

ISOGENY BASED CRYPTOGRAPHY MID-TERM REPORT

Dintyala Rahul Bhardwaj

Supervised by Prof. Venkata Koppula and Prof. Surjeet Kour

1	Introduction	2
2	Intro	2
3	Group Actions and Hard Homogeneous Spaces	3
3.1	Key Exchange	5
3.2	Authentication	6
4	Group Action Models	7
4.1	Effective Group Action (EGA)	7
4.2	Restricted Effective Group Action (REGA)	7
4.3	Known-Order Effective Group Action (KEGA)	8
4.4	Generic Group Action Model (GGAM)	9
4.5	Algebraic Group Action Model	9
5	Elliptic Curves and Isogenies	10

1 INTRODUCTION

2 INTRO

3 GROUP ACTIONS AND HARD HOMOGENEOUS SPACES

The objective of this section is to introduce group actions, for their own sake and as a means of constructing cryptographic primitives. We begin by defining group actions.

Definition 3.1 (Group Action). *A group \mathbb{G} is said to act on a set \mathcal{X} if there is a map $\star : \mathbb{G} \times \mathcal{X} \rightarrow \mathcal{X}$ that satisfies the following two properties :*

- *If e is the identity element of \mathbb{G} , then for any $x \in \mathcal{X}$, we have $e \star x = x$.*
- *For any $g, h \in \mathbb{G}$ and any $x \in \mathcal{X}$, we have $(gh) \star x = g \star (h \star x)$.*

◇

Based on the additional structure in the group action, the following definitions are given :

Definition 3.2. *A group action $(\mathbb{G}, \mathcal{X}, \star)$ is said to be :*

1. ***transitive** if for every $x_1, x_2 \in \mathcal{X}$, there exist a group element $g \in \mathbb{G}$ such that $x_2 = g \star x_1$. For such a transitive group action, the set \mathcal{X} is called a homogeneous space for G .*
2. ***faithful** if for each group element $g \in \mathbb{G}$, either G is the identity element or there exists a set element $x \in \mathcal{X}$ such that $x \neq g \star x$.*
3. ***free** if for each group element $g \in \mathbb{G}$, g is the identity element if and only if there exists some set element $x \in \mathcal{X}$ such that $x = g \star x$.*
4. ***regular** if it is both free and transitive.*

◇

We concern ourselves with regular group actions. Regularity of a group action induces a natural bijection between \mathbb{G} and \mathcal{X} , $g \mapsto g \star x$. So if \mathbb{G} (or \mathcal{X}) is finite, $|\mathcal{X}| = |\mathbb{G}|$.

Let \mathbb{G} be a commutative group, \mathcal{X} be a set, and \star be a regular group action. The for any $x_1, x_2 \in \mathcal{X}$, there exists a unique $g \in \mathbb{G}$ such that $x_2 = g \star x_1$. Borrowing the notation from [?], let $g := \delta(x_2, x_1)$. We also have that $(\exists x \in \mathcal{X}, g \star x = x) \implies g = e$.

The process of utilizing a mathematical construct, such as group actions, in the design of cryptographic primitives necessitates that certain operations be computationally efficient for practical implementation, while others must be inherently difficult to guarantee intractability and security.

The following are *easy*:

-
1. For \mathbb{G} :
 - (a) Given a string g , decide if it represents an element in \mathbb{G} .
 - (b) Given strings g_1, g_2 representing two elements in \mathbb{G} , compute $g_1 g_2, g_1^{-1}$ and decide if $g_1 = g_2$.
 - (c) Find a random element in \mathbb{G} with uniform probability.
 2. For \mathbb{X} :
 - (a) Given a string x , decide if h represents an element in \mathbb{X} .
 - (b) Given $x_1, x_2 \in \mathbb{X}$, decide if $x_1 = x_2$.
 3. For \star : Given $g \in \mathbb{G}$ and $x \in \mathbb{X}$ compute $g \star x$.

