it cannot be written as $V_1 \cup V_2$ where V_1, V_2 are closed, proper, non-empty subsets of V.

Definition 2.1.2. An affine variety $V \subseteq \mathbb{A}^n$ is **defined over a field** $L \subseteq \overline{K}$, denoted V/L, if there exists $f_1, \ldots, f_n \in L[x_1, \ldots, x_n]$ such that $I(V) = (f_1, \ldots, f_n)$.

In other words, an affine variety V is defined over L if we can describe the points in V as solutions to polynomial equations $f_1, \ldots, f_n$ with coefficients in L. If $V \subseteq \mathbb{A}^n$ is an affine variety, we define the **coordinate ring** as

$$A(V) = \overline{K}[x_1, \ldots, x_n] \big/ I(V).$$

This is a finitely generated $\overline{K}$-algebra without nilpotents. A polynomial in $\overline{K}[x_1, \dots, x_n]$ induces a map $\mathbb{A}^n \to \overline{K}$, so the maps induced by $f_1, f_2 \in \overline{K}[x_1, \dots, x_n]$ restrict to the same map $V \to \overline{K}$ if and only if $f_1 - f_2 \in I(V)$. Thus elements of $A(V)$ correspond to polynomial maps $V \to \overline{K}$.

The **function field** $\overline{K}(V)$ of an irreducible affine variety V is defined as $\overline{K}(V) = \operatorname{Frac}(A(V))$. Elements in $\overline{K}(V)$ are called **rational functions** on V. Given $f \in \overline{K}(V)$ and a point $p \in V$ we say f is **regular at** p if we can write $f = \frac{g}{h}$ where $g, h \in A(V)$ and $h(p) \neq 0$. A **rational map** $\phi \colon V \dashrightarrow W \subset \mathbb{A}^m$ between affine varieties is defined as

$$\phi = (f_1, \dots, f_m),$$

where f_i are rational functions on V. The map is defined in the set of points where all f_i are regular, which is an open set. A dashed arrow is used to indicate that a rational map is not necessarily defined everywhere. A rational map regular at all points is called a **morphism**.

Definition 2.1.3. Let $\phi \colon V_1 \to V_2$ be a morphism between affine varieties. The **pullback** is defined as

$$\begin{aligned} \phi^* \colon A(V_2) &\to A(V_1) \\ f &\mapsto f \circ \phi. \end{aligned}$$

There is a $1-1$ correspondence $V \leftrightarrow A(V)$ between affine varieties and finitely generated $\overline{K}$-algebras without nilpotents, in fact it is an *equivalence of categories*. We will freely switch between the geometric and the algebraic side, the latter being more convenient for computations.

Proposition 2.1.4. *Let $\phi \colon V \to \mathbb{A}^m$ be a morphism between affine varieties. Then $\overline{\operatorname{im}\phi} = Z(\ker \phi^*)$.*

Proof. We consider the diagram

$$V \xrightarrow{\quad} \overline{\operatorname{im}\phi} \hookrightarrow \mathbb{A}^m, \qquad V \xrightarrow{\ \phi\ } \mathbb{A}^m$$

where the map $V \to \overline{\operatorname{im}\phi}$ is dominant. Then we get the corresponding maps between the coordinate rings.

$$A(V) \xleftarrow[\alpha]{} A(\overline{\operatorname{im}\phi}) \xleftarrow[\beta]{} A(\mathbb{A}^m), \qquad A(V) \xleftarrow{\ \phi^*\ } A(\mathbb{A}^m)$$

It suffices to show that $\ker\beta = \ker\phi^*$. Let $f \in \ker\beta$. Because α is a ring homomorphism we have $\alpha(\beta(f)) = \alpha(0) = 0$, so $f \in \ker\phi^*$. On the other hand, let $g \in \ker\phi^*$. Then $0 = \phi^*(g) = \alpha(\beta(g))$. And since α is injective $\beta(g)$ must be 0, thus $g \in \ker\beta$. This shows that $\ker\beta = \ker\phi^*$, and we have

$$A(\mathbb{A}^m)/_{\ker\phi^*} = A(\mathbb{A}^m)/_{\ker\beta} \simeq A(\overline{\operatorname{im}\phi}),$$

which means that $\overline{\operatorname{im}\phi} = Z(\ker\phi^*)$. ∎

One can construct general varieties by gluing together affine ones. For us it will suffice to consider projective varieties.

2.2 Projective varieties

The **projective n-space** is defined as

$$\mathbb{P}^n = \mathbb{A}^{n+1} \setminus \mathbf{0}/\sim$$

where $\sim$ is the equivalence relation defined by $(x_0, \ldots, x_n) \sim (\lambda x_0, \ldots, \lambda x_n)$ for $\lambda \in \overline{K} \setminus 0$. Homogeneous coordinates are denoted by $(x_0 : \cdots : x_n)$. The projective n-space $\mathbb{P}^n$ is given the quotient topology induced from the Zariski topology on $\mathbb{A}^{n+1}$. Given a homogeneous ideal $\mathfrak{a} \subseteq \overline{K}[x_0, \ldots, x_n]$ we define the **zero set** $Z_+(\mathfrak{a}) \subseteq \mathbb{P}^n$ by

$$Z_+(\mathfrak{a}) = \{(x_0 : \cdots : x_n) \in \mathbb{P}^n \mid f_i(x_0, \ldots, x_n) = 0 \ \forall f_i \in \mathfrak{a}\}.$$

Definition 2.2.1. A subset of $\mathbb{P}^n$ of the type $Z_+(\mathfrak{a})$ is called a **projective variety**.

On the other hand, if $V \subseteq \mathbb{P}^n$ is a projective variety, we define the ideal $I(V) \subseteq \overline{K}[x_0, \ldots, x_n]$ as the ideal generated by homogeneous $f \in \overline{K}[x_0, \ldots, x_n]$ such that $f(p) = 0$ for all $p \in V$.

Definition 2.2.2. We say that a projective variety V is **defined over a field** $L \subseteq \overline{K}$, denoted V/L, if $I(V)$ can be generated by homogeneous polynomials in $L[x_0, \ldots, x_n]$.

If V is a projective variety defined over a field $L \subseteq \overline{K}$, we say that the **L-rational points of** V, denoted $V(L)$, is the set

$$V(L) = \{(p_0 : \cdots : p_n) \in V \ : \ p_i \in L \ \text{ for } i = 0, \ldots, n\}.$$

For a projective variety $V \subset \mathbb{P}^n$ we define the **homogeneous coordinate ring**

$$S(V) = \overline{K}[x_0, \ldots, x_n]/I(V).$$

Note that this depends on the choice of embedding $V \subset \mathbb{P}^n$. Elements $F \in S(V)$ do not define maps $F \colon V \to \overline{K}$. This is because homogeneous coordinates are only defined up to scaling, and the only polynomials $F \in S(V)$ that satisfy $F(p_0, \ldots, p_n) = F(\lambda p_0, \ldots, \lambda p_n)$ for all λ are the constants. If F is homogeneous of degree n then

$$F(\lambda p_0, \ldots, \lambda p_n) = \lambda^n F(p_0, \ldots, p_n).$$

If $G \in S(V)$ is another homogeneous polynomial of degree n, then

$$\frac{F(\lambda p_0, \ldots, \lambda p_n)}{G(\lambda p_0, \ldots, \lambda p_n)} = \frac{\lambda^n F(p_0, \ldots, p_n)}{\lambda^n G(p_0, \ldots, p_n)} = \frac{F(p_0, \ldots, p_n)}{G(p_0, \ldots, p_n)},$$

so $\frac{F}{G}$ induces a well defined map where $G \neq 0$.

Definition 2.2.3. Let $V \subset \mathbb{P}^n$ be a projective variety and let $\mathrm{Frac}(S(V))$ be the fraction field of $S(V)$. The **function field** of V is defined as

$$K(V) = \left\{ \frac{F}{G} \in \mathrm{Frac}(S(V)) \mid F, G \in S(V) \text{ homogeneous of the same degree} \right\}.$$

Example 2.2.4. Let $V = \mathbb{P}^1$. Then

$$K(\mathbb{P}^1) = \left\{ \frac{F(x,y)}{G(x,y)} \ : \ f, g \in \overline{K}[x,y] \text{ homogeneous of the same degree} \right\}$$

is isomorphic to $\overline{K}(x)$. Define a homomorphism $K(\mathbb{P}^1) \to \overline{K}(x)$ by

$$\frac{F(x,y)}{G(x,y)} \mapsto \frac{f(x)}{g(x)} = \frac{F(x,1)}{G(x,1)}.$$

Since the map is non-constant between fields, it must be injective. It remains to show that it is surjective. Given an element $\frac{f(x)}{g(x)} \in \overline{K}(x)$, we find that

$$y^{\deg g - \deg f} \frac{y^{\deg f} f(\frac{x}{y})}{y^{\deg g} g(\frac{x}{y})} \in K(\mathbb{P}^1)$$

is mapped to $\frac{f(x)}{g(x)}$. Thus $K(\mathbb{P}^1) \simeq \overline{K}(x)$.

Let $V_1 \subseteq \mathbb{P}^m$ and $V_2 \subseteq \mathbb{P}^n$ be projective varieties. A **rational map** $\phi : V_1 \dashrightarrow V_2$ is defined by

$$\phi = (f_0 : \cdots : f_n)$$

where ϕ is defined on an open set in V. A rational map $\phi : V \dashrightarrow \mathbb{P}^n$ is **regular** in $p \in V$ if there exists a $g \in \overline{K}(V)$ such that $(gf_0(p) : \cdots : gf_n(p))$ is a well defined point in $\mathbb{P}^n$. Furthermore, if ϕ is regular in all points, then it is called a **morphism**.

We will consider projective varieties in $\mathbb{P}^2$ in this thesis. It is sometimes practical to go to an *affine chart* $\mathbb{A}^2 \subset \mathbb{P}^2$ by assuming that one of the variables is not equal to zero. Then we can do computations using affine coordinates, the affine coordinate ring, and so on.

Example 2.2.5. Let $p = (p_0 : p_1 : p_2)$ be a point in $\mathbb{P}^2$. Assume that $p_2 \neq 0$, so we can let

$$p = \left(\frac{p_0}{p_2} : \frac{p_1}{p_2} : 1 \right) = (p_0' : p_1' : 1)$$

and we can associate this point with the point (p_0', p_1') in $\mathbb{A}^2$. When we do this with every point where the z-coordinate is not zero, we say that we go to the *affine chart where* $z \neq 0$. Of course, we can do the same with $x \neq 0$ and $y \neq 0$. This means that $\mathbb{P}^2$ is covered by 3 affine charts $\mathbb{A}^2$. In general, $\mathbb{P}^n$ is covered in $n+1$ affine charts $\mathbb{A}^n$.

Remark 2.2.6. In Chapter 6 and Chapter 7 we work in the projective space $\mathbb{P}^2$, but the computations in [Macaulay2] are done in the affine space $\mathbb{A}^3 \setminus \mathbf{0}$. Recall that $\mathbb{P}^2 = {}^{\mathbb{A}^3 \setminus \mathbf{0}}\!/_{\sim}$, so in computations we do operations equivariant with respect to the equivalence relation. The following will be particularly useful. Let $\phi \colon V_1 \to V_2$ be a morphism between projective varieties, and $S(V_1), S(V_2)$ the homogeneous coordinate rings. From ϕ we obtain a pullback map $\phi^* \colon S(V_2) \to S(V_1)$ where $Z_+(\ker \phi^*) = \overline{\operatorname{im} \phi}$. In fact, morphisms between projective varieties are closed maps, so $\overline{\operatorname{im} \phi} = \operatorname{im} \phi$ [SR94, Theorem 5.2.1.10].

2.3 Curves

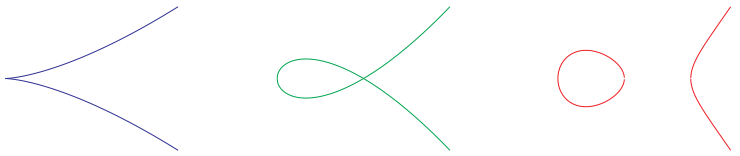
Definition 2.3.1. A **curve** is a variety of dimension 1.

A plane curve $C \subset \mathbb{P}^2$ is the zero set of one homogeneous polynomial $f \in \overline{K}[x, y, z]$, namely $Z_+(f)$. A point $p \in C$ is a **singular point** if

$$\frac{\partial f}{\partial x}(p) = \frac{\partial f}{\partial y}(p) = \frac{\partial f}{\partial z}(p) = 0.$$

A curve C is **singular** if it has singular points, and **non-singular** otherwise.

Example 2.3.2. The curve $Z_+(y^2z - x^3)$ is singular (with a *cusp*), the curve $Z_+(y^2z - x^3 - x^2z)$ is singular (with a *node*), and the curve $Z_+(y^2z - x^3 + 3x^2z - 2xz^2)$ is non-singular. In fact, the latter is a *Weierstrass* curve, which we will come back to later.



(a) A cusp. (b) A node. (c) A non-singular curve.

In this thesis we will consider rational maps between non-singular, irreducible and projective curves. The following proposition ensures us that such maps will always be morphisms.

Proposition 2.3.3 ([Sil09, Proposition II.2.1.])**.** *Let C be a non-singular, irreducible, projective curve, let $V \subseteq \mathbb{P}^n$ be an irreducible projective variety, and let $\phi\colon C \dashrightarrow V$ be a rational map. Then ϕ is a morphism.*

Furthermore, a non-constant morphism between irreducible, projective curves will always be surjective.

Proposition 2.3.4 ([Har77, Proposition II.6.8.])**.** *Let $\phi\colon C_1 \to C_2$ be a morphism between irreducible projective curves. Then ϕ is either constant or surjective.*

To any curve there is a fundamental invariant called the *genus*. For simplicity we only include the definition for plane curves.

Definition 2.3.5. Let $f \in \overline{K}[x_0, x_1, x_2]$ be a homogeneous polynomial of degree d defining a non-singular curve C in $\mathbb{P}^2$. The **genus** of C is

$$g(C) = \frac{(d-1)(d-2)}{2}.$$

In general, the genus of a curve C is defined as the dimension of the room of regular differentials. We omit the theory of divisors and differentials here.

Definition 2.3.6. Let $\phi : C_1 \to C_2$ be a non-constant morphism of irreducible non-singular curves, where $\phi = (g_0 : \cdots : g_n)$. Then the **pullback** $\phi^* : \overline{K}(C_2) \to \overline{K}(C_1)$ is defined by

$$\phi^*(f) = f(g_0, \ldots, g_n).$$

A non-constant morphism ϕ between curves must necessarily have finite *fibers* $\phi^{-1}(q)$. Most of these have the same size, which is the degree of the corresponding field extension.

Definition 2.3.7. If $\phi\colon C_1 \to C_2$ is a morphism of curves, then the **degree** of ϕ is defined as

$$\deg \phi = \begin{cases} 0 & \phi \text{ constant} \\ [\overline{K}(C_1) : \phi^*(\overline{K}(C_2))] & \text{otherwise.} \end{cases}$$

In general, the size of the fibers may vary. The morphisms that we will focus on (namely morphisms between non-singular irreducible curves of genus 1) will always have the same number of points in each fiber, and the degree will be equal to the number of such points.

Example 2.3.8. For $\phi = (x^n : 1)\colon \mathbb{P}^1 \to \mathbb{P}^1$ we have

$$\begin{aligned} \phi^*(K(\mathbb{P}^1)) &= \phi^*(\overline{K}(x)) \\ &= \overline{K}(x^n). \end{aligned}$$

Then

$$\begin{aligned} \deg \phi &= [K(\mathbb{P}^1) : \phi^*(K(\mathbb{P}^1))] \\ &= [\overline{K}(x) : \overline{K}(x^n)] \\ &= n. \end{aligned}$$

Recall that $\mathbb{P}^n$ is given the quotient topology induced from the Zariski topology on $\mathbb{A}^{n+1}$. In topology we say that a map ϕ between topological spaces is **continuous** if the inverse image of open (resp. closed) sets are open (resp. closed). We include a proposition that will be useful in Chapter 6 and Chapter 7.

Proposition 2.3.9. *Let $\phi\colon X \to Y$ be a surjective, continuous map between topological spaces. If X is irreducble, then so is Y.*

Proof. Assume for contradiction that Y is reducible, so Y can be written as $V_1 \cup V_2$ where V_1, V_2 are closed, proper, non-empty subsets of Y. Since ϕ is continuous, then

$$\begin{aligned} \phi^{-1}(Y) &= \phi^{-1}(V_1 \cup V_2) \\ &= \phi^{-1}(V_1) \cup \phi^{-1}(V_2), \end{aligned}$$

so $X = \phi^{-1}(V_1) \cup \phi^{-1}(V_2)$, where both $\phi^{-1}(V_1)$ and $\phi^{-1}(V_2)$ are closed. Since X is irreducible, either $\phi^{-1}(V_1)$ or $\phi^{-1}(V_2)$ (or both) is equal to X, a contradiction. ■

Finally, we include the well known theorem of Bezout.

Theorem 2.3.10 ([Har77, Corollary I.7.8.])**.** *Let $C_1, C_2 \subset \mathbb{P}^2$ be plane curves of degree d_1 and d_2 with no common components. Then $C_1 \cap C_2$ consists of $d_1 \cdot d_2$ points, counting multiplicities.*

CHAPTER 3

Elliptic curves and isogenies

Curves are often classified according to their genus g. The case $g = 1$ forms a special class of curves. The non-singular irreducible projective curves of genus 1 admit a group structure. In this chapter we introduce elliptic curves, and a certain type of morphisms between them called isogenies. These are morphisms that also preserve the group structure. At the end of this chapter we focus on elliptic curves on Hessian form, which are central objects to this thesis.

3.1 Elliptic curves

Definition 3.1.1. An **elliptic curve** is a pair $(E, \mathcal{O})$ where E is a non-singular irreducible projective curve with $g(E) = 1$ and $\mathcal{O}$ is a specified point on E.

An elliptic curve can be embedded into $\mathbb{P}^2$ as a *Weierstrass curve*, and conversely a Weierstrass curve is always an elliptic curve.

Theorem 3.1.2 ([Sil09, Proposition III.3.1.])**.** *Let E be an elliptic curve defined over a field K.*

1) *There exist functions $x, y \in K(E)$ such that the map*

$$\begin{aligned} \phi\colon E &\to \mathbb{P}^2 \\ p &\mapsto (x(p) : y(p) : 1) \end{aligned}$$

gives an isomorphism of E/K onto a curve given by a Weierstrass equation

$$C\colon y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

with coefficients $a_1, \ldots, a_6 \in K$, and such that $\phi(\mathcal{O}) = (0 : 1 : 0)$.

2) *Any two Weierstrass equations for E as in a) are related by a linear change of variables.*

3) *Conversely, every smooth cubic curve C given by a Weierstrass equation as in a) is an elliptic curve defined over K with origin $\mathcal{O} = (0 : 1 : 0)$.*

Remark 3.1.3. We will always assume that our elliptic curves are embedded in $\mathbb{P}^2$. To simplify notation, we often use the dehomogenized Weierstrass equation

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

to describe an elliptic curve.

If the characteristic of K is not equal to 2 or 3, we can make a change of variables to get the short Weierstrass form

$$y^2 - (x^3 + Ax + B) = 0.$$

There are several ways of representing elliptic curves, for instance using the Weierstrass, Hessian, Legendre, Huff or Montgomery form. They are useful in different contexts. Since there is a correspondence between elliptic curves and Weierstrass curves, we describe some important properties of elliptic curves using the short Weierstrass form, assuming that $\mathrm{char}(K) \neq 2, 3$. Later we will mainly focus on the Hessian form.

To any elliptic curve E we can associate its *j-invariant*, denoted $j(E)$. It can be defined using the short Weierstrass form.

Definition 3.1.4. Given a Weierstrass curve $E\colon y^2 = x^3 + Ax + B$, define the **$j$-invariant** as

$$j(E) = -1728\frac{(4A)^3}{-16(4A^3 + 27B^2)}.$$

The j-invariant has the following remarkable property.

Proposition 3.1.5 ([Sil09, Proposition III.1.4.(b).])**.** *Let E and E' be two elliptic curves defined over a field K. Then E and E' are isomorphic over $\overline{K}$ if and only if $j(E) = j(E')$.*

Example 3.1.6. Let

$$E_1 = Z(y^2 - x^3 - A_1x - B_1) = Z(y^2 - x^3 - x),$$
$$E_2 = Z(y^2 - x^3 - A_2x - B_2) = Z(y^2 - x^3 - 2x)$$

be two Weierstrass curves. These curves are isomorphic over $\overline{\mathbb{F}}_5$ because

$$j(E_1) = j(E_2) = 1728.$$

Furthermore, by [Sil09, p. 50] E_1 and E_2 are isomorphic over $\mathbb{F}_5$ if and only if there exists $u \in \mathbb{F}_5$ such that

$$A_2 = u^4A_1, \quad B_2 = u^6B_1.$$

Since $A_2 = 2A_1$, then $u^4 = 2 \mod 5$, which is impossible since $u^4 = 1 \mod 5$ for all non-zero $u \in \mathbb{F}_5$. Thus E_1 and E_2 are not isomorphic over $\mathbb{F}_5$.

3.2 The group law on elliptic curves

An elliptic curve forms a group under point addition. There are several ways to define this group law, for example via the theory of divisors. We will give the geometric definition of the group operation on elliptic curves. From this definition one can derive explicit formulas for point addition.

Let $(E, \mathcal{O})$ be an elliptic curve on Weierstrass form, where $\mathcal{O} = (0 : 1 : 0)$. If $l \in \mathbb{P}^2$ is a line, then by Bezout's theorem $l \cap E$ consists of three points (counted with multiplicities). Given two distinct points $p_1, p_2 \in E$ we write $l(p_1, p_2) \in \mathbb{P}^2$ for the unique line through p_1 and p_2. If $p_1 = p_2$ we let $l(p_1, p_2)$ be the tangent

line through p_1. As discussed, there is a third point p_3 in the intersection $l(p_1, p_2) \cap E$. We call this point $p_3 = T(p_1, p_2)$. We define an addition law $+$ on E by the following rule.

Definition 3.2.1. Let $p_1, p_2 \in E$, and $p_3 = T(p_1, p_2)$. Let l' be the line through p_3 and $\mathcal{O}$. Then define $p_1 + p_2$ to be the third point of intersection of l' with E.

This addition law defines a group operation on E:

Proposition 3.2.2 ([Sil09, Proposition III.2.2.])**.** *The addition law $+$ has the following properties.*

a) *If a line l intersects E at the (not necessarily distinct) points p_1, p_2, p_3 then $p_1 + p_2 + p_3 = \mathcal{O}$.*

b) *$p + \mathcal{O} = p$ for all $p \in E$.*

c) *$p + q = q + p$ for all $p, q \in E$.*

d) *Let $p \in E$. There is a point of E, denoted $-p$, so that $p + (-p) = 0$.*

e) *Let $p, q, r \in E$. Then $(p + q) + r = p + (q + r)$.*

In other words, the composition law makes E into an abelian group with identity element $\mathcal{O}$. We further have that if K is a field, the K-rational points $E(K)$ is a subgroup of E.

One can easily check that a)-d) holds directly by using the geometric definition. It is more complicated to verify that the operation is associative.

