

Generating supersingular curves with modular polynomials

Simon Pohmann

July 29, 2022

1 Introduction

2 Ordinary isogeny graphs

2.1 Imaginary quadratic orders

For this part, let \mathcal{O} be an order in an imaginary quadratic number field K .

Lemma 2.1. *Let $\mathfrak{p} \leq \mathcal{O}_K$ be a prime with $\mathfrak{N}(\mathfrak{p}) \perp [\mathcal{O}_K : \mathcal{O}]$. Then \mathfrak{p} has a set of generators in \mathcal{O} .*

Proof. Suppose \mathfrak{p} is a prime over p , and let $\mathcal{O} = \mathbb{Z}[\phi]$. We use the decomposition law in Dedekind ring extensions. Since $\mathfrak{N}(\mathfrak{p}) \perp [\mathcal{O}_K : \mathcal{O}]$ are coprime, we can apply it with a generator ϕ of \mathcal{O} .

If $\text{MiPo}(\phi) = f(X)g(X) \pmod{p}$ splits, then have

$$p\mathcal{O}_K = (p, f(\phi))(p, g(\phi))$$

and so the prime ideals over p are $(p, f(\phi))$ and $(p, g(\phi))$. If $\text{MiPo}(\phi) \pmod{p}$ is irreducible, then have that $p\mathcal{O}_K$ is prime and thus the only prime ideal over p . Hence, all prime ideals over p (including \mathfrak{p}) have a set of generators in \mathcal{O} . \square

Corollary 2.2. *Let $\mathfrak{a} \leq \mathcal{O}_K$ be an ideal with $\mathfrak{N}(\mathfrak{a}) \perp [\mathcal{O}_K : \mathcal{O}]$. Then \mathfrak{a} has a set of generators in \mathcal{O} .*

Proposition 2.3. *Let $\mathfrak{p} \leq \mathcal{O}$ be a prime ideal with $\mathfrak{N}(\mathfrak{p}) \perp [\mathcal{O}_K : \mathcal{O}]$ and $\mathfrak{p}' = \mathfrak{p}\mathcal{O}_K$. Then $\mathcal{O}_{\mathfrak{p}} = (\mathcal{O}_K)_{\mathfrak{p}'}$.*

Proof. We have $\mathcal{O}_K = \mathbb{Z}[\alpha]$ and $\mathcal{O} = \mathbb{Z}[f\alpha]$ where $f = [\mathcal{O}_K : \mathcal{O}]$. Thus $f \notin \mathfrak{p}$ and so $f \in \mathcal{O}_{\mathfrak{p}}^*$. Therefore $\mathcal{O}_K \subseteq \mathcal{O}_{\mathfrak{p}}$ and thus $(\mathcal{O}_K)_{\mathfrak{p}'} \subseteq \mathcal{O}_{\mathfrak{p}}$. \square

Proposition 2.4. *Let $\mathfrak{I}(\mathcal{O})$ resp. $\mathfrak{I}(\mathcal{O}_K)$ denote the set of invertible ideals of norm $\perp [\mathcal{O}_K : \mathcal{O}]$. Then*

$$\mathfrak{I}(\mathcal{O}) \rightarrow \mathfrak{I}(\mathcal{O}_K), \quad \mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$$

is a monoid isomorphism with inverse

$$\mathfrak{I}(\mathcal{O}_K) \rightarrow \mathfrak{I}(\mathcal{O}), \quad \mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}$$

Proof. Clearly, this is a well-defined monoid homomorphism. Hence, we have to show that it is bijective.

By Corollary 2.2, we know that any $\mathfrak{a} \leq \mathcal{O}_K$ with $\mathfrak{N}(\mathfrak{a}) \perp [\mathcal{O}_K : \mathcal{O}]$ has generators in \mathcal{O} , thus $(\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K = \mathfrak{a}$. This shows that $\mathfrak{a} \cap \mathcal{O}$ is a preimage of \mathfrak{a} , and so the map is surjective.

Assume now $\mathfrak{a}, \mathfrak{b} \leq \mathcal{O}$ with $\mathfrak{a}\mathcal{O}_K = \mathfrak{b}\mathcal{O}_K$ and $\mathfrak{N}(\mathfrak{a}), \mathfrak{N}(\mathfrak{b}) \perp [\mathcal{O}_K : \mathcal{O}]$. We show that $\mathfrak{a}_{\mathfrak{p}} = \mathfrak{b}_{\mathfrak{p}}$ for all primes $\mathfrak{p} \leq \mathcal{O}$. Note that if $\mathfrak{N}(\mathfrak{p}) \not\perp [\mathcal{O}_K : \mathcal{O}]$, this holds trivially, as $\mathfrak{a}_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}} = \mathfrak{b}_{\mathfrak{p}}$. Otherwise, note that