Definition 3.3. Let \mathbb{G} be an abelian group and $(\mathbb{G}, \mathbb{X}, \star)$ be. Then the following problems are defined :

1. **Vectorisation Problem:** Given x_1 and $x_2 \in \mathbb{X}$, find $\delta(x_2, x_1)$.
2. **Parallelisation Problem:** Given x_1, x_2 , and $x_3 \in \mathbb{X}$, find the unique x_4 such that $\delta(x_2, x_1) = \delta(x_4, x_3)$.
3. **Parallel Testing Problem:** Given x_1, x_2, x_3 , and $x_4 \in \mathbb{X}$ decide whether $\delta(x_2, x_1) = \delta(x_4, x_3)$.

◇

Remark 3.4. Note that if vectorisation is easy, then so is parallelisation. If parallelisation is easy, then so is parallel testing. We have no reason to believe necessarily, the converse of either of these implications. ◇

Definition 3.5 (Hard Homogeneous Space). A homogeneous space for which all the easy assumptions are true and vectorisation and parallelisation problems are hard is called a hard homogeneous space (HHS). ◇

Definition 3.6 (Very Hard Homogeneous Space). A homogeneous space for which all the easy assumptions are true and Parallel Testing Problem is hard, is called a Very Hard Homogeneous Space (VHHS). ◇

Example 3.7. Let $\mathbb{G} = \langle g \rangle$ be a cyclic group of order n . Let $\text{Aut}(\mathbb{G})$ be the set of automorphisms of \mathbb{G} . Note that any homomorphism ϕ from $\mathbb{G} \rightarrow \mathbb{G}$ is entirely described by $\phi(g)$. If $\phi(g) = g^k$. Then ϕ is an automorphism if $\{mk \pmod n\}_{k=1}^n = \mathbb{Z}_n$, which happens if and only if $\gcd(k, n) = 1$. Consider the map $\Psi : \text{Aut}(\mathbb{G}) \rightarrow \mathbb{Z}_n^*$ that maps $(g \mapsto g^c) \mapsto c$. This map is clearly an isomorphism.

Let \mathfrak{g} be the set of generators of \mathbb{G} . Then $\text{Aut}(\mathbb{G})$ acts regularly on \mathfrak{g} through the action $\star : \text{Aut}(\mathbb{G}) \times \mathfrak{g} \rightarrow \mathfrak{g}$, $((g \mapsto g^c), h) \mapsto h^c$.

◇

3.1 Key Exchange

Consider the following Key-Exchange Protocol

Construction 3.8 (Key Exchange via. Hard Homogeneous Spaces). Let \mathbb{G} be an abelian group and \mathcal{X} be a hard homogeneous space for \mathbb{G} with respect to the action \star . Alice and Bob use $(\mathbb{G}, \mathcal{X}, \star)$ to derive a shared key as follows :

1. Alice samples $x_0 \leftarrow \mathcal{X}$, $g_1 \leftarrow \mathbb{G}$ and sends $(x_0, x_1 = g_1 \star x_0)$ to Bob.
2. Bob samples $g_2 \leftarrow \mathbb{G}$ and sends $x_2 = g_2 \star x_0$ to Alice.
3. Alice computes $g_1 \star x_2$ and Bob computes $g_2 \star x_1$.

◇

The correctness for this protocol is clear since $g_1 \star x_2 = g_1 \star (g_2 \star x_0) = (g_1 g_2) \star x_0 = (g_2 g_1) \star x_0 = g_2 \star (g_1 \star x_0) = g_2 \star x_1$.

An eavesdropper can learn $(x_0, x_1 = g_1 \star x_0, x_2 = g_2 \star x_0)$. If an adversary \mathcal{A} can solve the parallelization problem, then $\mathcal{A}(x_0, x_1, x_2) = x_3$ such that $\delta(x_3, x_2) = \delta(x_1, x_0) = g_1$. Since $x_3 = g_1 \star x_2 = g_1 \star (g_2 \star x_0) = (g_1 g_2) \star x_0$, which is the required key, this key-exchange protocol is only as safe as the parallelisation problem is hard. We capture this in the following definition.