Example 3.2.3. Let $E = Z(y^2 - x(x-1)(x-2))$ be a Weierstrass curve, and let $p = (1, 0)$ and $q = (2, 0)$ be two points on E. We compute $p + q$ using the definition. To do so, we find the line $l(p, q)$ through these two points. The line is parameterized by

$$r(t) = tp + (1 - t)q = (t + 2(1 - t), 0),$$

which is the horisontal line $y = 0$. This line intersects E in the third point $(0, 0)$. Then

$$(1, 0) + (2, 0) = -(0, 0) = (0, 0).$$

Theorem 3.2.4 ([Sil09, Theorem III.3.6.])**.** *Let E be an elliptic curve defined over K. Then the group law on E define morphisms*

$$\begin{aligned} +\colon E \times E &\to E \\ (p_1, p_2) &\mapsto p_1 + p_2 \end{aligned}$$

and

$$\begin{aligned} -\colon E &\to E \\ p &\mapsto -p. \end{aligned}$$

Example 3.2.5. Let E be an elliptic curve defined over K, and let q be a point on E. We define the **translation-by-q** map

$$\begin{aligned} \tau_q \colon E &\to E \\ p &\mapsto p + q. \end{aligned}$$

This is a morphism by Theorem 3.2.4, in fact it is an isomorphism, with the inverse morphism being τ_{-q}.

Example 3.2.6. Let C be a curve with a singular point $p^* \in C$, and let q be a non-singular point on C. Suppose that C has a group structure, in particular the translation map

$$\begin{aligned} \tau_{p^*-q} \colon C &\to C \\ p &\mapsto p + (p^* - q) \end{aligned}$$

is an isomorphism. The non-singular point q is mapped to the singular point p^* through this isomorphism, a contradiction. This shows that singular curves cannot have a group structure.

3.3 Isogenies

Definition 3.3.1. Let E_1 and E_2 be elliptic curves. An **isogeny** between E_1 and E_2 is a morphism

$$\phi \colon E_1 \to E_2$$

satisfying $\phi(\mathcal{O}) = \mathcal{O}$.

By Proposition 2.3.4 we note that $\operatorname{im}\phi$ is either $\mathcal{O}$ or E_2. We define the zero isogeny by $[0](p) = \mathcal{O}$ for all $p \in E_1$. By the following proposition we have that isogenies are group homomorphisms.

Proposition 3.3.2 ([Sil09, Theorem III.4.8.])**.** *Let $\phi \colon E_1 \to E_2$ be an isogeny. Then $\phi(p_1 + p_2) = \phi(p_1) + \phi(p_2)$ for all $p_1, p_2 \in E_1$.*

Since isogenies are group homomorphisms the kernel of an isogeny is well defined.

Corollary 3.3.3 ([Sil09, Corollary III.4.9.])**.** *Let $\phi : E_1 \to E_2$ be a non-constant isogeny. Then $\ker\phi$ is a finite subgroup of E_1.*

In fact, every *fiber* $\phi^{-1}(q)$ of an isogeny is finite and contains the same number of points.

Proposition 3.3.4 ([Sil09, Theorem III.4.10.])**.** *The degree of a non-constant isogeny $\phi : E_1 \to E_2$ is the number of elements in the kernel, and $|\phi^{-1}(q)| = |\ker\phi|$ for all $q \in E_2$.*

Example 3.3.5. For each $n \in \mathbb{Z}$ we can define the **multiplication-by-n** isogeny

$$[n] \colon E \to E$$

in the following way. If $n > 0$ then

$$[n](p) = p + p + \cdots + p \ (n \text{ terms}).$$

If $n < 0$ then $[n](p) = [-n](-p)$, and if $n = 0$ then $[0](p) = \mathcal{O}$. Using Theorem 3.2.4 it follows by induction that this map is an isogeny. For convenience we use the notation np instead of $[n](p)$.

Definition 3.3.6. Let E be an elliptic curve and $n \in \mathbb{Z}$, $n \neq 0$. The **n-torsion subgroup of** E, denoted $E[n]$, is the set of points of order n in E;

$$E[n] = \{p \in E \colon np = \mathcal{O}\}.$$

The elements of $E[n]$ are called **n-torsion points**. The elements in $E[n]$ that is not an m-torsion point for any $m < n$ dividing n are called **primitive** n-torsion points. The number of primitive n-torsion points is denoted a_n.

Proposition 3.3.7. *Any finite subgroup $G \subset E$ consists only of torsion points.*

Proof. Let G be a finite subgroup of an elliptic curve E, and let $p \in G$. Then $mp \in G$ for all $m \in \mathbb{Z}$. Since G is finite, we have $m'p = \mathcal{O}$ for some m', so p is a torsion point. ■

The following proposition is important in isogeny-based cryptography, and will play a key role in this thesis.

Proposition 3.3.8 ([Sil09, Proposition III.4.12.])**.** *Let E be an elliptic curve, and let G be a finite subgroup of E. Then there exists a unique elliptic curve E' and an isogeny $\phi \colon E \to E'$ such that* $\ker \phi = G$.

Note that the curve E' is unique up to isomorphism. There is a useful correspondence between morphisms and isogenies in the following way.

Proposition 3.3.9 ([Sil09, Example III.4.7.])**.** *Any morphism $\phi \colon E_1 \to E_2$ between elliptic curves is the composition of an isogeny and a translation.*

On the other hand, it follows from this that any isogeny between elliptic curves is a composition of a morphism ϕ followed by the translation $\tau_{-\phi(\mathcal{O})}$. Furthermore, since each fiber of a translation contains exactly one element, and the fibers of an isogeny are finite and contains the same number of points, then the fibers of a morphism are finite and contains the same number of points.

Proposition 3.3.10 ([Sil09, Corollary III.6.4.])**.** *Let E be an elliptic curve and $n \in \mathbb{Z} \setminus \{0\}$. We have the following.*

- $\deg[n] = n^2$.
- *If $char(K) = 0$ or if $char(K) = p > 0$ and $p \nmid n$ then*
$$E[n] = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$
- *If $char(K) = p > 0$ then one of the following is true:*
  - $E[p^e] = \{\mathcal{O}\}$,
  - $E[p^e] = \mathbb{Z}/p^e\mathbb{Z}$.

  *In the first case, E is called **supersingular**. In the other case, E is called **ordinary**.*

The term *supersingular* is unrelated to the notion of singularities on the curve. Elliptic curves are by definition non-singular. We will come back to supersingular curves in Chapter 4.

3.4 The Hessian form

In this section we will focus on a particular form of representing an elliptic curve called the Hessian form. Curves on Hessian form have global addition formulas, meaning that the addition formulas do not depend on the curve. The Hessian form is closely related to the representation theory of certain groups that we will explore in more detail in Chapter 5.

Definition 3.4.1. The family of curves in $\mathbb{P}^2$ defined over K, generated by the two cubics $xyz = 0$ and $x^3 + y^3 + z^3 = 0$, is called the **Hesse pencil** $\mathcal{H}$. It consists of curves $E_{(a,b)}$ defined by polynomials

$$f = a(x^3 + y^3 + z^3) + bxyz = 0$$

for $[a : b] \in \mathbb{P}^1(K)$. We say that an elliptic curve in $\mathbb{P}^2$ is **on Hessian form** if it is a non-singular curve in $\mathcal{H}$, and we specify the point $\mathcal{O} = (0 : 1 : -1)$ as the additive identity.

Remark 3.4.2. Over $\overline{K}$ any elliptic curve is isomorphic to a curve on Hessian form [AD09, Lemma 1.]. Over general fields K it is more subtle. It is a necessary condition to have a 3-torsion point defined over K, but in general not sufficient. If $K = \mathbb{F}_q$ with $q = 2 \mod 3$ then any elliptic curve with a $\mathbb{F}_q$-rational 3-torsion point is isomorphic (over $\mathbb{F}_q$) to a Hessian curve [MW12, Theorem 3.2.].

Definition 3.4.3. The **Hessian** of a projective curve $C = Z(f(x_0, x_1, x_2))$ is defined by

$$H(C) = \begin{vmatrix} \frac{\partial^2 f}{\partial x_0^2} & \frac{\partial^2 f}{\partial x_0 x_1} & \frac{\partial^2 f}{\partial x_0 x_2} \\ \frac{\partial^2 f}{\partial x_0 x_1} & \frac{\partial^2 f}{\partial x_1^2} & \frac{\partial^2 f}{\partial x_1 x_2} \\ \frac{\partial^2 f}{\partial x_0 x_2} & \frac{\partial^2 f}{\partial x_1 x_2} & \frac{\partial^2 f}{\partial x_2^2} \end{vmatrix}$$

When C is irreducible of degree d, then each entry is (homogeneous) of degree $d-2$, so $H(C)$ is of degree $3(d-2)$. We have that $C \cap H(C)$ is exactly the *inflection points* of C [Ful08, p. 59]. Inflection points are the points in C which tangents meet the curve with multiplicity at least three. By Bezout's theorem, inflection points on an elliptic curve are points which tangents meet the curve with multiplicity exactly three. The Hessian of a curve in $\mathcal{H}$ is itself a curve in $\mathcal{H}$:

$$\begin{aligned} H(E_{(a,b)}) &= \begin{vmatrix} 6ax & bz & by \\ bz & 6ay & bx \\ by & bx & 6az \end{vmatrix} \\ &= 6ax(6^2a^2yz - b^2x^2) - bz(6abz^2 - b^2xy) + by(b^2xz - 6aby^2) \\ &= (6^3a^3 + 2b^3)xyz - 6ab^2(x^3 + y^3 + z^3). \end{aligned}$$

Furthermore, the curves in $\mathcal{H}$ have nine points in common (over $\mathbb{C}$);

$$\begin{aligned} \mathrm{B}(\mathcal{H}) &= Z(xyz) \cap Z(x^3 + y^3 + z^3) \\ &= \{(0 : 1 : -1),\ (0 : 1 : -\epsilon),\ (0 : 1 : -\epsilon^2), \\ &\quad (1 : -1 : 0),\ (1 : -\epsilon : 0),\ (1 : -\epsilon^2 : 0), \end{aligned}$$

$$(-1:0:1),\ (-\epsilon:0:1),\ (-\epsilon^2:0:1)\}.$$

By Bezout's theorem, these are the only common points.

Proposition 3.4.4. *The common points of the curves in $\mathcal{H}$ are exactly the 3-torsion points.*

Proof. Since the Hessian of a curve in $\mathcal{H}$ is itself a curve in $\mathcal{H}$, the nine common intersection points are inflection points. Moreover, inflection points p on elliptic curves are 3-torsion points, because the tangent through p meets the curve with multiplicity 3, so by the addition law on elliptic curves we have $p+p+p=\mathcal{O}$. Since there are nine 3-torsion points, then the inflection points are exactly the 3-torsion points. Hence the common points are exactly the 3-torsion points. ■

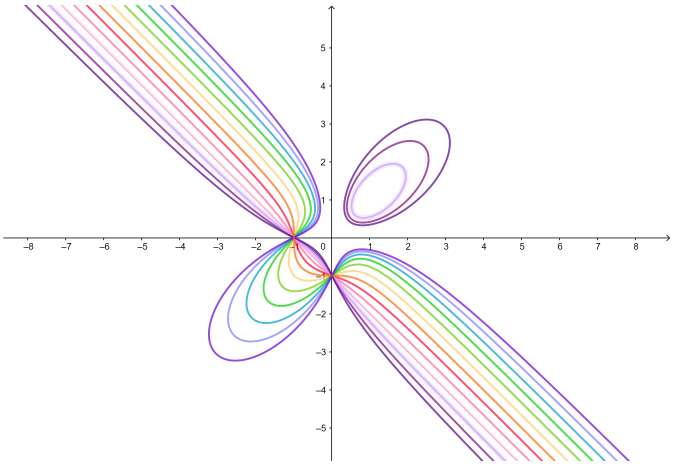


Figure 3.1: Some Hessian curves in an affine chart of $\mathbb{P}^2$.

Proposition 3.4.5. *Through any point in $\mathbb{P}^2 \setminus \mathrm{B}(\mathcal{H})$, there is exactly one curve in $\mathcal{H}$.*

Proof. Two distinct Hessian curves generates the Hesse pencil. So if two Hessian curves has a common point p, then p must be a common point of all curves in $\mathcal{H}$. This means that through any point in $\mathbb{P}^2 \setminus \mathrm{B}(\mathcal{H})$ there is at most one curve in $\mathcal{H}$. On the other hand, let $p=(p_1:p_2:p_3)\in\mathbb{P}^2$. Then it is clear that the linear equation $a(p_1^3+p_2^3+p_3^3)+b(p_1p_2p_3)=0$ has at least one solution (a,b), so through any point in $\mathbb{P}^2 \setminus \mathrm{B}(\mathcal{H})$ there is at least one curve in $\mathcal{H}$, and the result follows. ■

A curve in $\mathcal{H}$ is singular if and only if

$$3ax^2+byz = 3ay^2+bxz = 3az^2+bxy = 0.$$

This is precisely when $a=0$ or $27a^3+b^3=0$. These two equations give four singular curves in $\mathcal{H}$, namely

$$E_{(0,1)},\ E_{(1,-3)},\ E_{(1,-3\epsilon)},\ E_{(1,-3\epsilon^2)},$$

where ϵ is a primitive third root of unity. For an elliptic curve $E_{(a,b)}\colon a(x^3 + y^3 + z^3) + bxyz$ we must have $a \neq 0$, because otherwise it would be singular. So for an elliptic curve $E_{(a,b)}$ on Hessian form we can use the notation $E_\lambda = x^3 + y^3 + z^3 + \lambda xyz$ where $\lambda = \frac{b}{a}$.

Theorem 3.4.6 ([Fri02, Proposition 2.16])**.** *The j-invariant of an elliptic curve on Hesse form, $E_\lambda : x^3 + y^3 + z^3 + \lambda xyz$ over K is given by*

$$j(E_\lambda) = -\frac{\lambda^3(\lambda^3 - 216)^3}{(\lambda + 3)^3(\lambda + 3\epsilon)^3(\lambda + 3\epsilon^2)^3}. \tag{3.1}$$

Notice that for a fixed j-invariant there is at most 12 solutions to Equation (3.1). This means that there are at most 12 isomorphic curves for each j-invariant.

3.5 The addition formulas

The following formulas describe the group law on elliptic curves in $\mathcal{H}$. Note that these formulas do not depend on the curve E_λ.

Theorem 3.5.1 ([Ber+15, Theorem 3.1, 3.2, 4.2])**.** *The following formulas describe the group law on Hessian curves. Let $p_1 = (x_1 : y_1 : z_1)$, $p_2 = (x_2 : y_2 : z_2)$ be points on an elliptic curve $E_\lambda \in \mathcal{H}$. Let*

$$(x : y : z) = (x_2^2 y_1 z_1 - x_1^2 y_2 z_2 : z_2^2 x_1 y_1 - z_1^2 x_2 y_2 : y_2^2 x_1 z_1 - y_1^2 x_2 z_2),$$

and

$$(x' : y' : z') = (z_2^2 x_1 z_1 - y_1^2 x_2 y_2 : y_2^2 y_1 z_1 - x_1^2 x_2 z_2 : x_2^2 x_1 y_1 - z_1^2 y_2 z_2).$$

When $(x : y : z) \neq (0 : 0 : 0)$ then $p_1 + p_2$ is equal to $(x : y : z)$, and if $(x' : y' : z') \neq (0 : 0 : 0)$ then $p_1 + p_2$ is equal to $(x' : y' : z')$. Furthermore, we have

$$-(x_1 : y_1 : z_1) = (x_1 : z_1 : y_1).$$

Let E_λ be an elliptic curve in $\mathcal{H}$. Since the formulas for addition on E_λ does not depend on λ, we can extend the multiplication-by-n isogeny $[n]$ to a rational map (even better, a morphism, because every point in $\mathbb{P}^2$ lies on a Hessian curve)

$$[n] : \mathbb{P}^2 \xrightarrow{(F_0^n : F_1^n : F_2^n)} \mathbb{P}^2$$

such that the restriction to E_λ is the map $[n] : E_\lambda \to E_\lambda$. Note that we denote the polynomials F_i^n with n in superscript (not as exponent). The following claim is proven in [Fri02] for $n \leq 10$.

Claim 3.5.2 ([Fri02, pp. 16–17])**.** *If $n \neq 3$ then for all m such that $m \mid n$ and $3 \nmid m$ we have the following:*

- *F_0^m and $F_1^m + F_2^m$ have a common irreducible factor P_m of degree $\frac{a_m}{3}$, where a_m is the number of primitive m-torsion points.*
- *$Z(P_m)$ intersects every $E_\lambda \in \mathcal{H}$ in exactly the primitive m-torsion points.*

The polynomials P_m can be found in [Fri02] for $m = 1, \ldots, 10$. In Chapter 6 and Chapter 7 we will use P_2 and P_4 to find 2- and 4-torsion points on Hessian curves, so we give these polynomials here.

$$P_2 = z - y$$
$$P_4 = x^3y + x^3z - y^3z - z^3y.$$

Note that 2-torsion points p on an elliptic curve $E_\lambda \in \mathcal{H}$ are of the form $p = (s : 1 : 1)$, where $s^3 + 1^3 + 1^3 + \lambda s = 0$. On the other hand, given a 2-torsion point $(s : 1 : 1) \in \mathbb{P}^2$, we can find which curve $E_\lambda \in \mathcal{H}$ this point belongs to by solving $\lambda = -s^2 - \frac{2}{s}$.

CHAPTER 4

Elliptic curves in post-quantum cryptography

We will now describe how elliptic curves and isogenies are used in post-quantum cryptography. First we describe public key encryption and how quantum computers poses a threat to such cryptosystems. Then we include some properties of supersingular elliptic curves that are useful for cryptographic purposes. Furthermore we give a brief overview of the SIDH (Supersingular Isogeny Diffie-Hellman) algorithm, and we give a description of how to compute an isogeny ψ as a composition of low-degree isogenies, where the kernel of ψ is a specified subgroup. The presentation of SIDH is inspired by [Cos19], and the algorithm for computing isogeny compositions was first described in [JF11].

4.1 Public key encryption

A **public key encryption** (PKE) scheme is a scheme using both private and public keys. We encrypt a message using a public key, and decrypt using a private key. The opposite of PKE is **symmetric key encryption** (SKE) where both parties use the same secret key. Public key encryption can be used for secure communication, but symmetric key encryption is more suitable for this. We typically use PKE to establish a shared secret key, and then use this secret key in secure communication using symmetric methods.

Most of the public key cryptosystems used today rely on the complexity of factoring large numbers and solving the discrete logarithm problem. In 1994 Peter Shor found an algorithm that can easily solve these problems, but only on a full-scale quantum computer. It is possible that such computers will exist in a few decades, so it is necessary to develop alternative public key encryption methods. At the time of writing this thesis there is an ongoing process initiated by NIST (National Institute of Standards and Technology) to standardize one or more quantum resistant public key cryptographic algorithms. One of the candidates in this process is the suite SIKE (Supersingular Isogeny Key Encapsulation). SIKE is a special instance of the SIDH algorithm, which we will describe in this chapter.

4.2 Elliptic curves over finite fields

In cryptography we typically work with supersingular elliptic curves defined over finite fields $K = \mathbb{F}_{p^2}$, where p a is prime, and consider only the $\mathbb{F}_{p^2}$-rational points on E, denoted $E(\mathbb{F}_{p^2})$. In this section we will let p be a prime, and q be a prime power. Supersingular elliptic curves has some useful properties that we include here.

Proposition 4.2.1 ([Tat66, Theorem 1.c.])**.** *Two elliptic curves E and E' defined over a finite field $\mathbb{F}_q$ are isogeneous if and only if $|E(\mathbb{F}_q)| = |E'(\mathbb{F}_q)|$.*

Here $|E(\mathbb{F}_q)|$ denotes the number of $\mathbb{F}_q$-rational points on E. When $E/\overline{\mathbb{F}}_p$ is supersingular, then we are assured that the j-invariant can be found in a small field extension of $\mathbb{F}_p$, namely $\mathbb{F}_{p^2}$.

Proposition 4.2.2 ([Sil09, Theorem V.3.1.(iii).])**.** *Let $E/\overline{\mathbb{F}}_p$ be a supersingular curve, where p is prime. Then $j(E) \in \mathbb{F}_{p^2}$.*

When working with elliptic curves on computers we need to fix a base field, so it is useful that we can compute j-invariants in a field extension of $\mathbb{F}_p$ that is as small as possible. Furthermore, by Hasse's theorem we have that $|E(\mathbb{F}_q)| = q + 1 - t$ where $|t| \leq 2\sqrt{q}$ [Sil09, Theorem V.1.1.].

Proposition 4.2.3 ([MOV93, Lemma 2.])**.** *Let E be a supersingular curve defined over $\mathbb{F}_q$, and $|E(\mathbb{F}_q)| = q + 1 - t$. If $t^2 = 4q$, then either*

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/(\sqrt{q} - 1)\mathbb{Z} \times \mathbb{Z}/(\sqrt{q} - 1)\mathbb{Z}$$

or

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/(\sqrt{q} + 1)\mathbb{Z} \times \mathbb{Z}/(\sqrt{q} + 1)\mathbb{Z},$$

depending on whether $t = 2\sqrt{q}$ or $t = -2\sqrt{q}$, respectively.

In cryptography we typically choose a prime $p = l_1^{e_1} l_2^{e_2} - 1$ and a supersingular curve $E/\mathbb{F}_p^2$ such that $t = -2p$. Then we have $|E(\mathbb{F}_{p^2})| = p^2 + 1 + 2p = (p+1)^2$, and

$$E(\mathbb{F}_{p^2}) \simeq \mathbb{Z}/(p + 1)\mathbb{Z} \times \mathbb{Z}/(p + 1)\mathbb{Z},$$

so the $\mathbb{F}_{p^2}$-rational points on the curve are exactly the torsion points $E[l_1^{e_1} l_2^{e_2}]$, and we will see below that these are the only points that we need.

4.3 Supersingular Isogeny Diffie-Hellman

We now describe how elliptic curves and isogenies can be used to establish a shared secret between two parties, Alice and Bob. This presentation of SIDH is based on [Cos19].

Fix a prime $p = l_A^{e_A} l_B^{e_B} - 1$, and a supersingular curve E defined over $\mathbb{F}_{p^2}$. Alice's private key is a subgroup of $E/\mathbb{F}_{p^2}$ of order $l_A^{e_A}$, which gives rise to a unique isogeny by Proposition 3.3.8. Alice finds two generators for the group of

$l_A^{e_A}$-torsion points (recall Proposition 3.3.10), namely

$$\langle P_A, Q_A \rangle = E[l_A^{e_A}] = \mathbb{Z}/l_A^{e_A}\mathbb{Z} \times \mathbb{Z}/l_A^{e_A}\mathbb{Z}.$$

Then she finds a generator S_A for her secret subgroup of $l_A^{e_A}$-torsion points by choosing $k_A \in [0, l_A^{e_A})$ and letting

$$S_A = P_A + [k_A]Q_A.$$

Then Alice's private subgroup is $\langle S_A \rangle \subset E[l_A^{e_A}]$. Bob finds his private subgroup $\langle S_B \rangle \subset E[l_B^{e_B}]$ analogously.