$$\mathfrak{a}_{\mathfrak{p}} = \mathfrak{a}_{\mathfrak{p}}\mathcal{O}_{\mathfrak{p}} = \mathfrak{a}(\mathcal{O}_K)_{\mathfrak{p}} = \mathfrak{a}\mathcal{O}_K(\mathcal{O}_K)_{\mathfrak{p}} = \mathfrak{b}\mathcal{O}_K(\mathcal{O}_K)_{\mathfrak{p}} = \mathfrak{b}_{\mathfrak{p}}(\mathcal{O}_K)_{\mathfrak{p}} = \mathfrak{b}_{\mathfrak{p}}$$

as $\mathcal{O}_{\mathfrak{p}} = (\mathcal{O}_K)_{\mathfrak{p}}$. This shows that $\mathfrak{a}_{\mathfrak{p}} = \mathfrak{b}_{\mathfrak{p}}$ at all primes, so $\mathfrak{a} = \mathfrak{b}$ and our map is injective. Furthermore, since $(\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K = \mathfrak{a}$, we see that it has the inverse

$$\mathfrak{I}(\mathcal{O}_K) \rightarrow \mathfrak{I}(\mathcal{O}), \quad \mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}$$

which must then be well-defined. □

2.2 The class group action

The class group action that we will define in the following is the most important tool when working with isogeny graphs of ordinary curves. Because of this, it is mentioned in more or less all the literature dealing with the topic. For me, it was thus quite surprising that I could nowhere find a precise and relatively elementary proof for the statement in the case of finite fields.

Most sources cite [Wat69, Thm 4.5], however the statement there is not as explicit as one might wish, and the proof is done in the much more general theory of abelian schemes. Apart from that, there are many references to the corresponding statement for curves over \mathbb{C} , but these ignore some of the subtleties introduced by non-separable isogenies. Therefore, we now present a relatively simple proof of the class group action for ordinary curves defined over a finite field and explicitly handle the non-separable case.

Definition 2.5. For an integral ideal $\mathfrak{a} \leq \text{End}(E)$ of an ordinary Elliptic Curve E , define the \mathfrak{a} -torsion

$$E[\mathfrak{a}] := \bigcap_{\alpha \in \mathfrak{a}} \ker(\alpha)$$

From now on, we will often compare endomorphism rings of isogeneous curves. To do so, we embed those rings into an imaginary quadratic number field K . However, the field K and its orders can have nontrivial automorphisms, which means the embedding $\text{End}(E) \rightarrow K$ cannot be unique. Fortunately, there is a unique embedding that is canonical in the following sense.

Lemma 2.6. *Let $\phi : E \rightarrow E'$ be an isogeny. Then there is an isomorphism*

$$\Phi : \text{End}(E) \otimes \mathbb{Q} \rightarrow \text{End}(E') \rightarrow \mathbb{Q}, \quad \tau \mapsto \frac{1}{\deg(\phi)} \phi \circ \tau \circ \hat{\phi}$$

Furthermore, if we assume E to be ordinary, then this is canonical in the sense that for any other isogeny $\psi : E \rightarrow E'$ have $\Phi = \Psi$.

If we set $K = \text{End}(E) \otimes \mathbb{Q}$, then of course this gives a canonical embedding $\text{End}(E') \rightarrow K$ for each curve E' isogeneous to E . From now on, whenever we consider such an embedding, or identify isomorphic endomorphism rings of isogeneous curves, this embedding shall be used.

Proposition 2.7. *Let $\phi : E \rightarrow E'$ be an isogeny of prime degree p between (not necessarily ordinary) Elliptic Curves. Then (after embedding $\text{End}(E')$ via Φ and $\text{End}(E)$ into $\text{End}(E) \otimes \mathbb{Q}$) exactly one of the following is the case.*

- $\text{End}(E) = \text{End}(E')$ and we call ϕ horizontal.
- $\text{End}(E) \subseteq \text{End}(E')$ with $[\text{End}(E') : \text{End}(E)] = p$. We call ϕ ascending.
- $\text{End}(E) \supseteq \text{End}(E')$ with $[\text{End}(E) : \text{End}(E')] = p$. We call ϕ descending.

Furthermore, we will sometimes talk about horizontal or vertical isogenies *at a prime l* , which is defined by the next proposition. The advantage is that this is defined for all isogenies, not just those of prime degree.