Definition 3.9. Let \mathbb{G} be an abelian group, \mathcal{X} be a homogeneous space for \mathbb{G} and $(\mathbb{G}, \mathcal{X}, \star)$ be a regular group action. We say that the Decisional HHS problem is hard for $(\mathbb{G}, \mathcal{X}, \star)$ if, for any p.p.t. adversary \mathcal{A} , the following quantity is negligible:

$$\left| \Pr \left[\begin{array}{c} x_0 \leftarrow \mathcal{X}, g_1, g_2 \leftarrow \mathbb{G} \\ 0 \leftarrow \mathcal{A}(x_0, g_1 \star x_0, g_2 \star x_0, (g_1 g_2) \star x_0) \end{array} \right] - \Pr \left[\begin{array}{c} x_0 \leftarrow \mathcal{X}, g_1, g_2, g_3 \leftarrow \mathbb{G} \\ 0 \leftarrow \mathcal{A}(x_0, g_1 \star x_0, g_2 \star x_0, g_3 \star x_0) \end{array} \right] \right|$$

◇

3.2 Authentication

Authentication refers to the process of verifying the identity of a user, system, or entity, and ensuring that the information exchanged between two parties is genuine and that the person or entity on the other side is who they claim to be.

Couveignes adapts the Feige-Fiat-Shamir identification scheme to get the following construction.

Construction 3.10 (Authentication via. Hard Homogeneous Spaces). *Let \mathbb{G} be an abelian group and \mathcal{X} be a hard homogeneous space for \mathbb{G} with respect to the action \star and x_0 be an element of \mathcal{X} . $(\mathbb{G}, \mathcal{X}, \star, h_0)$ are publicly known.*

Every user i samples a group element g_i from \mathbb{G} , computes $x_i = g_i \star x_0$ and publishes x_i . Let Alice and Bob be user i and user j respectively. If Alice wants to confirm Bob's identity, it will do the following :

- 1. Alice will find x_j from the publicly available record, sample a random group element g_a from \mathbb{G} and send $x_a = g_a \star x_j$ to Bob.*
- 2. Bob computes $x_b = g_j^{-1} \star x_a$ and sends it to Alice.*
- 3. Alice verifies whether $x_b = g_a \star x_0$.*

◇

Correctness follows from the following : $g_a \star x_0 = (g_j^{-1} g_a g_j) \star x_0 = g_j^{-1} \star ((g_a g_j) \star x_0) = x_b$.

4 GROUP ACTION MODELS

4.1 Effective Group Action (EGA)

Definition 4.1 (Effective Group Action). A group action $(\mathbb{G}, \mathcal{X}, \star)$ is effective if:

1. \mathbb{G} is finite, with efficient algorithms for:
 - (a) **Membership testing:** Check if a bit string represents a valid element in \mathbb{G} .
 - (b) **Equality testing:** Check if two bit strings represent the same element in \mathbb{G} .
 - (c) **Sampling:** Sample an element $g \in \mathbb{G}$.
 - (d) **Inversion:** Compute g^{-1} for any $g \in \mathbb{G}$.
2. \mathcal{X} is finite, with efficient algorithms for:
 - (a) **Membership testing:** Check if a bit string represents an element in \mathcal{X} .
 - (b) **Unique representation:** Compute a canonical representation \hat{x} for any $x \in \mathcal{X}$.
3. A known distinguished element $x_0 \in \mathcal{X}$ (origin).
4. An efficient algorithm exists for computing $g \star x$ given any $g \in \mathbb{G}$ and $x \in \mathcal{X}$.

◇

Definition 4.2 (One-Way Group Action). A group action $(\mathbb{G}, \mathcal{X}, \star)$ is a one-way if the family of efficiently computable functions $\{f_x : \mathbb{G} \rightarrow \mathcal{X}\}_{x \in \mathcal{X}}$ is one-way, where $f_x : g \mapsto g \star x$.

◇

Definition 4.3 (Weak Unpredictable Group Action). A group action $(\mathbb{G}, \mathcal{X}, \star)$ is weakly unpredictable if the family of efficiently computable permutations $\{\pi_g : \mathcal{X} \rightarrow \mathcal{X}\}_{g \in \mathbb{G}}$ is

◇

4.2 Restricted Effective Group Action (REGA)

In the previous section, we made the assumption (or hoped) that for any $g \in \mathbb{G}$ and $x \in \mathcal{X}$, computing $g \star x$ is easy.