Now, Alice computes the secret isogeny $\psi_A \colon E \to E_A$ having $\langle S_A \rangle$ as kernel. Alice finds this isogeny by composing e_A isogenies of degree l_A (in Section 4.4 we describe exactly how she chooses the right l_A-isogenies). Alices public key is now

$$PK_A = (E_A, \psi_A(P_B), \psi_A(Q_B)).$$

Bob finds his public key analogously, and has the public key

$$PK_B = (E_B, \psi_B(P_A), \psi_B(Q_A)).$$

Now, Alice and Bob switch curves and computes their isogenies again, starting from the other's curve. Given Bob's public key, Alice finds a point S'_A on Bob's curve E_B, given by

$$S'_A = \psi_B(P_A) + [k_A]\psi_B(Q_A) = \psi_B(P_A + [k_A]Q_A) = \psi_B(S_A).$$

The group $\langle S'_A \rangle$ is a subgroup of E_B. Alice computes the isogeny $\psi'_A \colon E_B \to E_{AB}$ having $\langle S'_A \rangle$ as kernel. By construction, the kernel of $\psi'_A \circ \psi_B$ is $\langle S_A \rangle \cup \langle S_B \rangle$.

$$E \xrightarrow{\psi_B} E_B \xrightarrow{\psi'_A} E_{AB}, \qquad E \xrightarrow{\psi'_A \circ \psi_B} E_{AB}$$

In a similar fashion, Bob computes an isogeny $\psi'_B \colon E_A \to E_{BA}$ having $\langle S'_B \rangle = \langle \psi_A(P_B) + [k_B]\psi_A(Q_B) \rangle$ as kernel. Again, the kernel of $\psi'_B \circ \psi_A$ is $\langle S_A \rangle \cup \langle S_B \rangle$.

$$E \xrightarrow{\psi_A} E_A \xrightarrow{\psi'_B} E_{BA}, \qquad E \xrightarrow{\psi'_B \circ \psi_A} E_{BA}$$

Since $\ker(\psi'_A \circ \psi_B) = \ker(\psi'_B \circ \psi_A)$ then Alice and Bob land on the same curve (up to isomorphism). They can calculate the j-invariant of this curve, which is their shared secret.

The security of SIDH relies on the *supersingular isogeny walk problem*: Given two isogenous elliptic curves $E,\ E'$, find a path made of isogenies of small degree between E and E'. This problem is believed to be hard for both classical and quantum computers.

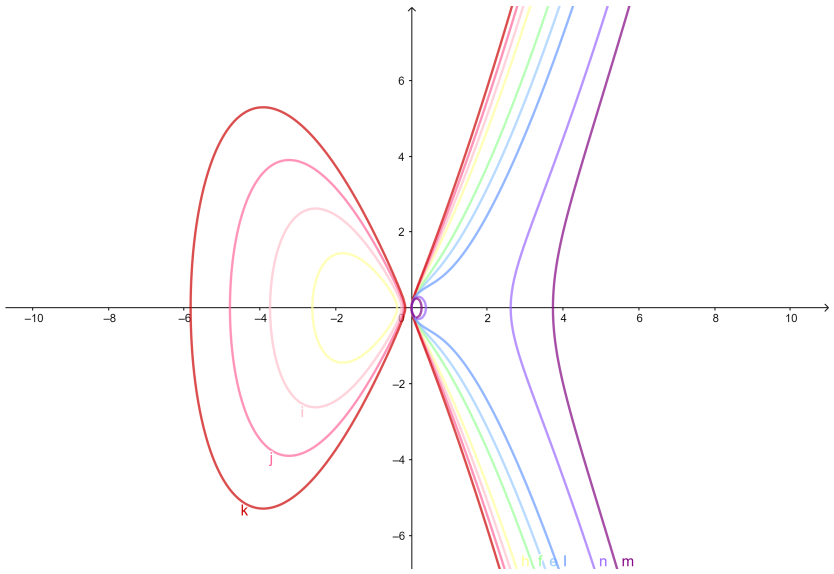


Figure 4.1: Some Montgomery curves in the affine chart of $\mathbb{P}^2$ where $z = 1$.

SIKE

Supersingular Isogeny Key Encapsulation (SIKE) is a special instance of SIDH, with fixed parameter sets. SIKE uses the Montgomery form of elliptic curves, and lets $p = 2^{e_A}3^{e_B} - 1$ where e_A and e_B are fixed public parameters. For $a, b \in \mathbb{F}_{p^2}$ such that $b(a^2 - 4) \neq 0$, we have that a Montgomery curve $E_{a,b}$ defined over $\mathbb{F}_{p^2}$ is the set of points $(x : y : z) \in \mathbb{P}^2$ satisfying

$$by^2z - x^3 - ax^2z - xz^2 = 0,$$

with a point $\mathcal{O}$ at infinity. In SIKE we only consider the $\mathbb{F}_{p^2}$-rational points of $E_{a,b}$, namely $E_{a,b}(\mathbb{F}_{p^2})$. The public starting curve in SIKE is the fixed (affine) supersingular Montgomery curve

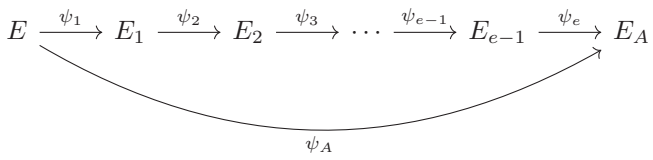
$$y^2 = x^3 + 6x^2 + x.$$

In SIKE the isogenies of degree $l_A^{e_A} = 2^{e_A}$ and $l_B^{e_B} = 3^{e_B}$ described above are computed as compositions of isogenies of degree 2, 3 and 4. One weakness of the SIKE is its time performance, and the isogeny computations account for much of the time consumption. Alternative isogeny formulas, using other forms of representing elliptic curves, could possibly improve the performance of SIKE.

4.4 Isogeny computations

In Section 4.3 we said that Alice, for instance, computes her private isogeny $\psi_A \colon E \to E_A$ where $\ker \psi_A = \langle S_A \rangle$, by composing e isogenies of degree l. How

does she find the right l-isogenies ψ_i so that $\ker(\psi_e \circ \cdots \psi_2 \circ \psi_1) = \langle S_A \rangle$?



The initial idea, given by [JF11], was as follows. Let S_A be Alice's secret l^e-torsion point, which generates her secret subgroup. She computes the point $p_1 = l^{e-1}S_A$, which is a l-torsion point. This points p_1 generates a subgroup of order l, and Alice finds the unique l-isogeny $\psi_1 \colon E \to E_1$ having $\langle p_1 \rangle$ as kernel. Since

$$\mathcal{O} = \psi_1(p_1) = \psi_1(l^{e-1}S_A) = l^{e-1}\psi(S_A),$$

$\psi_1(S_A)$ is a l^{e-1} torsion point. Now, Alice computes a new point $p_2 = l^{e-2}\psi_1(S_A) \in E_1$. We see that $lp_2 = \mathcal{O}$, so p_2 is a l-torsion point on E_1. Alice now finds the unique l-isogeny $\psi_2 \colon E_1 \to E_2$ having $\langle p_2 \rangle$ as kernel. By construction, $(\psi_2 \circ \psi_1)(S_A) \in E_2$ is now a l^{e-2}-torsion point. Alice continues like this until $(\psi_e \circ \cdots \circ \psi_2 \circ \psi_1)(S_A) \in E_A$ is a l^{e-e}-torsion point, namely $\mathcal{O}$. Then we will have

$$\psi_A(nS_A) = n\psi_A(S_A) = n\mathcal{O} = \mathcal{O}$$

for all $n \in \{1, \ldots, l^e\}$, so $\ker \psi_A = \langle S_A \rangle$ as wanted.

Computing the multiplication-by-l^{e-i} map on each step is cumbersome. In [DJP14] we can find an improved version of this isogeny computation algorithm, but we will not go further into this here. In Section 7.2 we present an alternative to this algorithm, where we use special morphisms (that are not isogenies) of degree 2 to compute an isogeny of degree 2^e.

CHAPTER 5

Group actions on the Hesse pencil

Let V be a vector space over $\mathbb{C}$. To give a representation V of a group G is equivalent to giving a group action of G on V. In this chapter we will study the representation theory of a group closely related to the Hesse pencil, namely the Heisenberg group H_3. We will also describe how the alternating group A_4 can be used to find isomorphic Hessian curves. Finally, we will find all the irreducible representations of H_3, and explain how these representations are related to isogenies between Hessian curves.

5.1 Representation theory

Let V be a vector space over $\mathbb{C}$ of dimension n, and $\mathrm{GL}(V)$ be the group of isomorphisms of V onto itself. Given a basis for V we can identify $\mathrm{GL}(V)$ with the group of invertible square matries of size n.

Definition 5.1.1. Let G be a finite group. A **linear representation** of G is a vector space V together with a homomorphism $\rho : G \to \mathrm{GL}(V)$.

When it is clear from context we often omit ρ in the notation and say that V is a representation of G. A linear subspace $W \subset V$ is called G-**invariant** if $\rho(g)w \in W$ for all $g \in G$ and all $w \in W$. The restriction of ρ to $\mathrm{GL}(W)$ where W is G-invariant, is called a **sub-representation.** A representation is called **irreducible** if it has only trivial sub-representations.

Theorem 5.1.2 ([Ser77, Theorem 1.4.2.])**.** *Every representation is a direct sum of irreducible representations.*

Let V be a vector space with a basis $\{e_1, \ldots, e_n\}$, and let a be a linear map of V into itself with matrix (a_{ij}). By the **trace** of a we mean the scalar

$$\mathrm{Tr}(a) = \sum_i a_{ii}.$$

The trace is equal to the sum of eigenvalues of a (counted with multiplicity), and does not depend on the choice of basis.

Definition 5.1.3. Let $\rho : G \to \mathrm{GL}(V)$ be a representation of a finite group G. For $g \in G$ let $\chi_\rho(g) = \mathrm{Tr}(\rho(g))$. The complex valued function χ_ρ on G is called the **character** of ρ.

Two elements a, b in a group G is called **conjugate** if there is an element $g \in G$ such that $b = gag^{-1}$. This is an equivalence relation, and the equivalence classes are called **conjugacy classes**. To find the character of a representation, we only need to calculate the trace of one element in each conjugacy class.

Proposition 5.1.4 ([Ser77, Proposition 2.1.1.(iii).])**.** *Elements in the same conjugacy class of a group has the same trace.*

To a group we can give the **character table**, a two-dimensional table where the rows corresponds to irreducible representations and the columns correspond to the conjugacy classes, and where the entries are the traces.

Theorem 5.1.5 ([Ser77, Theorem 2.5.7.])**.** *The number of irreducible representations of G is equal to the number of conjugacy classes of G.*

It follows that the character table is square. Given the characters of two representations of a group G, we also know the character of the direct sum representation.

Proposition 5.1.6 ([Ser77, Proposition 2.1.2.])**.** *Let $\rho_1 \colon G \to \mathrm{GL}(V_1)$ and $\rho_2 : G \to \mathrm{GL}(V_2)$ be two representations of G, and χ_1 and χ_2 be their characters. Then the character χ of the direct sum representation $V_1 \oplus V_2$ is equal to $\chi_1 + \chi_2$.*

The character is important because it characterizes the representation, thereby the name.

Proposition 5.1.7 ([Ser77, Corollary 2.3.2.])**.** *Two representations with the same character are isomorphic.*

In the rest of the chapter we will consider two groups that acts on the Hesse pencil $\mathcal{H}$, namely the Heisenberg group H_3 and the alternating group A_4.

5.2 The Heisenberg group

The *Heisenberg group* is the finite subgroup $H_3 = \langle \sigma, \tau \rangle$ of $\mathrm{SL}(3, \mathbb{C})$ where

$$\sigma = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \ \tau = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \epsilon & 0 \\ 0 & 0 & \epsilon^2 \end{pmatrix},$$

and ϵ is a primitive third root of unity. Here $\mathrm{SL}(3, \mathbb{C})$ denotes the multiplicative group of 3×3 matrices defined over $\mathbb{C}$ with determinant equal to 1. Let x_0, x_1, x_2 correspond to the standard basis vectors in $\mathrm{Span}(x_0, x_1, x_2) \simeq \mathbb{C}^3$. Then we see that

$$\sigma(x_i) = x_{i+1}, \ \tau(x_i) = \epsilon^i x_i, \ i \mod 3.$$

Example 5.2.1. Elements in H_3 acts on points in $\mathbb{P}^2$. If $p = (x : y : z) \in \mathbb{P}^2$, then

$$\begin{aligned} \sigma(p) &= (\sigma(x), \sigma(y), \sigma(z)) \\ &= (y : z : x), \end{aligned}$$

and

$$\begin{aligned}\tau(p) &= (\tau(x) : \tau(y) : \tau(z)) \\ &= (x : \epsilon y : \epsilon^2 z).\end{aligned}$$

Elements in H_3 also acts on polynomials. If $f(x, y, z)$ is a polynomial then

$$\sigma(f(x, y, z)) = f(y, z, x),\ \tau(f(x, y, z)) = f(x, \epsilon y, \epsilon^2 z).$$

Furthermore, H_3 fixes the curves in the Hesse pencil $\mathcal{H}$:

$$\begin{aligned}\sigma(a(x^3 + y^3 + z^3) + b(xyz)) &= a(y^3 + z^3 + x^3) + b(yzx) \\ &= a(x^3 + y^3 + z^3) + b(xyz),\end{aligned}$$

and

$$\begin{aligned}\tau(a(xyz) + b(x^3 + y^3 + z^3)) &= a(x\epsilon y\epsilon^2 z) + b(x^3 + (\epsilon y)^3 + (\epsilon^2 z)^3 \\ &= a(xyz) + b(x^3 + y^3 + z^3).\end{aligned}$$

Proposition 5.2.2. *H_3 acts on points on an elliptic curve $E_\lambda \in \mathcal{H}$ by translation by 3-torsion points.*

Proof. Let $p = (p_0 : p_1 : p_2) \in E_\lambda$. On one hand we have that $\sigma(p) = (p_1 : p_2 : p_0)$, and on the other hand we have

$$\begin{aligned}(p_0 : p_1 : p_2) + (1 : -1 : 0) &= (p_1 p_2 : p_2^2 : p_0 p_2) \\ &= (p_1 : p_2 : p_0),\end{aligned}$$

as long as $p_2 \neq 0$. If $p_2 = 0$ then $(p_0 : p_1 : p_2)$ is a 3-torsion point, and $\sigma(p_0 : p_1 : p_2)$ is also a 3-torsion point, so also for this case the action of σ must be a translation by a 3-torsion point.

Furthermore, we have $\tau(p) = (p_0, \epsilon p_1, \epsilon^2 p_2)$, and on the other hand

$$\begin{aligned}(p_0 : p_1 : p_2) + (0 : 1 : -\epsilon) &= (\epsilon p_0^2 : \epsilon^2 p_0 p_1 : p_0 p_2) \\ &= (p_0 : \epsilon p_1 : \epsilon^2 p_1),\end{aligned}$$

as long as $p_0 \neq 0$. If $p_0 = 0$ then $(p_0 : p_1 : p_2)$ is a 3-torsion point, and $\tau(p_0 : p_1 : p_2)$ is also a 3-torsion point, so also for this case the action of τ must be a translation by a 3-torsion point.

Since the 3-torsion points form a subgroup, and σ and τ generate H_3, we are done. ■

5.3 Orbits of isomorphic Hessian curves

Definition 5.3.1. The **normalizer** of a subset S in a group G is the set of elements $N_G(S)$ of G that leaves the set S fixed under conjugation.

The normalizer of H_3 in $\mathrm{SL}(3, \mathbb{C})$ is $N_3 = \langle \sigma, \tau, \delta, \nu \rangle$, where

$$\delta = k_\delta \begin{pmatrix} 1 & 1 & 1 \\ 1 & \epsilon & \epsilon^2 \\ 1 & \epsilon^2 & \epsilon \end{pmatrix},\ \nu = \begin{pmatrix} \epsilon^{\frac{2}{3}} & 0 & 0 \\ 0 & \epsilon^{\frac{4}{3}} & 0 \\ 0 & 0 & \epsilon^{\frac{4}{3}} \end{pmatrix}.$$

Here k_δ is the constant that gives $\det(\delta) = 1$. We have that

$$\delta(a(x^3+y^3+z^3)+b(xyz)) = k_\delta^3(b+3a)(x^3+y^3+z^3)+k_\delta^3(-3b+18a)xyz,$$

and

$$\nu(a(x^3+y^3+z^3)+b(xyz)) = a(x^3+y^3+z^3)+\epsilon b(xyz),$$

so $\delta(E_{(a,b)}) = E_{(b+3a,-3b+18a)}$ and $\nu(E_{(a,b)}) = E_{(a,\epsilon b)}$. Because elements of N_3 acts on $\mathcal{H}$ by linear transformations, the orbits of $\mathcal{H}$ under N_3 consists of isomorphic curves.

Proposition 5.3.2 ([Fri02, p. 14])**.** *The group* $G = {}^{N_3}\!/_{H_3}$ *is isomorphic to* $\mathrm{SL}(2,\mathbb{Z}_3)$.

For the element $\iota = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix} \in N_3 \setminus H_3$, we see that

$$\iota(a(x^3+y^3+z^3)+b(xyz)) = -a(x^3+y^3+z^3)-b(xyz),$$

so $\iota(E_{(a,b)}) = E_{(-a,-b)} = E_{(a,b)}$. Thus ι acts trivially on the Hesse pencil. In fact, ι fixes the line $Z_+(P_2) = Z_+(z-y)$ of 2-torsion points:

$$\iota(P) = -P = P \iff P \text{ is a 2-torsion point.}$$

Proposition 5.3.3 ([Fri02, p. 14])**.** *The group* ${}^{G}\!/_{\langle\iota\rangle}$ *is isomorphic to* A_4.

We know that there are at most 12 curves for each j-invariant, and also that $|A_4| = 12$. Then each orbit of ${}^{G}\!/_{\langle\iota\rangle}$ of length 12 consists of exactly the isomorphic Hessian curves.

Example 5.3.4. We will now demonstrate how we can use the group action of ${}^{G}\!/_{\langle\iota\rangle} \simeq A_4$ to find isomorphic Hessian curves. Let $E_\lambda = Z_+(x^3+y^3+z^3+\lambda xyz)$ he a Hessian curve, denoted by $(1:\lambda)$. Then the eleven non-trivial elements in ${}^{G}\!/_{\langle\iota\rangle}$ acts on $(1:\lambda)$ in the following way.

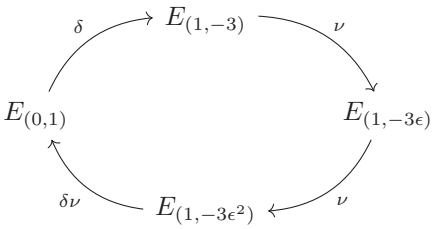
$$\begin{aligned}
\nu(1:\lambda) &= (1:\epsilon\lambda)\\
\nu^2(1:\lambda) &= (1:\epsilon^2\lambda)\\
\delta(1:\lambda) &= \left(1:\frac{-3\lambda+18}{\lambda+3}\right)\\
\nu\delta(1:\lambda) &= \left(1:\epsilon\frac{-3\lambda+18}{\lambda+3}\right)\\
\nu^2\delta(1:\lambda) &= \left(1:\epsilon^2\frac{-3\lambda+18}{\lambda+3}\right)\\
\delta\nu(1:\lambda) &= \left(1:\frac{-3(\epsilon\lambda)+18}{\lambda+3}\right)\\
\nu\delta\nu(1:\lambda) &= \left(1:\epsilon\frac{-3(\epsilon\lambda)+18}{\lambda+3}\right)\\
\nu^2\delta\nu(1:\lambda) &= \left(1:\epsilon^2\frac{-3(\epsilon\lambda)+18}{\lambda+3}\right)
\end{aligned}$$

$$\begin{aligned}
\delta\nu^2(1:\lambda) &= \left(1 : \frac{-3(\epsilon^2\lambda)+18}{\lambda+3}\right) \\
\nu\delta\nu^2(1:\lambda) &= \left(1 : \epsilon\frac{-3(\epsilon^2\lambda)+18}{\lambda+3}\right) \\
\nu^2\delta\nu^2(1:\lambda) &= \left(1 : \epsilon^2\frac{-3(\epsilon^2\lambda)+18}{\lambda+3}\right).
\end{aligned}$$

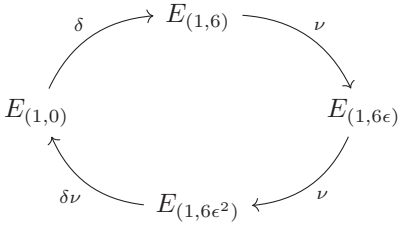
For a given λ, these expressions give precisely the other Hessian curves that are isomorphic to E_λ.

There are some curves that have orbit length less then 12, so they must be fixed by at least one element of A_4. We find these curves using the eleven expressions above. We must consider the singular curve $E_{(0,1)}$ as a special case, because this curve is not on the form E_λ. We find that there are three orbits with orbit length less than 12.

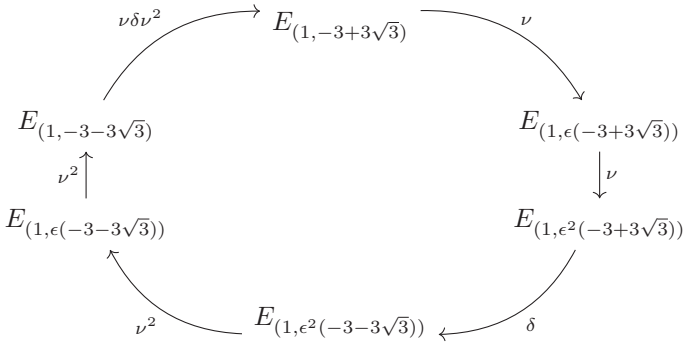
The first orbit consists of exactly the four singular Hessian curves. This means that all the singular Hessian curves are isomorphic.



The next orbit consists of the Fermat cubic and the three other isomorphic curves.



The last orbit of length less than 12 consists of 6 isomorphic curves.



5.4 Representations of the Heisenberg group

Now we will find all the irreducible representations of the Heisenberg group. We will see that there are exactly 9 irreducible representations of dimension 1 and exactly 2 irreducible representations of dimension 3.

1-dimensional representations

Let V be the vector space

$$V = \mathrm{Span}(xyz, x^3, y^3, z^3, x^2y, x^2z, xy^2, y^2z, z^2x, z^2y) \simeq \mathbb{C}^{10}.$$

We let the basis elements correspond to the standard basis vectors e_i, having a 1 in the i-th entry and 0 elsewhere. For example, the first basis element xyz corresponds to the vector $e_1 = (1, 0, \ldots, 0)$, and so on. Then

$$\begin{aligned} \rho\colon H_3 &\to \mathrm{GL}(V) \\ \sigma &\mapsto (e_1\ e_3\ e_4\ e_2\ e_8\ e_7\ e_{10}\ e_9\ e_5\ e_6) \\ \tau &\mapsto (e_1\ e_2\ e_3\ e_4\ \epsilon e_5\ \epsilon^2 e_6\ \epsilon^2 e_7\ \epsilon e_8\ \epsilon e_9\ \epsilon^2 e_{10}) \end{aligned}$$

is a representation of dimension 10. We will find the irreducible sub-representations of this representation. Their characters χ_i are given in the character table in Appendix A.

- We easily see that the basis element xyz is invariant under H_3. So we let $V_1 = \mathrm{Span}(f_1) = \mathrm{Span}(xyz)$, and then

  $$\begin{aligned} \rho_1\colon H_3 &\to \mathrm{GL}(V_1) \\ \sigma &\mapsto 1 \\ \tau &\mapsto 1 \end{aligned}$$

  is a 1-dimensional, hence irreducible, representation of H_3.

Now we look at the 3-dimensional subspace $\mathrm{Span}(x^3, y^3, z^3) \simeq \mathrm{Span}(e_1, e_2, e_3) = \mathbb{C}^3$, where e_i are the standard basis vectors of $\mathbb{C}^3$. We see that these three basis elements are invariant under H_3, so we have the sub-representation

$$\begin{aligned} H_3 &\to \mathrm{GL}(\mathrm{Span}(x^3, y^3, z^3)) \\ \sigma &\mapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \\ \tau &\mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \end{aligned}$$

The two matrices have common eigenvectors, which are

$$\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ \epsilon^2 \\ \epsilon \end{pmatrix}, \quad \begin{pmatrix} 1 \\ \epsilon \\ \epsilon^2 \end{pmatrix}.$$

These vectors give us the three following sub-representations, which are irreducible because they are 1-dimensional.

- Let $V_1' = \mathrm{Span}(f_1') = \mathrm{Span}(x^3 + y^3 + z^3)$. Then we have the irreducible representation

$$\begin{aligned} \rho_1' \colon H_3 &\to \mathrm{GL}(V_1') \\ \sigma &\mapsto 1 \\ \tau &\mapsto 1. \end{aligned}$$

  We note that this representation is isomorphic to V_1, because the character is clearly the same.

- Let $V_2 = \mathrm{Span}(f_2) = \mathrm{Span}(x^3 + \epsilon^2 y^3 + \epsilon z^3)$. Then we have the irreducible representation

$$\begin{aligned} \rho_2 \colon H_3 &\to \mathrm{GL}(V_2) \\ \sigma &\mapsto \epsilon \\ \tau &\mapsto 1. \end{aligned}$$

- Let $V_3 = \mathrm{Span}(f_3) = \mathrm{Span}(x^3 + \epsilon y^3 + \epsilon^2 z^3)$. Then we have the irreducible representation

$$\begin{aligned} \rho_3 \colon H_3 &\to \mathrm{GL}(V_3) \\ \sigma &\mapsto \epsilon^2 \\ \tau &\mapsto 1. \end{aligned}$$

Now we look at the 3-dimensional subspace $\mathrm{Span}(x^2y, y^2z, z^2x) \simeq \mathrm{Span}(e_1, e_2, e_3) = \mathbb{C}^3$. Again, we see that the three basis elements are invariant under H_3. Then we have the sub-representation

$$\begin{aligned} H_3 &\to \mathrm{GL}(\mathrm{Span}(x^2y, y^2z, z^2x)) \\ \sigma &\mapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \\ \tau &\mapsto \begin{pmatrix} \epsilon & 0 & 0 \\ 0 & \epsilon & 0 \\ 0 & 0 & \epsilon \end{pmatrix}. \end{aligned}$$

The two matrices have common eigenvectors, which are

$$\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ \epsilon^2 \\ \epsilon \end{pmatrix}, \quad \begin{pmatrix} 1 \\ \epsilon \\ \epsilon^2 \end{pmatrix}.$$

These vectors give us the three following sub-representations.

- Let $V_4 = \mathrm{Span}(f_4) = \mathrm{Span}(x^2y + y^2z + xz^2)$. Then we have the irreducible representation

$$\begin{aligned} \rho_4 \colon H_3 &\to \mathrm{GL}(V_4) \\ \sigma &\mapsto 1 \\ \tau &\mapsto \epsilon. \end{aligned}$$

- Let $V_5 = \mathrm{Span}(f_5) = \mathrm{Span}(x^2y + \epsilon^2 y^2 z + \epsilon x z^2)$. Then we have the irreducible representation

$$\begin{aligned} \rho_5 \colon H_3 &\to \mathrm{GL}(V_5) \\ \sigma &\mapsto \epsilon \\ \tau &\mapsto \epsilon. \end{aligned}$$

- Let $V_6 = \mathrm{Span}(f_6) = \mathrm{Span}(x^2y + \epsilon y^2 z + \epsilon^2 x z^2)$. Then we have the irreducible representation

$$\begin{aligned} \rho_6 \colon H_3 &\to \mathrm{GL}(V_6) \\ \sigma &\mapsto \epsilon^2 \\ \tau &\mapsto \epsilon. \end{aligned}$$

Now we look at the 3-dimensional subspace $\mathrm{Span}(x^2z, y^2x, z^2y) \simeq \mathrm{Span}(e_1, e_2, e_3) = \mathbb{C}^3$. Then we have a representation

$$\begin{aligned} H_3 &\to \mathrm{GL}(\mathrm{Span}(x^2z, y^2x, z^2y)) \\ \sigma &\mapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \\ \tau &\mapsto \begin{pmatrix} \epsilon^2 & 0 & 0 \\ 0 & \epsilon^2 & 0 \\ 0 & 0 & \epsilon^2 \end{pmatrix}. \end{aligned}$$

The two matrices have common eigenvectors, which are

$$\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ \epsilon^2 \\ \epsilon \end{pmatrix}, \quad \begin{pmatrix} 1 \\ \epsilon \\ \epsilon^2 \end{pmatrix}.$$

These vectors give us the three following sub-representations.

- Let $V_7 = \mathrm{Span}(f_7) = \mathrm{Span}(x^2z + xy^2 + yz^2)$. Then we have the irreducible representation

$$\begin{aligned} \rho_7 \colon H_3 &\to \mathrm{GL}(V_7) \\ \sigma &\mapsto 1 \\ \tau &\mapsto \epsilon^2. \end{aligned}$$

- Let $V_8 = \mathrm{Span}(f_8) = \mathrm{Span}(x^2z + \epsilon^2 xy^2 + \epsilon yz^2)$. Then we have the irreducible representation

$$\begin{aligned} \rho_8 \colon H_3 &\to \mathrm{GL}(V_8) \\ \sigma &\mapsto \epsilon \\ \tau &\mapsto \epsilon^2. \end{aligned}$$

- Let $V_9 = \mathrm{Span}(f_9) = \mathrm{Span}(x^2z + \epsilon xy^2 + \epsilon^2 yz^2)$. Then we have the irreducible representation

$$\rho_9 \colon H_3 \to \mathrm{GL}(V_9)$$

$$\sigma \mapsto \epsilon^2$$
$$\tau \mapsto \epsilon^2.$$

We have found 9 irreducible representations of H_3 of dimension 1. Their characters χ_i can be found in the character table in Appendix A. We get that

$$V = V_1^2 \oplus V_2 \oplus V_3 \oplus V_4 \oplus V_5 \oplus V_6 \oplus V_7 \oplus V_8 \oplus V_9.$$

We summarize the polynomials f_i from each representation V_i here, because they will come to use later.

$$\begin{aligned}
f_1 &= xyz \\
f_2 &= x^3 + \epsilon^2 y^3 + \epsilon z^3 \\
f_3 &= x^3 + \epsilon y^3 + \epsilon^2 z^3 \\
f_4 &= x^2 y + y^2 z + x z^2 \\
f_5 &= x^2 y + \epsilon^2 y^2 z + \epsilon x z^2 \\
f_6 &= x^2 y + \epsilon y^2 z + \epsilon^2 x z^2 \\
f_7 &= x^2 z + x y^2 + y z^2 \\
f_8 &= x^2 z + \epsilon^2 x y^2 + \epsilon y z^2 \\
f_9 &= x^2 z + \epsilon x y^2 + \epsilon^2 y z^2.
\end{aligned}$$

3-dimensional representations

We will now find the irreducible representations of dimension 3. Let

$$V_{10} = \mathrm{Span}(x, y, z) \simeq \mathbb{C}^3.$$

Again, we let the basis elements correspond to the standard basis vectors in $\mathbb{C}^3$. Then

$$\begin{aligned}
\rho_{10} \colon H_3 &\to \mathrm{GL}(V_{10}) \\
\sigma &\mapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \\
\tau &\mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & \epsilon & 0 \\ 0 & 0 & \epsilon^2 \end{pmatrix}
\end{aligned}$$

is a representation of dimension 3. The matrices of σ and τ have no common eigenvectors, hence the 3-dimensional representation V_{10} is irreducible. Its character χ_{10} is given in Appendix A.2. Now we consider the vector space

$$\mathrm{Span}(x^2, y^2, z^2, xy, xz, yz) \simeq \mathbb{C}^6.$$

We have that

$$\begin{aligned}
H_3 &\to \mathrm{GL}(\mathrm{Span}(x^2, y^2, z^2, xy, xz, yz)) \\
\sigma &\mapsto (e_2 \ e_3 \ e_1 \ e_6 \ e_4 \ e_5) \\
\tau &\mapsto (e_1 \ \epsilon^2 e_2 \ \epsilon e_1 \ \epsilon e_4 \ \epsilon^2 e_5 \ e_6)
\end{aligned}$$

is a representation of dimension 6, with the following sub-representations.

- Let $V_{11} = \text{Span}(x^2, z^2, y^2)$. Then

$$\begin{aligned} \rho_{11} \colon H_3 &\to \text{GL}(V_{11}) \\ \sigma &\mapsto \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \\ \tau &\mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & \epsilon & 0 \\ 0 & 0 & \epsilon^2 \end{pmatrix} \end{aligned}$$

  is a sub-representation. The matrices for σ and τ have no common eigenvectors, hence the representation is irreducible. Its character χ_{11} is given in Appendix A.2.

- Let $V'_{11} = \text{Span}(yz, xy, xz)$. Then

$$\begin{aligned} \rho'_{11} \colon H_3 &\to \text{GL}(V'_{11}) \\ \sigma &\mapsto \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \\ \tau &\mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & \epsilon & 0 \\ 0 & 0 & \epsilon^2 \end{pmatrix} \end{aligned}$$

  is a sub-representation. We notice that this representation has the same character as V_{11}, so they are isomorphic representations.

We have found nine 1-dimensional and two 3-dimensional representations of H_3. Since there are exactly 11 conjugacy classes of H_3, and we have found 11 irreducible sub-representations of H_3, we can conclude that we have found all the irreducible representations of H_3. The conjugacy classes and the character table can be found in Appendix A.

5.5 The multiplication-by-n isogeny

Let f_i be the polynomials found in the 1-dimensional representations of H_3. From [Fri02] we have the following formula for the multiplication-by-3 isogeny on Hessian curves.

Proposition 5.5.1 ([Fri02, p. 22])**.** *Let E_λ be an elliptic curve on Hessian form. The isogeny $[3] \colon E_\lambda \to E_\lambda$ is given by*

$$[3](x_0 : x_1 : x_2) = (f_1 f_2 f_3 : f_4 f_5 f_6 : f_7 f_8 f_9).$$

Furthermore, recall from Section 3.5 that P_m denotes the polynomial such that $Z(P_m)$ intersects each elliptic curve $E_\lambda \in \mathcal{H}$ in exactly the m-torsion points. From [Fri02] we have a formula for the multiplication-by-n isogeny on Hessian curves when $n \neq 0 \mod 3$. The claim is proven in [Fri02] for $n \leq 10$.

Claim 5.5.2 ([Fri02, p. 17])**.** *Let E_λ be an elliptic curve on Hessian form, and let $n \neq 0 \mod 3$. The isogeny $[n]\colon E_\lambda \to E_\lambda$ is given by*

$$\begin{aligned}[n](x_0 : x_1 : x_2) &= (F_0 : F_1 : F_2) \\ &= (x_0 \prod_{m|n}(P_m)(\tau P_m)(\tau^2 P_m) : \\ &\quad \sigma^n(x_0) \prod_{m|n}(\sigma^n P_m)(\tau\sigma^n P_m)(\tau^2\sigma^n P_m) : \\ &\quad \sigma^{-n}(x_0) \prod_{m|n}(\sigma^{-n} P_m)(\tau\sigma^{-n} P_m)(\tau^2\sigma^{-n} P_m)).\end{aligned}$$

We recall that P_m is of degree $\frac{a_m}{3}$, where a_m is the number of primitive m-torsion points. Then each F_i is of degree $1 + \sum_{m|n}\left(3 \cdot \frac{a_m}{3}\right)$, which is equal to the number of n-torsion points. Thus the polynomials are of lowest possible degree.

Example 5.5.3. For $n = 2$ we have $[2] = (F_0 : F_1 : F_2)$, where

$$\begin{aligned}F_0 &= x_0(x_1 - x_2)(\epsilon x_1 - \epsilon^2 x_2)(\epsilon^2 x_1 - \epsilon x_2) \\ F_1 &= x_2(x_0 - x_1)(x_0 - \epsilon x_1)(x_0 - \epsilon^2 x_1) \\ F_2 &= x_1(x_2 - x_0)(\epsilon^2 x_2 - x_0)(\epsilon x_2 - x_0).\end{aligned}$$

Example 5.5.4. We will show that the vector spaces spanned by $F_0,\ F_1,\ F_2$ for each $n \neq 0 \mod 3$ are representations of H_3 of dimension 3. First we consider the case $n = 1 \mod 3$. Then

$$\begin{aligned}\sigma(F_0) &= \sigma\left(x_0 \prod_{m|n}(P_m)(\tau P_m)(\tau^2 P_m)\right) \\ &= \sigma(x_0) \prod_{m|n}(\sigma P_m)(\sigma\tau P_m)(\sigma\tau^2 P_m) \\ &= \sigma(x_0) \prod_{m|n}(\sigma P_m)(\epsilon^2\tau\sigma P_m)(\epsilon\tau^2\sigma P_m) \\ &= \epsilon^3\sigma(x_0) \prod_{m|n}(\sigma P_m)(\tau\sigma P_m)(\tau^2\sigma P_m) \\ &= F_1,\end{aligned}$$

$$\begin{aligned}\sigma(F_1) &= \sigma\left(\sigma(x_0) \prod_{m|n}(\sigma P_m)(\tau\sigma P_m)(\tau^2\sigma P_m)\right) \\ &= \sigma^2(x_0) \prod_{m|n}(\sigma^2 P_m)(\sigma\tau\sigma P_m)(\sigma\tau^2\sigma P_m) \\ &= \sigma^{-1}(x_0) \prod_{m|n}(\sigma^{-1} P_m)(\epsilon^2\tau\sigma^2 P_m)(\epsilon\tau^2\sigma^2 P_m) \\ &= \epsilon^3\sigma^{-1}(x_0) \prod_{m|n}(\sigma^{-1} P_m)(\tau\sigma^{-1} P_m)(\tau^2\sigma^{-1} P_m)\end{aligned}$$

$$= F_2,$$

$$\begin{aligned}\sigma(F_2) &= \sigma\left(\sigma^{-1}(x_0)\prod_{m|n}(\sigma^{-1}P_m)(\tau\sigma^{-1}P_m)(\tau^2\sigma^{-1}P_m)\right)\\ &= x_0\prod_{m|n}(P_m)(\sigma\tau\sigma^{-1}P_m)(\sigma\tau^2\sigma^{-1}P_m)\\ &= x_0\prod_{m|n}(P_m)(\epsilon^2\tau P_m)(\epsilon\tau^2 P_m)\\ &= \epsilon^3 x_0\prod_{m|n}(P_m)(\tau P_m)(\tau^2 P_m)\\ &= F_0.\end{aligned}$$

Furthermore, we have that

$$\begin{aligned}\tau(F_0) &= \tau\left(x_0\prod_{m|n}(P_m)(\tau P_m)(\tau^2 P_m)\right)\\ &= F_0,\end{aligned}$$

$$\begin{aligned}\tau(F_1) &= \tau\left(\sigma(x_0)\prod_{m|n}(\sigma P_m)(\tau\sigma P_m)(\tau^2\sigma P_m)\right)\\ &= \epsilon\sigma(x_0)\prod_{m|n}(\tau\sigma P_m)(\tau^2\sigma P_m)(\sigma P_m)\\ &= \epsilon F_1,\end{aligned}$$

$$\begin{aligned}\tau(F_2) &= \tau\left(\sigma^{-1}(x_0)\prod_{m|n}(\sigma^{-1}P_m)(\tau\sigma^{-1}P_m)(\tau^2\sigma^{-1}P_m)\right)\\ &= \epsilon^2\sigma^{-1}(x_0)\prod_{m|n}(\tau\sigma^{-1}P_m)(\tau^2\sigma^{-1}P_m)(\sigma^{-1}P_m)\\ &= \epsilon^2 F_2.\end{aligned}$$

This shows that in the case $n = 1 \mod 3$ the vector space $\mathrm{Span}(F_0, F_1, F_2)$ is a representation of H_3, more precisely the representation with character χ_{10}.

We can show, in a similar fashion, that for $n = 2 \mod 3$ we get that $\mathrm{Span}(F_0, F_1, F_2)$ is the other representation of dimension 3, namely the representation with character χ_{11}. So let $n = -1 \mod 3$. Then

$$\begin{aligned}\sigma(F_0) &= \sigma\left(x_0\prod_{m|n}(P_m)(\tau P_m)(\tau^2 P_m)\right)\\ &= \sigma(x_0)\prod_{m|n}(\sigma P_m)(\sigma\tau P_m)(\sigma\tau^2 P_m)\end{aligned}$$

$$
\begin{aligned}
&= \sigma(x_0) \prod_{m|n} (\sigma P_m)(\epsilon^2 \tau\sigma P_m)(\epsilon\tau^2\sigma P_m) \\
&= \epsilon^3 \sigma(x_0) \prod_{m|n} (\sigma P_m)(\tau\sigma P_m)(\tau^2\sigma P_m) \\
&= F_2,
\end{aligned}
$$

$$
\begin{aligned}
\sigma(F_1) &= \sigma\left(\sigma^{-1}(x_0) \prod_{m|n} (\sigma^{-1} P_m)(\tau\sigma^{-1} P_m)(\tau^2\sigma^{-1} P_m)\right) \\
&= x_0 \prod_{m|n} (P_m)(\sigma\tau\sigma^{-1} P_m)(\sigma\tau^2\sigma^{-1} P_m) \\
&= x_0 \prod_{m|n} (P_m)(\epsilon^2\tau P_m)(\epsilon\tau^2 P_m) \\
&= \epsilon^3 x_0 \prod_{m|n} (P_m)(\tau P_m)(\tau^2 P_m) \\
&= F_0,
\end{aligned}
$$

$$
\begin{aligned}
\sigma(F_2) &= \sigma\left(\sigma(x_0) \prod_{m|n} (\sigma P_m)(\tau\sigma P_m)(\tau^2\sigma P_m)\right) \\
&= \sigma^2(x_0) \prod_{m|n} (\sigma^2 P_m)(\sigma\tau\sigma P_m)(\sigma\tau^2\sigma P_m) \\
&= \sigma^{-1}(x_0) \prod_{m|n} (\sigma^{-1} P_m)(\epsilon^2\tau\sigma^2 P_m)(\epsilon\tau^2\sigma^2 P_m) \\
&= \epsilon^3 \sigma^{-1}(x_0) \prod_{m|n} (\sigma^{-1} P_m)(\tau\sigma^{-1} P_m)(\tau^2\sigma^{-1} P_m) \\
&= F_1.
\end{aligned}
$$

Furthermore, we have that

$$
\begin{aligned}
\tau(F_0) &= \tau\left(x_0 \prod_{m|n} (P_m)(\tau P_m)(\tau^2 P_m)\right) \\
&= F_0,
\end{aligned}
$$

$$
\begin{aligned}
\tau(F_1) &= \tau\left(\sigma^{-1}(x_0) \prod_{m|n} (\sigma^{-1} P_m)(\tau\sigma^{-1} P_m)(\tau^2\sigma^{-1} P_m)\right) \\
&= \epsilon\sigma^{-1}(x_0) \prod_{m|n} (\tau\sigma^{-1} P_m)(\tau^2\sigma^{-1} P_m)(\sigma P_m) \\
&= \epsilon F_1,
\end{aligned}
$$

$$\begin{aligned}\tau(F_2) &= \tau\left(\sigma(x_0)\prod_{m|n}(\sigma P_m)(\tau\sigma P_m)(\tau^2\sigma P_m)\right)\\ &= \epsilon^2\sigma(x_0)\prod_{m|n}(\tau\sigma P_m)(\tau^2\sigma P_m)(\sigma P_m)\\ &= \epsilon^2 F_2.\end{aligned}$$

This shows that for $n = 2 \mod 3$, $\mathrm{Span}(F_0, F_1, F_2)$ is isomorphic to the representation of H_3 with character χ_{11}.

For cryptographic purposes, we are interested in isogenies $\phi\colon E_\lambda \to E_{\lambda'}$ between Hessian curves where the kernel is a *subgroup* of $E_\lambda[n]$. Inspired by [Fri02] we started our search for such isogeny formulas by looking at the representations of H_3. In the next chapter we will derive new formulas for isogenies of degree 2, 3 and 4 between Hessian curves, and the Heisenberg group will play an important role in these formulas. The reprensentations of H_3 will also appear in the formulas for some special morphisms in Chapter 7.

PART II

Isogenies and other morphisms

CHAPTER 6

Isogenies between Hessian curves

In this chapter we derive formulas for isogenies of degree 3 between Hessian curves. Furthermore, we look at the existing formula for isogenies between Hessian curves of degree $n \neq 0 \mod 3$, found in [Bro+21]. We derive formulas that give many other representatives for the isogenies of degree 2 and 4. This results in simpler representatives for the latter case, compared to [Bro+21].

6.1 Isogenies of degree 3

In [Bro+21] there are formulas for 3-isogenies between *twisted* Hessian curves, but these cannot be restricted to Hessian curves. We derive such formulas for Hessian curves, with help from representation theory.

Recall the nine polynomials $f_1, \ldots, f_9$ found in the 1-dimensional representations of the Heisenberg group H_3. Since we wanted to find isogenies

$$\phi\colon E_\lambda \xrightarrow{(G_0:G_1:G_2)} E_{\lambda'}$$

with $\ker\phi = \langle p \rangle$ for a primitive 3-torsion point p, and suspected that the G_i-s would be representations of the H_3, we presumed that the isogenies were on the form

$$(k_0 f_i : k_1 f_j : k_2 f_l).$$

We used [Macaulay2] (see Appendix B.1) to find solutions $(k_0, k_1, k_2, \lambda')$ to

$$F(x,y,z) = (k_0 f_i)^3 + (k_1 f_j)^3 + (k_2 f_l^3) + \lambda'(k_0 f_i)(k_1 f_j)(k_2 f_l) = 0$$

for different combinations of polynomials f_i, f_j, f_l. The results are given in Proposition 6.1.1 and Proposition 6.1.2.

Proposition 6.1.1. *Let E_λ be an elliptic curve on Hessian form. The map $\phi\colon E_\lambda \to E_{\lambda'}$ given by*

$$\begin{aligned}\phi(x:y:z) &= (kf_1 : f_2 : f_3) \\ &= (kxyz : x^3 + \epsilon^2 y^3 + \epsilon z^3 : x^3 + \epsilon y^3 + \epsilon^2 z^3)\end{aligned}$$

is an isogeny with kernel

$$G = \{(0:1:-1), (0:1:-\epsilon), (0:1:-\epsilon^2)\}$$

where $k^3 = -\lambda^3 - 27$ *and* $\lambda' = \frac{3\lambda}{k}$.