The group \mathbb{G} , the homogeneous space \mathcal{X} , and the corresponding group action \star we will be working with in the isogeny-based cryptography setting will be non-trivial. Evaluating the group action efficiently for all $g \in \mathbb{G}$ and $x \in \mathcal{X}$ will not be possible.

Since every group has a set of generators, if one can evaluate efficiently the group action for that set of generators, then as long as the exponents are polynomial in the security parameter, the group action can be evaluated efficiently.

[ADMP2020] capture this limitation through their definition of a *Restricted Effective Group Action* (REGA).

Definition 4.4 (Restricted Effective Group Action). *Let $(\mathbb{G}, \mathcal{X}, \star)$ be a group action with a not-necessarily minimal generating set $\mathbf{g} = \{g_1, \dots, g_n\}$ and $G = \langle \mathbf{g} \rangle$. The action is said to be \mathbf{g} -restricted effective if:*

1. \mathbb{G} is finite, and $n = \text{poly}(\log |\mathbb{G}|)$.
2. \mathcal{X} is finite, with efficient algorithms for:
 - (a) **Membership testing:** Check if a bit string represents an element in \mathcal{X} .
 - (b) **Unique representation:** Compute a canonical string \hat{x} for any $x \in \mathcal{X}$.
3. A known distinguished element $x_0 \in \mathcal{X}$ (origin).
4. There exists an efficient algorithm that, given any $i \in [n]$ and a bit string representation of $x \in \mathcal{X}$, computes $g_i \star x$ and $g_i^{-1} \star x$.

◇

4.3 Known-Order Effective Group Action (KEGA)

[ADMP2020] extend the Effective Group Action (EGA) model by assuming the group structure of \mathbb{G} is explicitly known. By "known order," we mean that the group \mathbb{G} has a known set of generators $\mathbf{g} = \{g_1, \dots, g_n\}$ along with their corresponding orders (m_1, \dots, m_n) . This is equivalent to expressing \mathbb{G} as a direct sum decomposition $\mathbb{G} \cong \bigoplus_{i=1}^n \mathbb{Z}_{m_i}$.

A special case of this model is when \mathbb{G} is cyclic, meaning $\mathbb{G} = \langle g \rangle \cong \mathbb{Z}/m\mathbb{Z}$. We define the lattice $\mathcal{L} = \bigoplus_{i=1}^n m_i \mathbb{Z}$, and the map $\phi : \mathbb{Z}^n / \mathcal{L} \rightarrow \mathbb{G}$, where $(a_1, \dots, a_n) \mapsto \prod_{i=1}^n g_i^{a_i}$. This mapping is an effective isomorphism, and its inverse corresponds to solving a generalized discrete logarithm problem.

4.4. GENERIC GROUP ACTION MODEL (GGAM)

If $(\mathbb{G}, \mathcal{X}, \star)$ is an instance of the EGA, it can be shown that $(\mathbb{Z}^n / \mathcal{L}, \mathcal{X}, \star)$ is also an EGA via the isomorphism ϕ . Consequently, $\mathbb{Z}^n / \mathcal{L}$ serves as a standard representation of the group \mathbb{G} .

Definition 4.5 (Known-Order Effective Group Action (KEGA) Model). *A Known-Order Effective Group Action (KEGA) is an EGA $(\mathbb{Z}^n / \mathcal{L}, \mathcal{X}, \star)$, where the lattice \mathcal{L} is determined by the tuple (m_1, \dots, m_n) , representing the orders of the generators.* \diamond

Remark 4.6. *Since for an abelian group \mathbb{G} , Shor's Algorithm and its generalization precisely compute an isomorphism $\mathbb{G} \cong \bigoplus_{i=1}^n \mathbb{Z}_{m_i}$, KEGA and abelian EGA are quantumly equivalent.* \diamond

4.4 Generic Group Action Model (GGAM)

4.5 Algebraic Group Action Model

5 ELLIPTIC CURVES AND ISOGENIES

Definition 5.1 (Plane Curves). *An affine plane algebraic curve C defined over \mathbb{k} is defined by a non-constant polynomial $f(x, y) \in \mathbb{k}[x, y]$, such that $C : f(x, y) = 0$.* \diamond

Example 5.2. $f(x, y) = y - 2x^2$, $f(x, y) = y - mx - c$ \diamond

Let \mathbb{k} be the algebraic closure of \mathbb{k} .