Proof. Since ϕ is given by polynomials, it is a rational map. By Proposition 2.3.3 we get that ϕ is a morphism. Furthermore we show that $\operatorname{im}\phi = E_{\lambda'}$. We use [Macaulay2] to check that

$$F(x, y, z) = (kf_1)^3 + f_2^3 + f_3^3 + \lambda' k f_1 f_2 f_3 = 0,$$

so $\operatorname{im}\phi \subseteq E_{\lambda'}$. Recall that elliptic curves are irreducible by definition, and that a morphism is a continuous map (with respect to the Zariski topology). By Proposition 2.3.9 the image of ϕ is irreducible, and by Remark 2.2.6 it is also closed. This means that $\operatorname{im}\phi = E_{\lambda'}$.

We use [Macaulay2] to check that $Z_+(f_1) \cap Z_+(f_2 + f_3) = G$. We also check that $Z_+(kf_1) \cap Z_+(f_2) \cap Z_+(f_3) = \emptyset$. This shows that there are no points where (this representation of) ϕ is not defined. We conclude that $\ker\phi = G$. The [Macaulay2] code can be found in Appendix B.2. ■

Proposition 6.1.2. *Let* E_λ *be an elliptic curve on Hessian form, and let* c *be a third root of* 1. *The map* $\phi\colon E_\lambda \to E_{\lambda'}$ *given by*

$$\phi(x : y : z) = (kxyz : x^2y + cy^2z + c^2z^2x : x^2z + c^2y^2x + cz^2y)$$

is an isogeny with kernel

$$G = \{(0 : 1 : -1), (1 : 0 : -c), (1 : -c : 0)\}$$

where $k^3 = c\lambda^2 - 3c^2\lambda + 9$ *and* $\lambda' = \frac{c\lambda - 6c^2}{k}$.

Proof. This proof is similar to the proof of Proposition 6.1.1. We consider the three cases $c = 1, \epsilon, \epsilon^2$.

- Let $c = 1$. Then $\phi = (kf_1 : f_4 : f_7)$. Since ϕ is given by polynomials, it is a rational map. By Proposition 2.3.3 we get that ϕ is a morphism. Now we show that $\operatorname{im}\phi = E_{\lambda'}$. We use [Macaulay2] to check that

  $$F(x, y, z) = (kf_1)^3 + f_4^3 + f_7^3 + \lambda' k f_1 f_4 f_7 = 0,$$

  so $\operatorname{im}\phi \subseteq E_{\lambda'}$. Recall that elliptic curves are irreducible by definition, and that a morphism is a continuous map (with respect to the Zariski topology). By Proposition 2.3.9 the image of ϕ is irreducible, and by Remark 2.2.6 it is also closed. This means that $\operatorname{im}\phi = E_{\lambda'}$.

  We check using Macaulay that $Z_+(kf_1) \cap Z_+(f_4 + f_7) = G$. We also check that $Z_+(kf_1) \cap Z_+(f_4) \cap Z_+(f_7) = \emptyset$. This shows that there are no points where (this representation of) ϕ is not defined. We conclude that $\ker\phi = G$.

- Let $c = \epsilon$. Then $\phi = (kf_1 : f_6 : f_8)$. The proof follows analogously.

- Let $c = \epsilon^2$. Then $\phi = (kf_1 : f_5 : f_9)$. The proof follows analogously.

The [Macaulay2] code can be found in Appendix B.3. ■

Remark 6.1.3. In total, we have used all the nine 1-dimensional representations of H_3 to find 3-isogenies between Hessian curves.

6.2 Isogenies of degree n

In this section we give the formula found in [Bro+21] for isogenies of degree $n \neq 0 \mod 3$ between twisted Hessian curves, which can be restricted to isogenies between Hessian curves. Furthermore we give examples using this formula for isogenies of degree 2 and 4 on Hessian curves, where we also find many, possibly all, other representatives of these isogenies.

Definition 6.2.1. A **twisted Hessian curve** over a field K is a projective curve $H(a,d)$ defined by $ax^3+y^3+z^3=dxyz$ with the specified point $(0:1:-1)$ as additive identity in $\mathbb{P}^2$, with $a,d \in K$ and $a(27a-d^3) \neq 0$.

Note that when $a=1$ we have an ordinary Hessian curve. The addition formulas for twisted Hessian curves are generalizations of the formulas for Hessian curves. We give the formulas for addition on twisted Hessian curves here, because they are a part the formula for isogenies between twisted Hessian curves below.

Theorem 6.2.2 ([Ber+15, Theorem 3.1, 3.2, 4.2])**.** *Let $p_1=(x_1:y_1:z_1)$, $p_2=(x_2:y_2:z_2) \in \mathbb{P}^2_k$ on an twisted Hessian curve $H(a,d)$. Let*

$$(x:y:z) = (x_2^2y_1z_1 - x_1^2y_2z_2 : z_2^2x_1y_1 - z_1^2x_2y_2 : y_2^2x_1z_1 - y_1^2x_2z_2),$$

and

$$(x':y':z') = (z_2^2x_1z_1 - y_1^2x_2y_2 : y_2^2y_1z_1 - ax_1^2x_2z_2 : ax_2^2x_1y_1 - z_1^2y_2z_2).$$

When $(x:y:z) \neq (0:0:0)$ then p_1+p_2 is equal to $(x:y:z)$, and if $(x':y':z') \neq (0:0:0)$ then p_1+p_2 is equal to $(x':y':z')$.

Theorem 6.2.3 ([Bro+21, Theorem 4.])**.** *Let $F = \{(0:-1:1)\} \cup \{(s_i:t_i:1)\}_{i=1}^{n-1}$ be a finite, cyclic subgroup of $H(a,d)$ of order n, where n is not divisible by 3. Then F is the kernel of an isogeny from $H(a,d)$ to $H(A,D)$ defined by*

$$\begin{aligned}\phi(P) &= (G_0:G_1:G_2)\\ &= \left(\prod_{R\in F} X(P+R) : \prod_{R\in F} Y(P+R) : \prod_{R\in F} Z(P+R)\right),\end{aligned}$$

where $A=a^n$ and

$$D = \frac{(1-2(n-1))d + 6\sum_{i=1}^{n-1}\frac{1}{s_it_i}}{\prod_{i=1}^{n-1} s_i}.$$

By $X(P+R)$ we mean the X-coordinate of the point $P+R$, and so on. We note that the polynomials G_i have degree $1+2(n-1)$, because $P+\mathcal{O}=(x:y:z)$ and for any other $R \in F$ then $P+R$ is given by polynomials of degree 2. We also note that if the starting curve is an ordinary Hessian curve, then the image curve is always an ordinary Hessian curve. Thus the formula can be restricted to ordinary Hessian curves.

Example 6.2.4. Let $H(1,-\lambda)$ be an ordinary Hessian curve E_λ, with subgroup

$$F = \{\mathcal{O}, (s:1:1)\} = \{(0:-1:1), (s:1:1)\}.$$

Using the addition formula we get

$$\begin{aligned} P + (0:-1:1) &= (x:y:z) + (0:-1:1) \\ &= (x:y:z), \end{aligned}$$

and

$$\begin{aligned} P + (s:1:1) &= (x:y:z) + (s:1:1) \\ &= (s^2yz - x^2 : xy - sz^2 : xz - sy^2). \end{aligned}$$

Then F is the kernel of an isogeny from $H(1,-\lambda)$ to the Hessian curve $H(1, \frac{\lambda}{s} + \frac{6}{s^2})$, defined by

$$\phi(P) = \left(x(s^2yz - x^2) : y(xy - sz^2) : z(xz - sy^2)\right).$$

We notice that this representative of ϕ is not defined at the primitive 2-torsion point. We resolve the indeterminacies of this map to show that this point is mapped to $\mathcal{O}$. For simplicity consider the specific example where $s = -1$ and $\lambda = 1$. Since the computation is local we assume $z = 1$, and we have to show that $p = (-1, 1)$ maps to $(0:-1:1)$. The blowup of the affine plane $\mathbb{A}^2$ in p is defined as

$$\mathrm{Bl}_p \mathbb{A}^2 = \{(x,y) \times [u:v] : (x+1)v - (y-1)u = 0\}.$$

We can explicitly compute $\mathrm{Bl}_p E_d$ by computing the strict transform of E_d in $\mathrm{Bl}_p \mathbb{A}^2$;

$$\begin{aligned} \mathrm{Bl}_p E_d = Z(&yu - xv - u - v, x^2u + y^2v - xu + xv + yv + 2u + v, \\ &x^3 + y^3 + xy + 1). \end{aligned}$$

We check that the point p corresponds to the point $((-1,1), [-\frac{1}{2} : 1])$, so we assume $v = 1$. Then we can substitute $x = u(y-1) - 1$, and the blowup becomes

$$\begin{aligned} U &= Z(u^3(y^2 - 2y + 1) + u^2(3 - 3y) + u(3 + y) + y^2 + y) \\ &= Z(u^3(y^2-1)^2 - 3u^2(y-1) + u(y+3) + y(y+1)). \end{aligned}$$

We have the following diagram, which is commutative. Here, π is the projection given by $\pi((u,y)) = (u(y-1) - 1, y)$.

$$\begin{array}{ccc} U & & \\ {\scriptstyle\pi}\downarrow & \searrow^{\psi} & \\ E & \overset{\phi}{\dashrightarrow} & \mathbb{P}^2 \end{array}$$

We compute the map $\psi = \phi \circ \pi$, and get

$$\begin{aligned} G_0(u(y-1)-1, y) &= (y-1)(yu - u - 1)(yu^2 - u^2 - 2u - 1) \\ G_1(u(y-1)-1, y) &= (y-1)y(1 - yu) \\ G_2(u(y-1)-1, y) &= (y-1)y(-y - u - 1). \end{aligned}$$

We may cancel the $(y-1)$ term, so

$$\begin{aligned}\psi(u,y) &= (G_0 : G_1 : G_2) \\ &= \left(\frac{G_0}{y-1} : \frac{G_1}{y-1} : \frac{G_2}{y-1}\right).\end{aligned}$$

Then we get

$$\begin{aligned}\psi\left(-\frac{1}{2}, 1\right) &= \left(0 : \frac{3}{2} : \frac{-3}{2}\right) \\ &= (0 : -1 : 1),\end{aligned}$$

so $\phi(p) = \mathcal{O}$. Finally, we remark that when calculating point addition $p_1 + p_2$ on Hessian curves, we distinguish between the two cases $p_1 \neq p_2$ and $p_1 = p_2$. So when evaluating ϕ in the 2-torsion point $(s : 1 : 1)$ in the kernel we actually have

$$\begin{aligned}\phi(s:1:1) &= (s(s\cdot 1^3 - s\cdot 1^3) : 1\cdot(1^3\cdot 1 - s^3\cdot 1) : 1\cdot(s^3\cdot 1 - 1\cdot 1^3)) \\ &= (0 : 1 - s^3 : s^3 - 1) \\ &= (0 : 1 : -1).\end{aligned}$$

Example 6.2.5. Let E_λ be an elliptic curve on Hessian form, and $G = \{(0:1:-1), (s_1:t_1:1), (s_2:t_2:1), (s_3:t_3:1)\}$ the subgroup generated by a primitive 4-torsion point $(s_1 : t_1 : 1)$. Then $\phi\colon E_\lambda \to E_{\lambda'}$ given by

$$\begin{aligned}\phi = (&x(s_1^2yz - x^2t_1)(s_2^2yz - x^2t_2)(s_3^2yz - x^2t_3) : \\ &y(xy - z^2s_1t_1)(xy - z^2s_2t_2)(xy - z^2s_3t_3) : \\ &z(t_1^2xz - y^2s_1)(t_2^2xz - y^2s_2)(t_3^2xz - y^2s_3))\end{aligned}$$

is an isogeny with kernel G. We see that this map is given by polynomials of degree 7.

Ideally, we would want n-isogenies to be represented by polynomials of degree n, instead of $1 + 2(n-1)$. We use the following proposition to find many, possibly all, the representatives of the isogenies given in Theorem 6.2.3, in the cases where $n = 2$ and $n = 4$.

Proposition 6.2.6 ([Bot+19, Proposition 2.1.])**.** *Let X be a projective variety and let $R = S(X)$ be the homogeneous coordinate ring of X. Let $F\colon X \dashrightarrow \mathbb{P}^m$ be a rational map and let $\mathbf{f} = \{f_0, \ldots, f_m\}$ be a representative of F with $f_i \in R$ (homogeneous of degree d for all i). Set $I = (f_0, \ldots, f_m)$. Then the set of such representatives of F corresponds bijectively to the homogeneous vectors in the rank 1 graded R-module $Hom_R(I, R) \simeq (R :_K I)$.*

Remark 6.2.7 ([Bot+19, p. 2]). The bijection comes from multiplying our fixed representative $\mathbf{f}$ of F by $h \in (R :_K I)$. Now, in the setting of Proposition 6.2.6 let

$$\bigoplus_s R(d_s) \xrightarrow{\mu} R(-d)^{m+1} \xrightarrow{[f_0,\ldots,f_m]} I \to 0$$

be a free resolution of I. Then we get

$$0 \to \mathrm{Hom}_R(I,R) \to (R(-d)^{m+1})^\vee \xrightarrow{\mu^T} \left(\bigoplus_s R(d_s)\right)^\vee$$

where μ^T is the transpose of μ and $M^\vee = \mathrm{Hom}_R(M,R)$ for any R-module M. Thus we get that $\mathrm{Hom}_R(I,R) \simeq \ker \mu^T$, and each representative of F corresponds to a vector in $\ker \mu^T$. The correspondence takes a representative $(hf_0,\dots,hf_m)$ to the map that multiplies vectors in R^{m+1} by $[hf_0,\dots,hf_m]$ on the left.

Example 6.2.8. Let E_λ be a Hessian curve with $\lambda = \frac{15\epsilon}{4}$, where ϵ is a primitive third root of unity. Recall from Section 3.5 that the intersection between E_λ and the line $Z_+(y-z)$ is exactly the three primitive 2-torsion points on E_λ. For instance, we find that $p = (\frac{-\epsilon^2}{2} : 1 : 1)$ is a 2-torsion point on E_λ. We use Theorem 6.2.3 to find the isogeny $\phi\colon E_\lambda \to E_{\lambda'}$ such that $\ker\phi = \{\mathcal{O}, p\}$. We get that

$$\phi = \left(x(s^2yz - x^2) : y(xy - sz^2) : z(xz - sy^2)\right),$$

where $s = \frac{-\epsilon^2}{2}$, and $\lambda' = -\frac{33\epsilon^2}{2}$. Then we use Proposition 6.2.6 to find all the representatives of this map. In particular, we calculate $\ker \mu^T$ where μ^T is given as in Remark 6.2.7. We find using [Macaulay2] that $\ker \mu^T$ is generated by the three vectors

$$\mathbf{u} = \begin{pmatrix} y^3 + 4\epsilon xyz + z^3 \\ xy^2 + \frac{\epsilon^2}{2}yz^2 \\ \frac{\epsilon^2}{2}y^2z + xz^2 \end{pmatrix},\ \mathbf{v} = \begin{pmatrix} xy^2 + 2\epsilon x^2z \\ x^2y + 2\epsilon y^2z \\ \frac{\epsilon^2}{2}xyz - 2\epsilon z^3 \end{pmatrix},\ \mathbf{w} = \begin{pmatrix} x^2y + \frac{\epsilon^2}{2}xz^2 \\ -y^3 + \frac{\epsilon}{4}xyz \\ \frac{\epsilon^2}{2}x^2z + yz^2 \end{pmatrix}.$$

We use the relation $x^3 + y^3 + z^3 + \frac{15\epsilon}{4}xyz = 0$ and rewrite these vectors to

$$\mathbf{u} = \begin{pmatrix} (\frac{\epsilon^2}{2})^2xyz - x^3 \\ xy^2 + \frac{\epsilon^2}{2}yz^2 \\ xz^2 + \frac{\epsilon^2}{2}y^2z \end{pmatrix}$$

$$\mathbf{v} = \begin{pmatrix} 2\epsilon(zx^2 + \frac{\epsilon^2}{2}xy^2) \\ 2\epsilon(zy^2 + \frac{\epsilon^2}{2}x^2y) \\ 2\epsilon((\frac{\epsilon^2}{2})^2xyz - z^3) \end{pmatrix}$$

$$\mathbf{w} = \begin{pmatrix} yx^2 + \frac{\epsilon^2}{2}z^2x \\ (\frac{\epsilon^2}{2})^2xyz - y^3 \\ yz^2 + \frac{\epsilon^2}{2}zx^2 \end{pmatrix}.$$

The vectors $\mathbf{u},\mathbf{v},\mathbf{w}$ generate all the representatives of the original map ϕ. In particular, a representative of ϕ is on the form $\phi' = (G_0 : G_1 : G_2)$ such that

$$\begin{pmatrix} G_0 \\ G_1 \\ G_2 \end{pmatrix} = f\mathbf{u} + g\mathbf{v} + h\mathbf{w},$$

where $f,g,h \in S(E_\lambda)$ are homogeneous of the same degree. When f,g,h are constants we get the lowest possible degree of the polynomials G_i, which is

3. Now let $\mathbf{v}' = \frac{1}{2\epsilon}v$, and let u_0, u_1, u_2 denote the entries in $\mathbf{u}$. We have the following relation between the vectors.

$$\mathbf{u} = \begin{pmatrix} u_0 \\ u_1 \\ u_2 \end{pmatrix}, \ \mathbf{v}' = \begin{pmatrix} \sigma^2(u_1) \\ \sigma^2(u_2) \\ \sigma^2(u_0) \end{pmatrix}, \ \mathbf{w} = \begin{pmatrix} \sigma(u_2) \\ \sigma(u_0) \\ \sigma(u_1) \end{pmatrix}.$$

The [Macaulay2] code can be found in Appendix B.4.

Example 6.2.9. Let E_λ be a Hessian curve with $\lambda = 1$. Recall from Section 3.5 that the intersection between E_λ and the line $Z_+(x^3y + x^3z - y^3z - z^3y)$ is exactly the twelve primitive 4-torsion points on E_λ. For instance, we find that $p_1 = (\frac{1-b}{2} : \frac{ab-a-b-1}{2} : 1)$ is a 4-torsion point on E_λ, where $a = \sqrt{2}$ and $b = \sqrt{5+4\sqrt{2}}$. Now, we use Theorem 6.2.3 to find the isogeny $\phi\colon E_\lambda \to E_{\lambda'}$ such that $\ker\phi = \langle p_1 \rangle = \{\mathcal{O}, p_1, p_2, p_3\}$. We get that

$$\begin{aligned}\phi = (&x(s_1^2yz - x^2t_1)(s_2^2yz - x^2t_2)(s_3^2yz - x^2t_3) : \\ &y(xy - z^2s_1t_1)(xy - z^2s_2t_2)(xy - z^2s_3t_3) : \\ &z(t_1^2xz - y^2s_1)(t_2^2xz - y^2s_2)(t_3^2xz - y^2s_3))\end{aligned}$$

where $p_i = (s_i : t_i : 1)$. Then we use Proposition 6.2.6 to find all the representatives of this map. In particular, we calculate $\ker\mu^T$ where μ^T is given as in Remark 6.2.7. We find using [Macaulay2] that $\ker\mu^T$ is generated by the three vectors

$$\begin{aligned}\mathbf{u} &= \begin{pmatrix} xy^4 - ax^2y^2z + (-a+1)xyz^3 + z^5 \\ y^5 + axyz^3 + (-a-1)x^2yz^2 \\ (a+1)y^4z - x^2z^3 + ayz^4 \end{pmatrix} \\ \mathbf{v} &= \begin{pmatrix} x^2y^3 + (a-1)y^4z + 2axy^2z^2 + x^2z^3 + (a-1)yz^4 \\ xy^4 + (a+1)x^2y^2z + y^3z^2 + (a+1)xyz^3 \\ (a+1)xy^3z + (a+1)x^2yz^2 + y^2z^3 + xz^4 \end{pmatrix} \\ \mathbf{w} &= \begin{pmatrix} -y^5 + (a-1)xy^3z + ax^2yz^2 - y^2z^3 - xz^4 \\ x^2y^3 - ay^4z + (-a-1)yz^4 \\ (a+1)x^2y^2z - axyz^3 - z^5 \end{pmatrix}.\end{aligned}$$

We use the relation $x^3 + y^3 + z^3 + xyz = 0$ and rewrite these vectors to

$$\begin{aligned}\mathbf{u} &= \begin{pmatrix} -(x^4y + x^3z^2 + (a+1)xyz^3 + (a+1)x^2y^2z) \\ -(x^3y^2 + y^2z^3 + (1-a)xy^3z + (a+1)x^2yz^2) \\ -(x^2z^3 + yz^4 + (a+1)x^3yz + (a+1)xy^2z^2) \end{pmatrix} \\ \mathbf{v} &= \begin{pmatrix} x^2z^3 + x^2y^3 + (1-a)x^3yz + (a+1)xy^2z^2 \\ y^3z^2 + xy^4 + (a+1)xyz^3 + (a+1)x^2y^2z \\ xz^4 + y^2z^3 + (a+1)xy^3z + (a+1)x^2yz^2 \end{pmatrix} \\ \mathbf{w} &= \begin{pmatrix} x^3y^2 + x^4z + (a+1)xy^3z + (a+1)x^2yz^2 \\ y^4z + x^2y^3 + (a+1)x^3yz + (a+1)xy^2z^2 \\ y^3z^2 + x^3z^2 + (1-a)xyz^3 + (a+1)x^2y^2z \end{pmatrix}.\end{aligned}$$

The vectors $\mathbf{u}, \mathbf{v}, \mathbf{w}$ generates all the representatives of the original map ϕ. In particular, a representative of ϕ is on the form $\phi' = (G_0 : G_1 : G_2)$ such that

$$\begin{pmatrix} G_0 \\ G_1 \\ G_2 \end{pmatrix} = f\mathbf{u} + g\mathbf{v} + h\mathbf{w},$$

where $f, g, h \in S(E_\lambda)$ are homogeneous of the same degree. When f, g, h are constants we get the lowest possible degree of the polynomials G_i, which is 5. Now let $\mathbf{u}' = -\mathbf{u}$, and let u_0, u_1, u_2 denote the entries in $\mathbf{u}'$. We notice the following relation between the vectors.

$$\mathbf{u}' = \begin{pmatrix} u_0 \\ u_1 \\ u_2 \end{pmatrix}, \ \mathbf{v} = \begin{pmatrix} \sigma^2(u_1) \\ \sigma^2(u_2) \\ \sigma^2(u_0) \end{pmatrix}, \ \mathbf{w} = \begin{pmatrix} \sigma(u_2) \\ \sigma(u_0) \\ \sigma(u_1) \end{pmatrix}.$$

The [Macaulay2] code can be found in Appendix B.5.

6.3 Isogenies of degree 2 and 4

By looking at patterns in several examples similar to Example 6.2.8 we found a general formula that gives many, possibly all, representatives of the 2-isogenies between Hessian curves.

Proposition 6.3.1. *Let E_λ be an elliptic curve on Hessian form, with a subgroup*

$$G = \{(0 : -1 : 1), (s : 1 : 1)\}.$$

Let

$$\begin{aligned} u_0 &= x(s^2yz - x^2) \\ u_1 &= y(xy - sz^2) \\ u_2 &= z(xz - s_2y^2), \end{aligned}$$

let $f, g, h \in S(E_\lambda)$ be homogeneous of the same degree, and let

$$\begin{aligned} G_0 &= fu_0 + g\sigma^2(u_1) + h\sigma(u_2) \\ G_1 &= fu_1 + g\sigma^2(u_2) + h\sigma(u_0) \\ G_2 &= fu_2 + g\sigma^2(u_0) + h\sigma(u_1). \end{aligned}$$

Then $\phi\colon E_\lambda \to E_{\lambda'}$ is an isogeny given by

$$\phi(x : y : z) = (G_0 : G_1 : G_2)$$

where $\lambda' = s - \frac{4}{s^2}$, and $\ker\phi = G$.

Proof. Since ϕ is given by polynomials, it is a rational map. By Proposition 2.3.3 ϕ is also a morphism. Now we show that $\operatorname{im}\phi = E_{\lambda'}$. We use [Macaulay2] to check that

$$F(x, y, z) = G_0^3 + G_1^3 + G_2^3 + \lambda' G_0 G_1 G_2 = 0,$$

so $\operatorname{im}\phi \subseteq E_{\lambda'}$. Recall that elliptic curves are irreducible by definition, and that a morphism is a continuous map (with respect to the Zariski topology). By Proposition 2.3.9 the image of ϕ is irreducible, and by Remark 2.2.6 it is also closed. This means that $\operatorname{im}\phi = E_{\lambda'}$.

We check using [Macaulay2] that the subgroup G is mapped to $\mathcal{O}$. It remains to show that the map is 2-to-1, because then $\ker\phi = G$. Assume for contradiction that the map is 3-to-1. We find using [Macaulay2] that $L = Z_+(G_0) \cap Z_+(G_1) \cap Z_+(G_2) \neq \emptyset$, so ϕ has base points (points where the map is not defined). By Bezout's theorem we have $|E_\lambda \cap L| \leq 9$, so there are at most 9 base points. We can find a line $l = Z_+(ax + by + cz) \subset \mathbb{P}^2$ such that $\phi^{-1}(l \cap E_{\lambda'})$ consists of 9 points, where none of these are base points. But

$$\phi^{-1}(l \cap E_{\lambda'}) = Z_+(aG_0 + bG_1 + cG_2) \cap E_\lambda,$$

which must necessarily contain all the base points, a contradiction.

This shows that the map is 2-to-1, so $\ker\phi = G$. The [Macaulay2] code can be found in Appendix B.6. ■

Note that the isogeny ϕ and the image curve $E_{\lambda'}$ only depends on the 2-torsion point $(s : 1 : 1)$. Furthermore, when f, g, h are constants then the G_i's are of degree 3, and otherwise the G_i's are of higher degree. When $f = 1$, $g = h = 0$ we have the representative given in Theorem 6.2.3. Also note that

$$\tau(u_0) = u_0,\ \tau(u_1) = \epsilon^2 u_1,\ \tau(u_2) = \epsilon u_2.$$

and if $f = g = h$ is a constant, we have

$$\sigma(G_0) = G_1,\ \sigma(G_1) = G_2,\ \sigma(G_2) = G_0.$$

Remark 6.3.2. We give an alternative proof of Proposition 6.3.1, using Proposition 6.2.6. We can simply show that the map $\phi = (G_0 : G_1 : G_2)$ is a representative of the isogeny given in Theorem 6.2.3. So let E_λ be a Hessian curve with a 2-torsion point $(s : 1 : 1)$, and let $\psi\colon E_\lambda \to E_{\lambda'}$ defined by

$$\begin{aligned}\psi &= (F_0 : F_1 : F_2)\\ &= (x(s^2yz - x^2) : y(xy - sz^2) : z(xz - sy^2))\end{aligned}$$

be the isogeny given in Theorem 6.2.3 having $\{\mathcal{O}, (s : 1 : 1)\}$ as kernel. By Remark 6.2.7 must show that $(G_0, G_1, G_2) = (kF_0, kF_1, kF_2)$ for some $k \in (R :_K I)$. We find using [Macaulay2] (see the end of Appendix B.6) that

$$\frac{G_0}{F_0} = \frac{G_1}{F_1} = \frac{G_2}{F_2},$$

so we can take $k = \frac{G_0}{F_0}$. This shows that the maps given in Proposition 6.3.1 are representatives of the 2-isogeny given in Theorem 6.2.3.

Again, by looking at patterns in several examples similar to Example 6.2.9 we found a general formula that gives many, possibly all, representatives of the 4-isogenies on Hessian curves. Note that this formula gives simpler representatives of the 4-isogenies compared to Theorem 6.2.3.

Proposition 6.3.3. *Let E_λ be an elliptic curve on Hessian form, with a cyclic subgroup*

$$G = \{(0 : -1 : 1)\} \cup \{(s_i : t_i : 1)\}_{i=1}^{3},$$

generated by a primitive 4-torsion point $(s_1 : t_1 : 1)$. Let

$$\begin{aligned} u_0 &= x(x^3y + K_1x^2z^2 + K_1K_2yz^3 + K_2xy^2z) \\ u_1 &= y(x^3y + K_1^2K_2x^2z^2 + yz^3 + (\frac{2}{K_1} - K_2)xy^2z) \\ u_2 &= z(K_1K_2x^3y + K_1x^2z^2 + yz^3 + K_2xy^2z), \end{aligned}$$

where

$$\begin{aligned} K_1 &= -s_2 = \frac{s_1t_1 + s_1}{t_1} \\ K_2 &= -s_1s_3 = \frac{-s_1^2}{t_1}. \end{aligned}$$

Let $f, g, h \in S(E_\lambda)$ be homogeneous of the same degree, and let

$$\begin{aligned} G_0 &= fu_0 + g\sigma^2(u_1) + h\sigma(u_2) \\ G_1 &= fu_1 + g\sigma^2(u_2) + h\sigma(u_0) \\ G_2 &= fu_2 + g\sigma^2(u_0) + h\sigma(u_1). \end{aligned}$$

Then $\phi\colon E_\lambda \to E_{\lambda'}$ is an isogeny given by

$$\phi(x : y : z) = (G_0 : G_1 : G_2)$$

where

$$\lambda' = \frac{-8s_1^3 + 4t_1^3 - 12t_1^2 - 12t_1 + 4}{4s_1t_1^2 + 4s_1},$$

and $\ker\phi = G$.

Proof. Since ϕ is given by polynomials, it is a rational map. By Proposition 2.3.3 we get that ϕ is a morphism. Now we show that $\operatorname{im}\phi = E_{\lambda'}$. We use [Macaulay2] to check that

$$F(x, y, z) = G_0^3 + G_1^3 + G_2^3 + \lambda' G_0G_1G_2 = 0,$$

so $\operatorname{im}\phi \subseteq E_{\lambda'}$. Recall that elliptic curves are irreducible by definition, and that a morphism is a continuous map (with respect to the Zariski topology). By Proposition 2.3.9 the image of ϕ is irreducible, and by Remark 2.2.6 it is also closed. Then $E_{\lambda'}$ must be the entire image, so $\operatorname{im}\phi = E_{\lambda'}$.

We check using [Macaulay2] that the subgroup G is mapped to $\mathcal{O}$. It remains to show that the map is 4-to-1, because then $\ker\phi = G$. We want to show that $L = Z_+(G_0) \cap Z_+(G_1) \cap Z_+(G_2) \neq \emptyset$, because then ϕ would have base points (points where the map is not defined), and the map cannot be 5-to-1, so it must

be 4-to-1. We could not find a way for [Macaulay2] to decompose the ideal (G_0, G_1, G_2), so we give an alternative proof.

The alternative proof is similar to Remark 6.3.2, and goes as follows using Proposition 6.2.6. We can simply show that the map $\phi = (G_0 : G_1 : G_2)$ is a representative of the isogeny given in Theorem 6.2.3. So let $\psi\colon E_\lambda \to E_{\lambda'}$ defined by

$$\begin{aligned}\psi &= (F_0 : F_1 : F_2)\\ &= (x(s_1^2yz - x^2t_1)(s_2^2yz - x^2t_2)(s_3^2yz - x^2t_3) :\\ &\quad y(xy - z^2s_1t_1)(xy - z^2s_2t_2)(xy - z^2s_3t_3) :\\ &\quad z(t_1^2xz - y^2s_1)(t_2^2xz - y^2s_2)(t_3^2xz - y^2s_3))\end{aligned}$$

be the isogeny given in Theorem 6.2.3 having G as kernel. By Remark 6.2.7 we must show that $(G_0, G_1, G_2) = (kF_0, kF_1, kF_2)$ for some $k \in (R :_K I)$. We find using [Macaulay2] that

$$\frac{G_0}{F_0} = \frac{G_1}{F_1} = \frac{G_2}{F_2},$$

so we can take $k = \frac{G_0}{F_0}$. This shows that the maps given in Proposition 6.3.3 are representatives of the 4-isogeny given in Theorem 6.2.3. The [Macaulay2] code can be found in Appendix B.7. ■

Note that the isogeny ϕ and the image curve $E_{\lambda'}$ only depends on the generator $(s_1 : t_1 : 1)$. Also notice that

$$\tau(u_0) = \epsilon u_0,\ \tau(u_1) = \epsilon^2 u_1,\ \tau(u_2) = u_2,$$

and if $f = g = h$ is a constant, we have

$$\sigma(G_0) = G_1,\ \sigma(G_1) = G_2,\ \sigma(G_2) = G_0.$$

Example 6.3.4. Let E_λ be the Hessian curve with $\lambda = \frac{15}{4}$, and let $\langle (s_1 : t_1 : 1)\rangle \subset E_{\frac{15}{4}}$ be the cyclic subgroup generated by the primitive 4-torsion point $(s_1 : t_1 : 1)$, where $s_1 = \frac{1}{4}(1 + \sqrt{33 + 24\sqrt{2}})$ and $t_1 = \frac{2s_1}{1-2s_1}$. Then we have the isogeny $\phi\colon E_\lambda \to E_{\lambda'}$ having G as kernel, where $\lambda' = \frac{189\sqrt{2}}{2} - 138$ and $\phi = (G_0 : G_1 : G_2)$ is given by, for instance

$$\begin{aligned}G_0 &= u_0 = x(x^3y + K_1x^2z^2 + K_1K_2yz^3 + K_2xy^2z)\\ G_1 &= u_1 = y(x^3y + K_1^2K_2x^2z^2 + yz^3 + (\frac{2}{K_1} - K_2)xy^2z)\\ G_2 &= u_2 = z(K_1K_2x^3y + K_1x^2z^2 + yz^3 + K_2xy^2z),\end{aligned}$$

where $K_1 = \frac{1}{2}$ and $K_2 = \frac{3}{2}\sqrt{2} + 2$. Here we chose the representative where $f = 1$ and $g = h = 0$.

CHAPTER 7

Morphisms between Hessian curves

In Chapter 6 we derived new isogeny formulas for 2-, 3- and 4-isogenies between ordinary Hessian curves. The 3-isogenies are given by the 1-dimensional representations of $H_3 = \langle \sigma, \tau \rangle$, and the 2- and 4-isogenies can be either σ- and τ-invariant, but not both. Curious about where the 3-dimensional representations of H_3 where hiding, we loosened the requirements and allowed the map $\phi\colon E_\lambda \to E_{\lambda'}$ to be a morphism (not necessarily an isogeny).

Let E_λ be a Hessian curve with a subgroup $\langle p \rangle$ generated by a primitive n-torsion point p. For $n = 2$ and $n = 3$ we will derive a formula for a morphism $\phi\colon E_\lambda \to E_{\lambda'}$ where the subgroup $\langle p \rangle$ is mapped to a primitive n-torsion point, and λ' is as given in Proposition 6.1.1, Proposition 6.1.2 or Proposition 6.3.1, respectively. We also describe how we think such morphisms can be constructed for a general $n \neq 0 \mod 3$. Furthermore, given an elliptic curve E_0 (not necessarily on Hessian form) and a subgroup $G \subset E_0$ of order 2^e, we present an algorithm to compute an isogeny having G as kernel. This isogeny is a composition of e morphisms (instead of isogenies) of degree 2 and a single translation morphism.

7.1 Morphisms of degree 2

Proposition 7.1.1. *Let E_λ be an elliptic curve on Hessian form, and let $(s : 1 : 1)$ be a 2-torsion point on E_λ. Then $\phi\colon E_\lambda \xrightarrow{(G_0:G_1:G_2)} E_{\lambda'}$ where*

$$\begin{aligned} G_0 &= ax^2 + yz \\ G_1 &= az^2 + xy \\ G_2 &= ay^2 + xz \end{aligned}$$

is a morphism with image $E_{\lambda'}$ where $\lambda' = s - \frac{4}{s^2}$, and a is a solution to

$$s^2a^2 + 2a + s = 0. \tag{7.1}$$

The subgroup $H = \{\mathcal{O}, (s : 1 : 1)\}$ is mapped to the 2-torsion point $(-1 : a : a)$ on $E_{\lambda'}$.

Conversely, let $(-1 : a : a)$ be a 2-torsion point on a curve $E_{\lambda'}$. Let s be a solution to Equation (7.1), and E_λ the Hessian curve containing s. Then

$(G_0 : G_1 : G_2)$ *induces a morphism*

$$\phi\colon E_\lambda \to E_{\lambda'}$$

such that the subgroup $H = \{\mathcal{O}, (s : 1 : 1)\}$ *is mapped to the* 2*-torsion point* $(-1 : a : a)$.

Proof. Since ϕ is given by polynomials, it is clear that it is a morphism. We check using [Macaulay2] that $G_0^3 + G_1^3 + G_2^3 + \lambda' G_0 G_1 G_2 = 0$, so $\mathrm{im}(\phi) \subseteq E_{\lambda'}$. Recall that elliptic curves are irreducible by definition, and that a morphism is a continuous map (with respect to the Zariski topology). By Proposition 2.3.9 the image of ϕ is irreducible, and by Remark 2.2.6 it is also closed. This means that $\mathrm{im}\,\phi = E_{\lambda'}$. We check using [Macaulay2] that $\phi(\mathcal{O}) = \phi(s : 1 : 1) = (-1 : a : a)$.

On the other hand, fix a point $(-1 : a : a)$ on a curve $E_{\lambda'}$. Then λ' is a given by

$$-1 + 2a^3 - \lambda' a^2 = 0$$
$$\lambda' = \frac{1 - 2a^3}{a^2}.$$

Furthermore, let s be a solution to Equation (7.1). The point $(s : 1 : 1)$ is a 2-torsion point on the curve E_λ where λ is a solution to $s^3 + 2 + \lambda s = 0$. By the first part of the proof, $(G_0 : G_1 : G_2)$ induces a map $\phi\colon E_\lambda \to E_{\lambda''}$ where $\lambda'' = s - \frac{4}{s^2}$. It suffices to show that $\lambda'' = \lambda'$, which is equivalent to showing that

$$-s^2 + 2a^3 s^2 - a^2 s^3 + 4a^2 = (2a - s)(a^2 s^2 + 2a + s) = 0.$$

This follows by the assumption on s. The [Macaulay2] code can be found in Appendix B.8.

■

Remark 7.1.2. We have that

$$\sigma(G_0) = G_2,\ \sigma(G_1) = G_0,\ \sigma(G_2) = G_1,$$

and

$$\tau(G_0) = G_0,\ \tau(G_1) = \epsilon G_1,\ \tau(G_2) = \epsilon^2 G_2.$$

This shows that $\mathrm{Span}(G_0, G_1, G_2)$ can be viewed as a representation of H_3, namely the 3-dimensional representation corresponding to the character χ_{11} found in Section 5.4.

Corollary 7.1.3. *Let* $\phi\colon E \to E'$ *be a morphism between elliptic curves mapping a subgroup* $\{\mathcal{O}, p\}$ *to a point* $q \in E'$. *Then the difference between the points in each fiber of* ϕ *is* p.

Proof. Let ψ be the isogeny which is the composition

$$E \xrightarrow{\phi} E' \xrightarrow{\tau_{-q}} E', \qquad \psi\colon E \to E'$$

where $\phi(p) = \phi(\mathcal{O}) = q$. Let $\{p_1, p_2\} = \phi^{-1}(q')$ for any $q' \in E_{\lambda'}$. Since ψ is a homomorphism, we get

$$\begin{aligned}\psi(p_1 - p_2) &= (\tau_{-q} \circ \phi)(p_1 - p_2) \\ &= (\tau_{-q} \circ \phi)(p_1) - (\tau_{-q} \circ \phi)(p_2) \\ &= (\phi(p_1) - q) - (\phi(p_2) - q) \\ &= \phi(p_1) - \phi(p_2) \\ &= \mathcal{O}.\end{aligned}$$

On the other hand,

$$\begin{aligned}\psi(p_1 - p_2) &= (\tau_{-q} \circ \phi)(p_1 - p_2) \\ &= \phi(p_1 - p_2) - q.\end{aligned}$$

This means that $\phi(p_1 - p_2) = q$. Since the two points that are mapped to q is p and $\mathcal{O}$, we must have either $p_1 - p_2 = \mathcal{O}$ or $p_1 - p_2 = p$. By Proposition 3.3.4 and the fact that a translation is an isomorphism (see Example 3.2.5) each fiber must contain two points. Then $p_1 - p_2 \neq \mathcal{O}$, so we must have $p_1 - p_2 = p$. ■

We can also describe the two points that are mapped to $\mathcal{O}$.

Corollary 7.1.4. *Let $\phi\colon E \to E'$ be a morphism between elliptic curves mapping a subgroup $\{\mathcal{O}, p\} \subset E$ to a primitive 2-torsion point $q \in E'$. The points $\{p_\mathcal{O}, p_\mathcal{O} + p\} = \phi^{-1}(\mathcal{O})$ are two points such that $2p_\mathcal{O}$ is either p or $\mathcal{O}$.*

Proof. Notice that $2(p_\mathcal{O} + p) = 2p_\mathcal{O} + 2p = 2p_\mathcal{O}$. We consider the composition

$$E \xrightarrow{\phi} E' \xrightarrow{\tau_{-q}} E'$$
$$E \xrightarrow{\qquad\psi\qquad} E'$$

where $q = \phi(\mathcal{O})$. Firstly we have

$$\begin{aligned}\psi(2p_\mathcal{O}) &= \psi(p_\mathcal{O} + p_\mathcal{O}) \\ &= (\tau_{-q} \circ \phi)(p_\mathcal{O}) + (\tau_{-q} \circ \phi)(p_\mathcal{O}) \\ &= (\phi(p_\mathcal{O}) - q) + (\phi(p_\mathcal{O}) - q) \\ &= -2q \\ &= \mathcal{O}.\end{aligned}$$

Furthermore, we have

$$\begin{aligned}\psi(2p_\mathcal{O}) &= (\tau_{-q} \circ \phi)(2p_\mathcal{O}) \\ &= \phi(2p_\mathcal{O}) - q.\end{aligned}$$

This means that $\phi(2p_\mathcal{O}) = q$. We know that the two points that are sent to q are exactly $\mathcal{O}$ and p. Then $2p_\mathcal{O}$ must be equal to either $\mathcal{O}$ or p. ■

Corollary 7.1.5. *In the setting of Proposition 7.1.1, the points $\{p_\mathcal{O}, p_\mathcal{O} + p\} = \phi^{-1}(\mathcal{O})$ are two primitive 4-torsion points such that $2p_\mathcal{O} = p$.*

Proof. Assume for contradiction that $p_{\mathcal{O}}$ is a primitive 2-torsion point. Then $p_{\mathcal{O}}$ is on the form $p_{\mathcal{O}} = (t : 1 : 1)$. Since $2(p_{\mathcal{O}} + p) = 2p_{\mathcal{O}} + 2p = \mathcal{O} + \mathcal{O} = \mathcal{O}$, then $p_{\mathcal{O}} + p$ is also a primitive 2-torsion point. We see that

$$\phi(p_{\mathcal{O}}) = \phi(t : 1 : 1) = (at^2 + 1 : a + t : a + t),$$

which cannot be equal to $(0 : 1 : -1)$, a contradiction. Hence $\phi^{-1}(\mathcal{O}) = \{p_{\mathcal{O}}, p_{\mathcal{O}} + p\}$ are two primitive 4-torsion points such that $2p_{\mathcal{O}} = p$. ■

In the setting of Proposition 7.1.1, fix a 2-torsion point $p = (s : 1 : 1) \in E_\lambda$. The 2-torsion points on $E_{\lambda'}$ are on the form $(-1 : a : a)$ where a is a solution to

$$\begin{aligned}(-1)^3 + a^3 + a^3 + \lambda'(-1)a^2 &= 0\\ -1 + 2a^3 - a^2\left(s - \frac{4}{s^2}\right) &= 0\\ -s^2 + 2a^3s^2 - a^2s^3 + 4a^2 &= 0\\ (2a - s)(a^2s^2 + 2a + s) &= 0.\end{aligned}$$

We see that $q = (-1 : \frac{s}{2} : \frac{s}{2}) = (-2 : s : s)$ is a 2-torsion point on $E_{\lambda'}$. We cannot use Proposition 7.1.1 to construct a morphism $\mu\colon E_\lambda \to E_{\lambda'}$ where $\mu(\mathcal{O}) = q$. Anyway, such morphism μ exists, and we can find it by using a 2-isogeny ψ from Proposition 6.3.1 together with the translation τ_{+q}.

Moreover, there are 6 cyclic subgroups of E_λ of order 4. Two of them contains the 2-torsion points p, and they are on the form

$$\{\mathcal{O}, p_{\mathcal{O}}, p, p_{\mathcal{O}} + p\} \quad \text{and} \quad \{\mathcal{O}, p'_{\mathcal{O}}, p, p'_{\mathcal{O}} + p\}.$$

For one solution a of Equation (7.1), the fiber $\phi^{-1}(\mathcal{O})$ is equal to, say, $\{p_{\mathcal{O}}, p_{\mathcal{O}} + p\}$. For the other solution a' of Equation (7.1) the fiber $\phi^{-1}(\mathcal{O})$ is equal to $\{p'_{\mathcal{O}}, p'_{\mathcal{O}} + p\}$. Then for the morphism μ that maps $(s : 1 : 1)$ to $(-2 : s : s)$, we must have that $\mu^{-1}(\mathcal{O})$ consists of two primitive 2-torsion points.

Now let E_0 be an elliptic curve, not necessarily on Hessian form. We will see in the next section that when we use morphisms ϕ of degree 2 to compute an isogeny $\psi\colon E_0 \to E_e$ of degree 2^e for some e, then we will only need the morphisms where $\phi^{-1}(\mathcal{O})$ are primitive 4-torsion points. If we let the elliptic curves be on Hessian form, then the morphisms from Proposition 7.1.1 are sufficient.