Definition 5.3. *The set of points (x, y) in \mathbb{k}^2 (resp. $\overline{\mathbb{k}}$) such that $f(x, y) = 0$ is called the set of \mathbb{k} -rational points (resp. set of $\overline{\mathbb{k}}$ -rational points).* \diamond

Definition 5.4 (Smooth Curve). *A plane curve $C : f(x, y) = 0$ is called smooth if and only if $\left(\frac{\partial f}{\partial x}(x, y), \frac{\partial f}{\partial y}(x, y)\right) \neq (0, 0)$ for all $(x, y) \in C(\overline{\mathbb{k}})$.* \diamond

Example 5.5. Let $f(x, y) = y^2 - x^3$, $C : y^2 = x^3$. Then $\left(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}\right) = (-3x^2, 2y) = (0, 0) \iff (x, y) = (0, 0)$. Therefore, C is not smooth. \diamond

Since the goal of this section is to showcase the details of the group action behind the abstraction, we will not go into too much mathematical detail and take certain results as facts.

Definition 5.6 (Elliptic Curve). *Let \mathbb{k} be a field. An elliptic curve E/\mathbb{k} is a smooth projective algebraic curve of genus 1 defined over \mathbb{k} with a distinguished \mathbb{k} -rational point \mathcal{O}_E .* \diamond

Fact 1. Let $f(x, y) \in \mathbb{k}[x, y]$ of degree d . If the curve $C : f(x, y) = 0$ is smooth, then its genus is $g = \frac{(d-1)(d-2)}{2}$.

Considering this fact and 5.6, we equate 1 with $(d-1)(d-2)/2$ to get that $d = 3$. So, $C : f(x, y) = 0$ is an elliptic curve if and only if :

1. $f(x, y) = 0$, $\frac{\partial f}{\partial x}(x, y) = 0$, $\frac{\partial f}{\partial y} = 0$ has no solution in \mathbb{C}^2 .
2. $\deg f = 3$
3. the point at infinity is non-singular.

Lemma 5.7. *The short Weierstrass equation $y^2 = x^3 + Ax + B$ defines a genus one curve if and only if $4a_4^3 + 27a_6^2 \neq 0$.*

Proof. Suppose there were a point $(x, y) \in \overline{\mathbb{k}}^2$ such that $\partial f / \partial x = -3x^2 - A = 0$, $\partial f / \partial y = 2y = 0$, and $y^2 = x^3 + Ax + B$. These equations give us $x^3 + Ax + B = 0$, $3x^2 + A = 0$. Therefore, $\frac{2}{3}Ax + B = 0$ or $x = -\frac{3B}{2A}$. If $3(-3B/2A)^2 + A \neq 0$, then these equations have no solution. Therefore the curve is smooth if and only if $-27B^2 - 4A^3 = 0$. \square

Definition 5.8 (Short Weierstrass Form). *The curve $E : y^2 = x^3 + Ax + B$, $A, B \in \mathbb{k}$, $4A^3 + 27B^2 \neq 0$ is an elliptic curve defined over \mathbb{k} in Short Weierstrass form.* \diamond

Fact 2. *By Riemann-Roch Theorem it can be shown that any plane curve has genus one if and only if it is isomorphic to a plane curve of the form :*

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

If the characteristic of \mathbb{k} is not 2 (resp. 2 or 3), then a_1 and a_3 (resp. a_1, a_2 , and a_3) can be made zero via a linear change of coordinates.

Combining this fact with 5.8, we note that every elliptic curve defined over $\mathbb{k}(\text{char}(\mathbb{k}) \neq 2, 3)$ is isomorphic to an elliptic curve in short Weierstrass form.