7.2 Isogeny computations using morphisms

We will present an algorithm to construct an isogeny of degree 2^e, for some positive integer e, using morphisms of degree 2 instead of isogenies of degree 2, similar to the algorithm in Section 4.4. For simplicity we describe the idea for the case when $e = 4$. We begin with an elliptic curve E_0 (not necessarily on Hessian form), and a cyclic subgroup $\langle p\rangle \subset E_0[2^4]$ generated by a primitive 2^4-torsion point p. We want to construct the unique isogeny $\psi\colon E_0 \to E_4$ having $\langle p\rangle$ as kernel. In Section 4.4 such isogeny was constructed as a composition

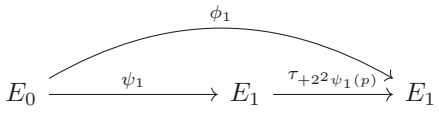
$$\psi = \psi_4 \circ \psi_3 \circ \psi_2 \circ \psi_1$$

of isogenies ψ_i. We will construct the same isogeny as a composition

$$\psi = \tau \circ \phi_4 \circ \phi_3 \circ \phi_2 \circ \phi_1$$

of morphisms ϕ_i and a translation τ, where $\phi_i = \tau_i \circ \psi_i$ and τ_i are translations by 2-torsion points.

Firstly, we find the morphism $\phi_1 \colon E_0 \to E_1$ of degree 2 that maps the 4-torsion point $2^2 p$ to $\mathcal{O}$. As illustrated in the diagram below, we will then get $\phi_1(2^3 p) = 2^2 \psi_1(p)$, which is a 2-torsion point on E_1. So ϕ_1 is the morphism mapping the 2-torsion point $2^3 p \in E_0$ to the 2-torsion point $2^2 \psi_1(p) \in E_1$.



$$\{\mathcal{O}, 2^3 p\} \longmapsto \mathcal{O} \longmapsto 2^2 \psi_1(p)$$

$$\{7p, 7p + 2^3 p\} \longmapsto 7\psi_1(p) \longmapsto 3\psi_1(p)$$

$$\{6p, 6p + 2^3 p\} \longmapsto 6\psi_1(p) \longmapsto 2\psi_1(p)$$

$$\{5p, 5p + 2^3 p\} \longmapsto 5\psi_1(p) \longmapsto \psi_1(p)$$

$$\{2^2 p, 2^2 p + 2^3 p\} \longmapsto 2^2 \psi_1(p) \longmapsto \mathcal{O}$$

$$\{3p, 3p + 2^3 p\} \longmapsto 3\psi_1(p) \longmapsto 7\psi_1(p)$$

$$\{2p, 2p + 2^3 p\} \longmapsto 2\psi_1(p) \longmapsto 6\psi_1(p)$$

$$\{p, p + 2^3 p\} \longmapsto \psi_1(p) \longmapsto 5\psi_1(p)$$

Then we find the unique morphism $\phi_2 \colon E_1 \to E_2$ of degree 2 that maps the 4-torsion point $\phi_1(2p) = 6\psi_1(p)$ to $\mathcal{O}$. As illustrated in the diagram below, we will then get $\phi_2(\phi_1(2^3 p)) = 2\psi_2(\psi_1(p))$, which is a 2-torsion point on E_2. So ϕ_2 is the morphism mapping the 2-torsion point $\phi_1(2^3 p) \in E_1$ to the 2-torsion point $2\psi_2(\psi_1(p)) \in E_2$.

$$E_1 \xrightarrow{\psi_2} E_2 \xrightarrow{\tau_{+2\psi_2(\psi_1(p))}} E_2 \quad (\phi_2 = \tau_{+2\psi_2(\psi_1(p))} \circ \psi_2)$$

$$2^2\psi_1(p) \longmapsto \mathcal{O} \longmapsto 2\psi_2(\psi_1(p))$$

$$3\psi_1(p) \longmapsto 3\psi_2(\psi_1(p)) \longmapsto \psi_2(\psi_1(p))$$

$$2\psi_1(p) \longmapsto 2\psi_2(\psi_1(p)) \longmapsto \mathcal{O}$$

$$\psi_1(p) \longmapsto \psi_2(\psi_1(p)) \longmapsto 3\psi_2(\psi_1(p))$$

$$\mathcal{O} \longmapsto \mathcal{O} \longmapsto 2\psi_2(\psi_1(p))$$

$$7\psi_1(p) \longmapsto 3\psi_2(\psi_1(p)) \longmapsto \psi_2(\psi_1(p))$$

$$6\psi_1(p) \longmapsto 2\psi_2(\psi_1(p)) \longmapsto \mathcal{O}$$

$$5\psi_1(p) \longmapsto \psi_2(\psi_1(p)) \longmapsto 3\psi_2(\psi_1(p))$$

Next we find the morphism $\phi_3 \colon E_2 \to E_3$ of degree 2 that maps the 4-torsion point $\phi_2(\phi_1(p)) = 3\psi_2(\psi_1(p))$ to $\mathcal{O}$. As illustrated in the diagram below, we will then get $\phi_3(\phi_2(\phi_1(2^3p))) = \psi_3(\psi_2(\psi_1(p)))$, which is a 2-torsion point on E_3. So ϕ_3 is the morphism mapping the 2-torsion point $\phi_2(\phi_1(2^3p)) \in E_2$ to the 2-torsion point $\psi_3(\psi_2(\psi_1(p))) \in E_3$.

$$E_2 \xrightarrow{\psi_3} E_3 \xrightarrow{\tau_{+\psi_3(\psi_2(\psi_1(p)))}} E_3 \quad (\phi_3 = \tau_{+\psi_3(\psi_2(\psi_1(p)))} \circ \psi_3)$$

$$2\psi_2(\psi_1(p)) \longmapsto \mathcal{O} \longmapsto \psi_3(\psi_2(\psi_1(p)))$$

$$\psi_2(\psi_1(p)) \longmapsto \psi_3(\psi_2(\psi_1(p))) \longmapsto \mathcal{O}$$

$$\mathcal{O} \longmapsto \mathcal{O} \longmapsto \psi_3(\psi_2(\psi_1(p)))$$

$$3\psi_2(\psi_1(p)) \longmapsto \psi_3(\psi_2(\psi_1(p))) \longmapsto \mathcal{O}$$

Then we choose any morphism $\phi_4 \colon E_3 \to E_4$ of degree 2 that maps the subgroup $\{\mathcal{O}, \psi_3(\psi_2(\psi_1(p)))\}$ to a 2-torsion point $q_4 \in E_4$, and finally we translate the point q_4 to the origin using the translation $\tau_{-q4} \colon E_4 \to E_4$.

$$E_3 \xrightarrow{\psi_4} E_4 \xrightarrow{\tau_{+q4}} E_4 \xrightarrow{\tau_{-q4}} E_4 \qquad (\phi_4 : E_3 \to E_4)$$

$$\psi_3(\psi_2(\psi_1(p))) \longmapsto \mathcal{O} \longmapsto q_4 \longmapsto \mathcal{O}$$

$$\mathcal{O} \longmapsto \mathcal{O} \longmapsto q_4 \longmapsto \mathcal{O}$$

Then we get the (unique) isogeny $\psi \colon E_0 \to E_4$ having $\langle p \rangle$ as kernel, where

$$\psi = \tau_{-q_4} \circ \phi_4 \circ \phi_3 \circ \phi_2 \circ \phi_1.$$

Remark 7.2.1. We mention that even though the morphism ϕ_i in each step i must necessarily be a unique isogeny ψ_i followed by a specific translation, it is not required that we must compute ϕ_i *as* this composition. For instance, between Hessian curves the formulas for 2-isogenies ψ in Proposition 6.3.1 are given by polynomials of degree 3, and translations τ are given by polynomials of degree 2. Then compositions $\tau \circ \psi$ are given by polynomials of degree $2 \cdot 3$. The point is that there might be simpler representatives of the morphisms ϕ, like the morphisms of degree 2 between Hessian curves from Proposition 7.1.1 that are given by polynomials of degree 2 (instead of 6).

In general, the algorithm goes as follows. Let E_0 be an elliptic curve, and $\langle p \rangle$ be a cyclic subgroup of $E_0[2^e]$. We construct the isogeny ψ as a composition of morphisms ϕ_i of degree 2

$$E_0 \xrightarrow{\phi_1} \cdots \xrightarrow{\phi_i} E_i \xrightarrow{\phi_{i+1}} E_{i+1} \xrightarrow{\phi_{i+1}} \cdots \xrightarrow{\phi_{e-1}} E_{e-1} \xrightarrow{\phi_e} E_e \xrightarrow{\tau_{-q_e}} E_e \qquad (\psi : E_0 \to E_e)$$

where for each step $i = 0, \ldots, e-2$ we find $\phi_{i+1} \colon E_i \to E_{i+1}$ as the morphism of degree 2 mapping the 4-torsion point $\phi_i(\cdots(\phi_1(2^{e-(i+2)}p))) \in E_i$ to $\mathcal{O} \in E_{i+1}$. Then the 2-torsion point

$$\phi_i(\cdots(\phi_1(2^{e-1}))) = 2^{e-(i+1)}\psi_i(\cdots(\psi_1(p))) \in E_i$$

will be mapped to

$$\phi_{i+1}(\cdots(\phi_1(2^{e-1}p))) = 2^{e-(i+2)}\psi_{i+1}(\cdots(\psi_1(p))) \in E_{i+1}.$$

When $i = e-1$ we can choose any morphism $\phi_e \colon E_{e-1} \to E_e$ of degree 2 mapping the subgroup

$$\{\mathcal{O}, \phi_{e-1}(\cdots(\phi_1(2^{e-1}p)))\} = \{\mathcal{O}, 2^{e-e}\psi_{e-1}(\cdots(\psi_1(p)))\} \subset E_{e-1}$$

to a 2-torsion point $q_e \in E_e$. Then $\psi\colon E_0 \to E_e$ is the unique isogeny having $\langle p \rangle$ as kernel, where

$$\psi = \tau_{-q_e} \circ \phi_e \circ \phi_{e-1} \circ \cdots \circ \phi_2 \circ \phi_1.$$

In particular,

$$\psi = \psi_e \circ \cdots \circ \psi_i \circ \cdots \circ \psi_1,$$

where ψ_i are the 2-isogenies from the similar algorithm described in Section 4.4 (from [JF11]).

Remark 7.2.2. If the curves E_i are on Hessian form, then the morphisms ϕ_i can be found in Proposition 7.1.1. In particular, for this algorithm we need morphisms of degree 2 that maps 4-torsion points to $\mathcal{O}$, and by Corollary 7.1.5 these are exactly the morphisms given in Proposition 7.1.1.

7.3 Morphisms of degree 3

We recall that the group $E_\lambda[3]$ of 3-torsion points is

$$\begin{aligned} B(\mathcal{H}) &= Z(xyz) \cap Z(x^3 + y^3 + z^3) \\ &= \{(0:1:-1),\ (0:1:-\epsilon),\ (0:1:-\epsilon^2), \\ &\quad (1:-1:0),\ (1:-\epsilon:0),\ (1:-\epsilon^2:0), \\ &\quad (-1:0:1),\ (-\epsilon:0:1),\ (-\epsilon^2:0:1)\}, \end{aligned}$$

and see that this is actually equal to

$$\begin{aligned} U = \{&\mathcal{O},\ \tau(\mathcal{O}),\ \tau^2(\mathcal{O}), \\ &\sigma(\mathcal{O}),\ \sigma\tau(\mathcal{O}),\ \sigma\tau^2(\mathcal{O}), \\ &\sigma^2(\mathcal{O}),\ \sigma^2\tau(\mathcal{O}),\ \sigma^2\tau^2(\mathcal{O})\}. \end{aligned}$$

We also recall that a Hessian curve E_λ is σ- and τ-invariant. We exploit this to construct morphisms on Hessian curves that maps a given subgroup of 3-torsion points to a primitive 3-torsion point (instead of $\mathcal{O}$), using the 3-isogenies from Proposition 6.1.1 and Proposition 6.1.2.

Proposition 7.3.1. *Let $\phi\colon E_\lambda \to E_{\lambda'}$ be an isogeny $\phi = (G_0 : G_1 : G_2)$ from Proposition 6.1.1 or Proposition 6.1.2, and H the subgroup of 3-torsion points mapped to $\mathcal{O}$ by ϕ. Furthermore, let $\theta \in \{\tau, \tau^2, \sigma, \sigma^2, \sigma\tau, \sigma\tau^2, \sigma^2\tau, \sigma^2\tau^2\}$. Then*

$$\phi_\theta\colon E_\lambda \to E_{\lambda'}$$

given by $\phi_\theta = (\theta G_0 : \theta G_1 : \theta G_2)$ is a morphism mapping the subgroup H to the primitive 3-torsion point $\theta(\mathcal{O}) \in E_{\lambda'}$.

By the notation we mean $\sigma G_i = G_{i+1}$ and $\tau G_i = \epsilon^i G_i$ for $i \mod 3$.

Proof. This is an immediate consequence of the fact that the polynomial defining a Hessian curve is invariant under σ and τ. ■

Example 7.3.2. Let $\phi\colon E_\lambda \to E_{\lambda'}$ be the isogeny given by

$$\begin{aligned}\phi &= (G_0 : G_1 : G_2)\\ &= (kxyz : x^3 + \epsilon^2 y^3 + \epsilon z^3 : x^3 + \epsilon y^3 + \epsilon^2 z^3)\end{aligned}$$

from Proposition 6.1.1 with kernel $H = \{\mathcal{O}, (0:1:-\epsilon), (0:1:-\epsilon^2)\}$, and let $\theta = \sigma^2\tau^2$. Then

$$\begin{aligned}\phi_{\sigma^2\tau^2} &= \sigma^2\tau^2(G_0 : G_1 : G_2)\\ &= \sigma^2\tau(G_0 : \epsilon G_1 : \epsilon^2 G_2)\\ &= \sigma^2(G_0 : \epsilon^2 G_1 : \epsilon G_2)\\ &= \sigma(\epsilon^2 G_1 : \epsilon G_2 : G_0)\\ &= (\epsilon G_2 : G_0 : \epsilon^2 G_1)\\ &= ((\epsilon x^3 + \epsilon^2 y^3 + z^3) : kxyz : \epsilon^2 x^3 + \epsilon y^3 + z^3)).\end{aligned}$$

We see that

$$\begin{aligned}\phi_{\sigma^2\tau^2}(\mathcal{O}) &= (\epsilon^2 - 1 : 0 : \epsilon - 1)\\ &= (-\epsilon^2 : 0 : 1)\\ &= \sigma^2\tau^2(\mathcal{O}).\end{aligned}$$

7.4 Morphisms of degree n

Let E_λ be a Hessian curve, and $H \subset E_\lambda$ a cyclic subgroup of order n, where $n \neq 0 \mod 3$. We presume that it is possible to find morphism $\phi\colon E_\lambda \to E_{\lambda'}$ where λ' is as given in Theorem 6.2.3, such that H is mapped to a primitive n-torsion point and $\phi = (G_0 : G_1 : G_2)$ can be viewed as a 3-dimensional representation of H_3. In particular, the representation with character χ_{10} when $n = 1 \mod 3$ and the representation with character χ_{11} when $n = 2 \mod 3$, similar to the multiplication-by-n-isogeny in Claim 5.5.2.

In Proposition 7.1.1 we found such morphism for $n = 2$. We have not found a general formula for the case when $n = 4$, but we give an example that supports the presumption for this case.

Example 7.4.1. Let $\lambda = 1$, and let $H = \{(s_i : t_i : 1)\}_{i=1}^4 \subset E_\lambda$ be a subgroup of order 4 generated by a primitive 4-torsion point $p_1 = (s_1 : t_1 : 1)$ where

$$s_1 = \frac{1 - \sqrt{5 + 4\sqrt{2}}}{2},\ t_1 = \frac{s_1}{1 - s_1}.$$

In particular, we have

$$\begin{aligned}H &= \{(s_1 : t_1 : 1),\ (s_2 : t_2 : 1),\ (s_3 : t_3 : 1),\ (s_4 : t_4 : 1)\}\\ &= \{(s_1 : t_1 : 1),\ (-1 : 1 : 1),\ (s_1 : t_1 : 1) + (-1 : 1 : 1),\ (0 : 1 : -1)\}.\end{aligned}$$

Here $(s_4 : t_4 : 1) = (0 : 1 : -1) = \mathcal{O}$. We will construct a morphism $\phi\colon E_\lambda \to E_{\lambda'}$ where $\lambda' = 7\sqrt{2} - 13$ is as given in Proposition 6.3.3, and such that $\phi = (G_0 : G_1 : G_2)$ can be viewed as a 3-dimensional representation of

the Heisenberg group H_3, more precisely the representation with character χ_{10}. Therefore we let

$$\begin{aligned} G_0(x:y:z) &= ax^4 + bx^2yz + cxy^3 + dxz^3 + ey^2z^2 \\ G_1(x:y:z) &= ay^4 + bxy^2z + cyz^3 + dx^3y + ex^2z^2 \\ G_2(x:y:z) &= az^4 + bxyz^2 + cx^3z + dy^3z + ex^2y^2, \end{aligned}$$

because then we have

$$\begin{aligned} \tau(G_0) = G_0,\ \tau(G_1) = \epsilon G_1,\ \tau^2(G_2) = \epsilon^2 G_2, \\ \sigma(G_0) = G_1,\ \sigma(G_1) = \ G_2,\ \sigma(G_2) = G_0. \end{aligned}$$

We must determine the coefficients so that $\operatorname{im}\phi = E_{\lambda'}$. Since a morphism between elliptic curves must be an isogeny together with a translation, we also require that H is mapped to the same point. We evaluate ϕ in each point in H,

$$\phi(s_i : t_i : 1) = (q_i^x : q_i^y : q_i^z),$$

and denote $\phi(\mathcal{O}) = (q_{\mathcal{O}}^x : q_{\mathcal{O}}^y : q_{\mathcal{O}}^z)$. We require that the points $(q_i^x : q_i^y : q_i^z)$ for $i = 1, 2, 3$ are equal to $\phi(\mathcal{O})$, and we get six equations

$$q_{\mathcal{O}}^x q_i^z - q_i^x q_{\mathcal{O}}^z = 0 \text{ and } q_{\mathcal{O}}^y q_i^z - q_i^y q_{\mathcal{O}}^z = 0.$$

These equations give relations between the coefficients a, b, c, d, e. We use [Macaulay2] to find solutions to this system, and get for instance the solution

$$d = e = 1,\ a = \frac{c-1}{2},\ b = \frac{c-3}{2},\ c^2 - 2c + 4\sqrt{2} + 1 = 0.$$

With this solution we get that ϕ is a morphism $\phi\colon E_\lambda \to E_{\lambda'}$ where $\lambda' = 7\sqrt{2}-13$, and the subgroup H of 4-torsion points is mapped to the primitive 4-torsion point

$$q = (2 : -c-1 : c-3) \in E_{\lambda'}.$$

The [Macaulay2] code can be found in Appendix B.9.

Appendices

APPENDIX A

The Heisenberg group

A.1 Conjugacy classes

We have the following conjugacy classes of H_3.

$$
\begin{aligned}
C_1 &= \mathrm{id} \\
C_2 &= \epsilon\mathrm{id} = \tau\sigma\tau^2\sigma^2 \\
C_3 &= \epsilon^2\mathrm{id} = \tau^2\sigma\tau\sigma^2 \\
C_4 &= \{\sigma, \epsilon\sigma, \epsilon^2\sigma\} = \{\sigma, \tau\sigma\tau^{-1}, \tau^2\sigma\tau^{-2}\} \\
C_5 &= \{\tau, \epsilon\tau, \epsilon^2\tau\} = \{\tau, \sigma^2\tau\sigma^{-2}, \sigma\tau\sigma^{-1}\} \\
C_6 &= \{\sigma\tau, \epsilon\sigma\tau, \epsilon^2\sigma\tau\} = \{\sigma\tau, \sigma^2(\sigma\tau)\sigma^{-2}, \sigma(\sigma\tau)\sigma^{-1}\} \\
C_7 &= \{\sigma^2\tau, \epsilon\sigma^2\tau, \epsilon^2\sigma^2\tau\} = \{\sigma^2\tau, \sigma^2(\sigma^2\tau)\sigma^{-2}, \sigma(\sigma^2\tau)\sigma^{-1}\} \\
C_8 &= \{\tau^2, \epsilon\tau^2, \epsilon^2\tau^2\} = \{\tau^2, \sigma(\tau^2)\sigma^{-1}, \sigma^2(\tau^2)\sigma^{-2}\} \\
C_9 &= \{\sigma\tau^2, \epsilon\sigma\tau^2, \epsilon^2\sigma\tau^2\} = \{\sigma\tau^2, \sigma(\sigma\tau^2)\sigma^{-1}, \sigma^2(\sigma\tau^2)\sigma^{-2}\} \\
C_{10} &= \{\sigma^2\tau^2, \epsilon\sigma^2\tau^2, \epsilon^2\sigma^2\tau^2\} = \{\sigma^2\tau^2, \sigma(\sigma^2\tau^2)\sigma^{-1}, \sigma^2(\sigma^2\tau^2)\sigma^{-2}\} \\
C_{11} &= \{\sigma^2, \epsilon\sigma^2, \epsilon^2\sigma^2\} = \{\sigma^2, \tau^2\sigma^2\tau^{-2}, \tau\sigma^2\tau^{-1}\}
\end{aligned}
$$

A.2 The character table

Let χ_i denote the characters of the representations V_i found in Chapter 5. The character table of H_3 is given below.

	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	C_{11}
χ_1	1	1	1	1	1	1	1	1	1	1	1
χ_2	1	1	1	ϵ	1	ϵ	ϵ^2	1	ϵ	ϵ^2	ϵ^2
χ_3	1	1	1	ϵ^2	1	ϵ^2	ϵ	1	ϵ^2	ϵ	ϵ
χ_4	1	1	1	1	ϵ	ϵ	ϵ	ϵ^2	ϵ^2	ϵ^2	1
χ_5	1	1	1	ϵ	ϵ	ϵ^2	1	ϵ^2	1	ϵ	ϵ^2
χ_6	1	1	1	ϵ^2	ϵ	1	ϵ^2	ϵ^2	ϵ	1	ϵ
χ_7	1	1	1	1	ϵ^2	ϵ^2	ϵ^2	ϵ	ϵ	ϵ	1
χ_8	1	1	1	ϵ	ϵ^2	1	ϵ	ϵ	ϵ^2	1	ϵ^2
χ_9	1	1	1	ϵ^2	ϵ^2	ϵ	1	ϵ	1	ϵ^2	ϵ
χ_{10}	3	3ϵ	$3\epsilon^2$	0	0	0	0	0	0	0	0
χ_{11}	3	$3\epsilon^2$	3ϵ	0	0	0	0	0	0	0	0

APPENDIX B

Macaulay2 code

B.1 Find 3-isogenies

```
-- The coordinate ring
K = QQ[k1,k2,e,L,Lprime]/ideal(e^3-1,e^2+e+1)
R = K[x,y,z]/ideal(x^3+y^3+z^3+L*x*y*z)


f1 = x*y*z
f2 = x^3+e^2*y^3+e*z^3
f3 = x^3+e*y^3+e^2*z^3
f4 = x^2*y+y^2*z+z^2*x
f5 = x^2*y+e^2*y^2*z+e*z^2*x
f6 = x^2*y+e*y^2*z+e^2*z^2*x
f7 = x^2*z+y^2*x+z^2*y
f8 = x^2*z+e^2*y^2*x+e*z^2*y
f9 = x^2*z+e*y^2*x+e^2*z^2*y


G0 = k1*f1
G1 = k2*f2
G2 = f3

--G0 = k1*f1
--G1 = k2*f4
--G2 = f7

--G0 = k1*f1
--G1 = k2*f6
--G2 = f8

--G0 = k1*f1
--G1 = k2*f5
--G2 = f9

F = G0^3+G1^3+G2^3+Lprime*G0*G1*G2

-- Find solutions to F=0
mons = flatten entries monomials(F)
Ilist = for m in mons list (coefficient(m,F))
I = ideal(Ilist)
M = decompose I
```

B.2 Proof of Proposition 6.1.1

```
-- The coordinate ring.
K = QQ[k,e,L,Lprime]/ideal(e^3-1,e^2+e+1,k*Lprime-3*L,k^3-(-L^3-27))
R = K[x,y,z]/ideal(x^3+y^3+z^3+L*x*y*z)

f1 = x*y*z
f2 = x^3+e^2*y^3+e*z^3
f3 = x^3+e*y^3+e^2*z^3

-- Create the map phi=(G0:G1:G2)
G0 = k*f1
G1 = f2
G2 = f3

-- Check that F = 0
F = G0^3+G1^3+G2^3+Lprime*G0*G1*G2

-- Check that the kernel is the 3-torsion points
-- (0:1:-1), (0:1:-e), (0:1:-e^2)
decompose ideal(G0,G1+G2)

-- Check that the map is defined everywhere
decompose ideal(G0,G1,G2)

-- We also demonstrate that ker(phi*) defines the right curve
S = K[X,Y,Z]
phistar = map(R,S,{G0,G1,G2})
trim ker phistar
```

B.3 Proof of Proposition 6.1.2

Part 1

```
-- The coordinate ring
K = QQ[k,L,Lprime]/ideal(k*Lprime-(L-6),k^3-(L^2-3*L+9))
R = K[x,y,z]/ideal(x^3+y^3+z^3+L*x*y*z)

f1 = x*y*z
f4 = x^2*y+y^2*z+z^2*x
f7 = x^2*z+y^2*x+z^2*y

-- Create the map phi=(G0:G1:G2)
G0 = k*f1
G1 = f4
G2 = f7

-- Check that F = 0, which means that F is in ker(phi*)
F = G0^3+G1^3+G2^3+Lprime*G0*G1*G2

-- Check that the kernel is the 3-torsion points
-- (0:1:-1), (1:0:-1), (1:-1:0)
decompose ideal(G0,G1+G2)

-- Check that the map is defined everywhere
decompose ideal(G0,G1,G2)

-- We also demonstrate that ker(phi*) defines the right curve
S = K[X,Y,Z]
```

```
phistar = map(R,S,{G0,G1,G2})
trim ker phistar
```

Part 2

```
-- Here e is a third root of unity
K = QQ[k,e,L,Lprime]/ideal(e^3-1,e^2+e+1,k*Lprime-(e*L-6*e^2),
                                          k^3-(e*L^2-3*e^2*L+9))
R = K[x,y,z]/ideal(x^3+y^3+z^3+L*x*y*z)

f1 = x*y*z
f6 = x^2*y+e*y^2*z+e^2*z^2*x
f8 = x^2*z+e^2*y^2*x+e*z^2*y

-- Create the map phi=(G0:G1:G2)
G0 = k*f1
G1 = f6
G2 = f8

-- Check that F = 0, which means that F is in ker(phi*)
F = G0^3+G1^3+G2^3+Lprime*G0*G1*G2

-- Check that the kernel is the 3-torsion points
-- (0:1:-1), (1:0:-e), (1:-e:0)
decompose ideal(G0,G1+G2)

-- Check that the map is defined everywhere
decompose ideal(G0,G1,G2)

-- We also demonstrate that ker(phi*) defines the right curve
S = K[X,Y,Z]
phistar = map(R,S,{G0,G1,G2})
trim ker phistar
```

Part 3

```
-- Here e is a third root of unity
K = QQ[k,e,L,Lprime]/ideal(e^3-1,e^2+e+1,k*Lprime-(e^2*L-6*e),
                                          k^3-(e^2*L^2-3*e*L+9))
R = K[x,y,z]/ideal(x^3+y^3+z^3+L*x*y*z)

f1 = x*y*z
f5 = x^2*y+e^2*y^2*z+e*z^2*x
f9 = x^2*z+e*y^2*x+e^2*z^2*y

-- Create the map phi=(G0:G1:G2)
G0 = k*f1
G1 = f5
G2 = f9

-- Check that F = 0, which means that F is in ker(phi*)
F = G0^3+G1^3+G2^3+Lprime*G0*G1*G2

-- Check that the kernel is the 3-torsion points
-- (0:1:-1), (1:0:-e^2), (1:-e^2:0)
decompose ideal(G0,G1+G2)

-- Check that the map is defined everywhere
```

```
decompose ideal(G0,G1,G2)

-- We also demonstrate that ker(phi*) defines the right curve
S = K[X,Y,Z]
phistar = map(R,S,{G0,G1,G2})
trim ker phistar
```

B.4 Example 6.2.8

```
-- The coordinate ring
K = toField(QQ[e,f,g,h]/ideal(e^3-1,e^2+e+1))
R = K[x,y,z]/ideal(x^3+y^3+z^3+(15*e/4)*x*y*z)

-- The 2-torsion point (s:1:1)
s = -e^2/2

-- Create the map phi=(H0:H1:H2)
H0 = x*(s^2*y*z-x^2)
H1 = y*(x*y-z^2*s)
H2 = z*(x*z-y^2*s)

-- Find the matrix where the columns are generators of mu^T
M = gens ker transpose presentation image matrix {{H0,H1,H2}}

-- Extract the entries of the matrix
u0 = 1*(M^{0}_{0}_0_0)
u1 = 1*(M^{1}_{0}_0_0)
u2 = 1*(M^{2}_{0}_0_0)

v0 = 1*(M^{0}_{1}_0_0)
v1 = 1*(M^{1}_{1}_0_0)
v2 = 1*(M^{2}_{1}_0_0)

w0 = 1*(M^{0}_{2}_0_0)
w1 = 1*(M^{1}_{2}_0_0)
w2 = 1*(M^{2}_{2}_0_0)

G0 = f*u0+g*v0+h*w0
G1 = f*u1+g*v1+h*w1
G2 = f*u2+g*v2+h*w2

-- Check that F=0
Lprime = -((15*e/4) + 6*(1/(s)))/s
F = G0^3+G1^3+G2^3+Lprime*G0*G1*G2
```

B.5 Example 6.2.9

```
-- The coordinate ring
K = toField(QQ[e,a,b,i,f,g,h]/ideal(e^3-1,e^2+e+1,i^2+1,a^2-2,b^2-(5+4*a)))
R = K[x,y,z]/ideal(x^3+y^3+z^3+1*x*y*z)

-- The primitive 4-torsion (s1:t1:1)
s1 = (1/2)*(1-b)
t1 = s1/(1-s1)

doubleX = s1*1^3-s1*t1^3
doubleY = t1^3*1-s1^3*1
```

```
doubleZ = s1^3*t1-t1*1^3

-- The 2-torsion point (s2:t2:1)
s2 = doubleX/doubleZ
t2 = doubleY/doubleZ

tripleX = t1*1*doubleX^2-s1^2*doubleY*doubleZ
tripleY = s1*t1*doubleZ^2-1^2*doubleX*doubleY
tripleZ = s1*1*doubleY^2-t1^2*doubleX*doubleZ

-- The primitive 4-torsion point (s3:t3:1)
s3 = tripleX/tripleZ
t3 = tripleY/tripleZ

-- Create the map phi=(H0:H1:H2)
H0 = x*(s1^2*y*z-x^2*t1)*(s2^2*y*z-x^2*t2)*(s3^2*y*z-x^2*t3)
H1 = y*(x*y-z^2*s1*t1)*(x*y-z^2*s2*t2)*(x*y-z^2*s3*t3)
H2 = z*(t1^2*x*z-y^2*s1)*(t2^2*x*z-y^2*s2)*(t3^2*x*z-y^2*s3)

-- Find the matrix where the columns are generators of mu^T
M = gens ker transpose presentation image matrix {{H0,H1,H2}}

-- Extract the entries of the matrix
u0 = 1*(M^{0}_{0}_0_0)
u1 = 1*(M^{1}_{0}_0_0)
u2 = 1*(M^{2}_{0}_0_0)

v0 = 1*(M^{0}_{1}_0_0)
v1 = 1*(M^{1}_{1}_0_0)
v2 = 1*(M^{2}_{1}_0_0)

w0 = 1*(M^{0}_{2}_0_0)
w1 = 1*(M^{1}_{2}_0_0)
w2 = 1*(M^{2}_{2}_0_0)

G0 = f*u0+g*v0+h*w0
G1 = f*u1+g*v1+h*w1
G2 = f*u2+g*v2+h*w2

-- Check that F=0
Lprime = -((1-2*3)*(-1) + 6*(1/(s1*t1)+1/(s2*t2)+1/(s3*t3)))/(s1*s2*s3)
F = G0^3+G1^3+G2^3+Lprime*G0*G1*G2
```

B.6 Proof of Proposition 6.3.1

```
-- Given s, then lambda = -s^2-2/s
K = QQ[s,f,g,h]
R = K[x,y,z]/ideal(s*(x^3+y^3+z^3)+(-s^3-2)*x*y*z)

-- Create the map phi=(G0:G1:G2)

u0 = -x^3+s^2*x*y*z
u1 = x*y^2-s*y*z^2
u2 = x*z^2-s*y^2*z

sigma_u0 = sub(u0,{x=>y, y=>z,z=>x})
sigma_u1 = sub(u1,{x=>y, y=>z,z=>x})
sigma_u2 = sub(u2,{x=>y, y=>z,z=>x})

sigma2_u0 = sub(sigma_u0,{x=>y, y=>z,z=>x})
```

```
sigma2_u1 = sub(sigma_u1,{x=>y, y=>z,z=>x})
sigma2_u2 = sub(sigma_u2,{x=>y, y=>z,z=>x})

G0 = f*u0 + g*sigma2_u1 + h*sigma_u2
G1 = f*u1 + g*sigma2_u2 + h*sigma_u0
G2 = f*u2 + g*sigma2_u0 + h*sigma_u1

-- Check that F=0
F = s^2*(G0^3+G1^3+G2^3)+(s^3-4)*G0*G1*G2

-- Check that the subgroup is mapped to (0:1:-1)
decompose ideal(G0,G1+G2)

-- Check that phi has base point
decompose ideal(G0,G1,G2)


-- We also demonstrate that ker(phi*) = F
S = K[X,Y,Z]
phistar = map(R,S,{G0,G1,G2})
ker phistar

-- Remark 6.3.2
-- Check that (G0:G1:G2) are other representatives
-- of the map (F0:F1:F2)
F0 = -x^3+s^2*x*y*z
F1 = x*y^2-s*y*z^2
F2 = x*z^2-s*y^2*z

F0*G1-F1*G0
F1*G2-F2*G1
```

B.7 Proof of Proposition 6.3.3

```
-- The coordinate ring
K = toField(QQ[s1,t1,f,g,h,L]/ideal(s1^3*t1+s1^3*1-t1^3*1-1^3*t1,
                                    s1^3+t1^3+1^3+L*s1*t1*1))
R = K[x,y,z]/ideal(x^3+y^3+z^3+L*x*y*z)

-- The generator 4-torsion point is (s1:t1:1), and the other group elements
-- are (s2:t2:1), (s3:t3:1) and (0:1:-1)
s2 = -s1-s1/t1
t2 = 1

s3 = s1/t1
t3 = 1/t1

-- Find the coefficients
K1 = -s2
K2 = -s1*s3
K3 = 2/K1

-- Create the map phi=(G0:G1:G2)
u0 = x*(x^3*y+K1*x^2*z^2+K1*K2*y*z^3+K2*x*y^2*z)
u1 = y*(x^3*y+K1^2*K2*x^2*z^2+y*z^3+(K3-K2)*x*y^2*z)
u2 = z*(K1*K2*x^3*y+K1*x^2*z^2+y*z^3+K2*x*y^2*z)

sigma_u0 = sub(u0,{x=>y, y=>z,z=>x})
sigma_u1 = sub(u1,{x=>y, y=>z,z=>x})
sigma_u2 = sub(u2,{x=>y, y=>z,z=>x})
```

```
sigma2_u0 = sub(sigma_u0,{x=>y, y=>z,z=>x})
sigma2_u1 = sub(sigma_u1,{x=>y, y=>z,z=>x})
sigma2_u2 = sub(sigma_u2,{x=>y, y=>z,z=>x})

G0 = f*u0 + g*sigma2_u1 + h*sigma_u2
G1 = f*u1 + g*sigma2_u2 + h*sigma_u0
G2 = f*u2 + g*sigma2_u0 + h*sigma_u1

-- Check that the subgroup is sent to (0:1:-1)
sub(G0,{x=>0,y=>1,z=>-1})
sub(G1,{x=>0,y=>1,z=>-1})
sub(G2,{x=>0,y=>1,z=>-1})

sub(G0,{x=>s1,y=>t1,z=>1})
sub(G1,{x=>s1,y=>t1,z=>1})
sub(G2,{x=>s1,y=>t1,z=>1})

sub(G0,{x=>s2,y=>t2,z=>1})
sub(G1,{x=>s2,y=>t2,z=>1})
sub(G2,{x=>s2,y=>t2,z=>1})

sub(G0,{x=>s3,y=>t3,z=>1})
sub(G1,{x=>s3,y=>t3,z=>1})
sub(G2,{x=>s3,y=>t3,z=>1})

-- Check that F=0
Lprime = (-8*s1^3+4*t1^3-12*t1^2-12*t1+4)/(4*s1*t1^2+4*s1)
F = G0^3+G1^3+G2^3+Lprime*G0*G1*G2

-- Check that the map(s) (G0:G1:G2) are other representatives
-- of the map (F0:F1:F2)
F0 = x*(s1^2*y*z-x^2*t1)*(s2^2*y*z-x^2*t2)*(s3^2*y*z-x^2*t3)
F1 = y*(x*y-z^2*s1*t1)*(x*y-z^2*s2*t2)*(x*y-z^2*s3*t3)
F2 = z*(t1^2*x*z-y^2*s1)*(t2^2*x*z-y^2*s2)*(t3^2*x*z-y^2*s3)

F0*G1-G0*F1
F0*G2-F2*G0
```

B.8 Proof of Proposition 7.1.1

```
-- The coordinate ring
K = QQ[a,s]/ideal(a^2*s^2+s+2*a)
R = K[x,y,z]/ideal(s*(x^3+y^3+z^3)+(-s^3-2)*x*y*z)

-- Create the map phi=(G0:G1:G2)
G0 = a*x^2+y*z
G1 = a*z^2+x*y
G2 = a*y^2+x*z

-- Check where (0:1:-1) and (s:1:1) are mapped
q0x = sub(G0,{x=>0,y=>1,z=>-1})
q0y = sub(G1,{x=>0,y=>1,z=>-1})
q0z = sub(G2,{x=>0,y=>1,z=>-1})

q1x = sub(G0,{x=>s,y=>1,z=>1})
q1y = sub(G1,{x=>s,y=>1,z=>1})
q1z = sub(G2,{x=>s,y=>1,z=>1})

-- Check that (0:1:-1) and (s:1:1) are mapped to the same point
```

```
q0x*q1y-q1x*q0y

-- Check that F=0
F = s^2*(G0^3+G1^3+G2^3)+(s^3-4)*G0*G1*G2

-- We also demonstrate ker(phi*) defines the right curve
S = K[X,Y,Z]
phistar = map(R,S,{G0,G1,G2})
trim ker phistar
```

B.9 Example 7.4.1

```
-- The coordinate ring
K = toField(QQ[a..d,e,A,B]/ideal(e^3-1,e^2+e+1,A^2-2,B^2-(5+4*A)))
R = K[x,y,z]/(x^3+y^3+z^3+1*x*y*z)

-- The 4-torsion point
s = (1/2)*(1-B)
t = s/(1-s)

G0 = a*x^4+b*x^2*y*z+c*x*y^3+d*x*z^3+1*y^2*z^2
G1 = d*x^3*y+1*x^2*z^2+b*x*y^2*z+a*y^4+c*y*z^3
G2 = c*x^3*z+1*x^2*y^2+b*x*y*z^2+d*y^3*z+a*z^4

s1 = s
t1 = t

s2 = s*t^3+s^2*t*(1)+2*s*t^2+s^2*(1)+s
t2 = 1

s3 = -s*t^3-s^2*t*(1)-2*s*t^2-s^2*(1)-2*s
t3 = -t^3-s*t*(1)-2*t^2-s*(1)-2

q0x = sub(G0,{x=>0, y=>1, z=>-1})
q0y = sub(G1,{x=>0, y=>1, z=>-1})
q0z = sub(G2,{x=>0, y=>1, z=>-1})

q1x = sub(G0,{x=>s1, y=>t1, z=>1})
q1y = sub(G1,{x=>s1, y=>t1, z=>1})
q1z = sub(G2,{x=>s1, y=>t1, z=>1})

q2x = sub(G0,{x=>s2, y=>t2, z=>1})
q2y = sub(G1,{x=>s2, y=>t2, z=>1})
q2z = sub(G2,{x=>s2, y=>t2, z=>1})

q3x = sub(G0,{x=>s3, y=>t3, z=>1})
q3y = sub(G1,{x=>s3, y=>t3, z=>1})
q3z = sub(G2,{x=>s3, y=>t3, z=>1})

-- Require that the points in H are mapped to
-- the same point
F1 = q0x*q1z-q1x*q0z
F2 = q0y*q1z-q1y*q0z
F3 = q0x*q2z-q2x*q0z
F4 = q0y*q2z-q2y*q0z
F5 = q0x*q3z-q3x*q0z
F6 = q0y*q3z-q3y*q0z

-- We find one solution using equation F3 and F4, and
-- also require that (1:a-c:a-d) is a primitive
```

```
-- 4-torsion point
decompose ideal(F3,F4)

-- Now we verify the solution
restart
K = toField(QQ[c,A,B]/ideal(A^2-2,B^2-(5+4*A), c^2-2*c+4*A+1))
R = K[x,y,z]/(x^3+y^3+z^3+1*x*y*z)

a = (c-1)/2
b = (c-3)/2
d = 1

s = (1/2)*(1-B)
t = s/(1-s)

G0 = a*x^4+b*x^2*y*z+c*x*y^3+d*x*z^3+1*y^2*z^2
G1 = d*x^3*y+1*x^2*z^2+b*x*y^2*z+a*y^4+c*y*z^3
G2 = c*x^3*z+1*x^2*y^2+b*x*y*z^2+d*y^3*z+a*z^4

s1 = s
t1 = t

s2 = s*t^3+s^2*t*(1)+2*s*t^2+s^2*(1)+s
t2 = 1

s3 = -s*t^3-s^2*t*(1)-2*s*t^2-s^2*(1)-2*s
t3 = -t^3-s*t*(1)-2*t^2-s*(1)-2

q0x = sub(G0,{x=>0, y=>1, z=>-1})
q0y = sub(G1,{x=>0, y=>1, z=>-1})
q0z = sub(G2,{x=>0, y=>1, z=>-1})

q1x = sub(G0,{x=>s1, y=>t1, z=>1})
q1y = sub(G1,{x=>s1, y=>t1, z=>1})
q1z = sub(G2,{x=>s1, y=>t1, z=>1})

q2x = sub(G0,{x=>s2, y=>t2, z=>1})
q2y = sub(G1,{x=>s2, y=>t2, z=>1})
q2z = sub(G2,{x=>s2, y=>t2, z=>1})

q3x = sub(G0,{x=>s3, y=>t3, z=>1})
q3y = sub(G1,{x=>s3, y=>t3, z=>1})
q3z = sub(G2,{x=>s3, y=>t3, z=>1})

F1 = q0x*q1z-q1x*q0z
F2 = q0y*q1z-q1y*q0z
F3 = q0x*q2z-q2x*q0z
F4 = q0y*q2z-q2y*q0z
F5 = q0x*q3z-q3x*q0z
F6 = q0y*q3z-q3y*q0z

Lprime = (-8*s1^3+4*t1^3-12*t1^2-12*t1+4)/(4*s1*t1^2+4*s1)
F = G0^3+G1^3+G2^3+Lprime*G0*G1*G2
```

Bibliography

[AD09] Artebani, M. and Dolgachev, I. V. 'The Hesse pencil of plane cubic curves'. In: *L'Enseignement Mathématique* vol. 55, no. 3 (2009), pp. 235–273.

[Ber+15] Bernstein, D. J. et al. 'Twisted hessian curves'. In: *International Conference on Cryptology and Information Security in Latin America*. Springer. 2015, pp. 269–294.

[Bot+19] Bott, C. et al. 'RationalMaps, a package for Macaulay2'. In: *arXiv preprint arXiv:1908.04337* (2019).

[Bro+21] Broon, F. L. P. et al. 'Isogenies on twisted Hessian curves'. In: *Journal of mathematical cryptology* vol. 15, no. 1 (2021), pp. 345–358.

[Cos19] Costello, C. 'Supersingular isogeny key exchange for beginners'. In: *International Conference on Selected Areas in Cryptography*. Springer. 2019, pp. 21–50.

[DJP14] De Feo, L., Jao, D. and Plût, J. 'Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies'. In: *Journal of Mathematical Cryptology* vol. 8, no. 3 (2014), pp. 209–247.

[Fri02] Frium, H. R. 'The group law on elliptic curves on Hesse form'. In: *Finite Fields with Applications to Coding Theory, Cryptography and Related Areas*. Springer, 2002, pp. 123–151.

[Ful08] Fulton, W. 'Algebraic curves'. In: *An Introduction to Algebraic Geom* vol. 54 (2008).

[Har77] Hartshorne, R. *Algebraic geometry*. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977, pp. xvi+496.

[JF11] Jao, D. and Feo, L. D. 'Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies'. In: *International Workshop on Post-Quantum Cryptography*. Springer. 2011, pp. 19–34.

[KES20] Kristensen, E. W., Ellingsen, L. and Strand, M. 'Testing av kvantesikre kandidatalgoritmer på en mikrokontroller–Norges sikreste chat'. In: (2020).

[Macaulay2] Grayson, D. R. and Stillman, M. E. *Macaulay2, a software system for research in algebraic geometry*. Available at http://www.math.uiuc.edu/Macaulay2/.

[MOV93] Menezes, A. J., Okamoto, T. and Vanstone, S. A. 'Reducing elliptic curve logarithms to logarithms in a finite field'. In: *iEEE Transactions on information Theory* vol. 39, no. 5 (1993), pp. 1639–1646.

[MW12] Moody, D. and Wu, H. 'Families of elliptic curves with rational 3-torsion'. In: *Journal of Mathematical Cryptology* vol. 5, no. 3-4 (2012), pp. 225–246.

[Ser77] Serre, J.-P. *Linear representations of finite groups*. Vol. 42. Springer, 1977.

[Sil09] Silverman, J. H. *The arithmetic of elliptic curves*. Vol. 106. Springer, 2009.

[SR94] Shafarevich, I. R. and Reid, M. *Basic algebraic geometry*. Vol. 2. Springer, 1994.

[Tat66] Tate, J. 'Endomorphisms of abelian varieties over finite fields'. In: *Inventiones mathematicae* vol. 2, no. 2 (1966), pp. 134–144.