Example 5.9. $E : y^2 = x^3 + x + 3$ over \mathbb{F}_5 , $y^2 = x^3 + 2x + 27$ over \mathbb{F}_{47} . \diamond

We define the following sets :

$$E(\mathbb{k}) := \{(x, y) \in \mathbb{k}^2 : y^2 = x^3 + Ax + B\}$$

$$E(\overline{\mathbb{k}}) := \{(x, y) \in \overline{\mathbb{k}}^2 : y^2 = x^3 + Ax + b\}.$$

Example 5.10. Let $E : y^2 = x^3 + x$ over \mathbb{F}_3 . Then $E(\overline{\mathbb{F}_3})$ is infinite whereas $E(\mathbb{F}_3) = \{(0, 0), (2, 1), (2, 2), O_E\}$. \diamond

Definition 5.11 (Group Law on Elliptic Curves). *Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points on E different from the point at infinity, then we define a composition law \oplus on E as follows :*

1. $P \oplus O = O \oplus P = P$ for any point $P \in E$.
2. If $x_1 = x_2$ and $y_1 = -y_2$, then $P_1 \oplus P_2 = O$.
3. Otherwise set $\lambda := \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & P \neq Q \\ \frac{3x_1^2 + A}{2y_1} & P = Q \end{cases}$. Then the point $P_1 \oplus P_2 = (\lambda^2 - x_1 - x_2, -\lambda x_3 - y_1 + \lambda x_1)$.

\diamond

Remark 5.12. *It can be verified that the sets $E(\mathbb{k})$, and $E(\overline{\mathbb{k}})$ along with the operation \oplus form abelian groups. Wherever unambiguous, we will just write $+$ instead of \oplus .* \diamond

Definition 5.13 (Isogeny). Let E_1 and E_2 be two elliptic curves defined over \mathbb{k} . An isogeny $\varphi : E_1 \rightarrow E_2$ is a non-constant rational map which is also a group homomorphism. \diamond

Lemma 5.14. Let E_1 and E_2 be elliptic curves over \mathbb{k} in short Weierstrass form, and let $\varphi : E_1 \rightarrow E_2$ be an isogeny. Then φ can be defined by an affine rational map of the form $\varphi(x, y) = \left(\frac{f_1(x)}{g_1(x)}, \frac{f_2(x)}{g_2(x)}y \right)$, where $f_1, f_2, g_1, g_2 \in \mathbb{k}[x]$ and $\gcd(f_1, g_1) = \gcd(f_2, g_2) = 1$.

Definition 5.15 (Standard Form of an Isogeny). Let E_1 and E_2 be elliptic curves over \mathbb{k} , then an isogeny $\varphi : E_1 \rightarrow E_2$ is said to be in standard form if :

$$\varphi(x, y) = \left(\frac{f_1(x)}{g_1(x)}, \frac{f_2(x)}{g_2(x)}y \right),$$

where $f_1, f_2, g_1, g_2 \in \mathbb{k}[x]$ and $\gcd(f_1, g_1) = \gcd(f_2, g_2) = 1$. \diamond

Lemma 5.16. Let $E_1 : y^2 = f_1(x)$ and $E_2 : y^2 = f_2(x)$ be two elliptic curves over \mathbb{k} and let $\varphi : \varphi(x, y) = \left(\frac{f_1(x)}{g_1(x)}, \frac{f_2(x)}{g_2(x)}y \right)$ be an isogeny from E_1 to E_2 in standard form. Then g_2^3 divides g_1^2 and g_1^2 divides $g_2^3 f_1$. Moreover, $g_1(x)$ and $g_2(x)$ have the same set of roots in \mathbb{k} .

Corollary 5.17. Let $\varphi : \varphi(x, y) = \left(\frac{f_1(x)}{g_1(x)}, \frac{f_2(x)}{g_2(x)}y \right)$ be an isogeny from $E_1 \rightarrow E_2$ in standard form. Then $\ker \varphi = \{P \in E_1(\overline{\mathbb{k}}) : \varphi P = O_{E_2}\} = \{(x_0, y_0) \in E_1(\overline{\mathbb{k}}) : g_1(x_0) = 0\} \cup \{O_{E_1}\}$. The kernel of φ is a finite subgroup of $E_1(\overline{\mathbb{k}})$.

Definition 5.18 (Degree and Separability of an Isogeny). Let $\varphi(x, y) = \left(\frac{f_1(x)}{g_1(x)}, \frac{f_2(x)}{g_2(x)}y \right)$ be an isogeny in standard form. The degree of φ is $\deg \varphi := \max\{\deg f_1, \deg g_1\}$, and we say that φ is separable if the derivative of $\frac{f_1(x)}{g_1(x)}$ is non-zero; otherwise we say that φ is inseparable. \diamond

Example 5.19. Let $E : y^2 = x^3 + x + 3$ over \mathbb{F}_5 and $E' : y^2 = x^3 + x$ over \mathbb{F}_5 . Let $\varphi : E \rightarrow E', (x, y) \mapsto \left(\frac{x^2-x-1}{x-1}, \frac{x^2-2x-2}{x^2-2x+1}y \right)$ be an isogeny in standard form. Then :

- $\deg \varphi = 2$,
- $\left(\frac{x^2-x-1}{x-1} \right)' = 1 + \frac{1}{(x-1)^2} \neq 0$, and

-
- $\ker \varphi = \{(x_0, y_0) \in E_1(\overline{\mathbb{k}}) : x_0 - 1 = 0\} \cup \{\mathcal{O}_{E_1}\} = \{(1, 0), \mathcal{O}_{E_1}\} \cong \mathbb{Z}/2\mathbb{Z}$.

◇

Definition 5.20 (*m-torsion subgroup*). Let E be an elliptic curve over \mathbb{k} . Let $[m] : E \rightarrow E$ denote the map $P \mapsto mP$. Then the kernel of $[m]$ is called the *m-torsion subgroup* of E .

◇

Example 5.21. Let $E : y^2 = x^3 + x + 3$ over \mathbb{F}_5 . Let $[2] : E \rightarrow E$ denote the map $P \mapsto 2P = P + P$. The multiplication by 2 isogeny in standard form is given by $(x, y) \mapsto \left(\frac{x^4 - 2x^2 + x + 1}{x^3 + x + 3}, \frac{x^6 - 2x + 2}{x^6 + 2x^4 + x^3 + x^2 + x - 1}y \right)$. Then :

- $\deg [2] = 4$,
- $[2]$ is separable, and
- $E[2] = \ker [2] = \{P \in E(\overline{\mathbb{F}_5}) : 2P = \mathcal{O}_E\} = \{(x_0, y) \in E(\overline{\mathbb{F}_5}) : x_0^3 + x_0 + 3 = 0\} = \{(1, 0), (\alpha, 0), (4\alpha + 4), \mathcal{O}_E\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

◇

Example 5.22. Let $E : y^2 = x^3 + Ax + B$ over \mathbb{k} . Let $[-1] : E \rightarrow E$ denote the map $P \mapsto -P$ or $(x, y) \mapsto (x, -y)$. Then :

- $\deg [-1] = 1$,
- $[-1]$ is separable, and
- $\ker [-1] = \{\mathcal{O}_E\}$ is trivial.

◇

Example 5.23. Let $E : y^2 = x^3 + Ax + B$ over \mathbb{F}_q , $q = p^n$ for a prime p . Then the Frobenius Endomorphism $\pi_E : E \rightarrow E$ maps $(x, y) \mapsto (x^q, y^q)$. Then :

- $\deg \pi_E = q$,
- π_E is inseparable $((x^q)' = qx^{q-1} = 0)$, and
- $\ker \pi_E = \{\mathcal{O}_E\}$ is trivial.

◇

Fact 3. An isogeny φ is separable if and only if $|\ker \varphi| = \deg \varphi$.

Definition 5.24 (*Cyclic Isogeny*). An isogeny φ is said to be cyclic if $\ker \varphi$ is a cyclic subgroup.

◇

Definition 5.25 (Endomorphism, Isomorphism, Automorphism). *Let E be an elliptic curve. An isogeny from E to itself is called an endomorphism. An isogeny of degree 1 is called an isomorphism. An endomorphism which is also an isomorphism is called an automorphism.* \diamond