Proposition 2.8. *Similarly, let $\phi : E \rightarrow E'$ be an isogeny of any degree n . Further, let l be a prime. Then (after embedding $\text{End}(E') \otimes \mathbb{Z}_{(l)}$ via Φ and $\text{End}(E) \otimes \mathbb{Z}_{(l)}$ into $\text{End}(E) \otimes \mathbb{Q}$) exactly one of the following is the case.*

- $\text{End}(E) \otimes \mathbb{Z}_{(l)} = \text{End}(E') \otimes \mathbb{Z}_{(l)}$ and we call ϕ horizontal at l .
- $\text{End}(E) \otimes \mathbb{Z}_{(l)} \subseteq \text{End}(E') \otimes \mathbb{Z}_{(l)}$ with $[\text{End}(E') \otimes \mathbb{Z}_{(l)} : \text{End}(E) \otimes \mathbb{Z}_{(l)}] = l^r$ for $r > 0$. We call ϕ ascending at l .
- $\text{End}(E) \otimes \mathbb{Z}_{(l)} \supseteq \text{End}(E') \otimes \mathbb{Z}_{(l)}$ with $[\text{End}(E) \otimes \mathbb{Z}_{(l)} : \text{End}(E') \otimes \mathbb{Z}_{(l)}] = p$ for $r > 0$. We call ϕ descending at l .

Now we can make a step towards the class group action and present how we assign isogenies to (integral, invertible) ideals of the endomorphism ring.

Definition 2.9. For an ordinary Elliptic Curve E and an integral, invertible ideal ¹ $\mathfrak{a} = \mathfrak{b}(p, \pi_E)^r \leq \text{End}(E)$ with $\mathfrak{b} \perp (p, \pi_E)$ define the isogeny

$$\phi_{E, \mathfrak{a}} : E \longrightarrow E/E[\mathfrak{b}] \xrightarrow{\pi} E_{\mathfrak{a}} := (E/E[\mathfrak{b}])^{(p^r)}$$

where $E \rightarrow E/E[\mathfrak{b}]$ is the separable isogeny with kernel $E[\mathfrak{b}]$ and $\pi : E/E[\mathfrak{b}] \rightarrow (E/E[\mathfrak{b}])^{(p^r)}$ is the r -th power Frobenius map.

In order to define a group action later, we need to be able to chain such isogenies given by ideals. The obvious difficulty here is that the ideals are all in the same ring, but subsequent isogenies will have different curves as domain. Hence, we need to be able to view an ideal $\mathfrak{a} \leq \text{End}(E)$ as an ideal of another endomorphism ring $\text{End}(E')$. As it turns out, the endomorphism rings we consider are all isomorphic, and so this works out nicely.

Lemma 2.10. *Let E be an ordinary Elliptic Curve and $\mathfrak{a} \leq \text{End}(E)$ an integral, invertible ideal. Then $\text{End}(E) \cong \text{End}(E_{\mathfrak{a}})$. In particular, $\phi_{E, \mathfrak{a}}$ is horizontal at every prime l .*

Proof. Let $\mathfrak{a} = \mathfrak{b}(p, \pi_E)^r$ with $\mathfrak{b} \perp (p, \pi_E)$. We show that $\text{End}(E) \cong \text{End}(E/E[\mathfrak{b}])$ and the claim follows, as for any Elliptic Curve E , have an isomorphism

$$\text{End}(E) \rightarrow \text{End}(E^{(p)}), \quad \alpha \mapsto \alpha^{(p)}$$

It suffices to show that the separable isogeny $\phi := \phi_{E, \mathfrak{b}}$ is horizontal at each prime l .

Assume for a contradiction that ϕ is descending at l . In other words, there is $\tau \in \text{End}(E)$ such that $\phi \circ \tau \circ \hat{\phi}$ is not divisible by l . Hence, $E'[l] \not\subseteq \ker(\phi \circ \tau \circ \hat{\phi})$ and there is a point $P \in E'[l]$ with $\phi(\tau(\hat{\phi}(P))) \neq O$. This implies $\tau(\hat{\phi}(P)) \notin E[\mathfrak{a}]$ and thus there is $\alpha \in \mathfrak{a}$ with $\tau(\hat{\phi}(P)) \notin \ker(\alpha)$. Note that α factors through ϕ as

$$\begin{array}{ccccc} & & \alpha & & \\ & \nearrow & & \searrow & \\ E & \xrightarrow{\phi} & E' & \xrightarrow{\psi} & E \end{array}$$

We assume $l \mid n$, otherwise the claim is trivial. However, then we have the contradiction

$$\begin{aligned} \psi((\phi \circ \tau \circ \hat{\phi})(P)) &= (\psi \circ \phi \circ \tau \circ \hat{\phi})(P) = (\alpha \circ \tau \circ \hat{\phi})(P) \\ &= (\tau \circ \alpha \circ \hat{\phi})(P) = (\tau \circ \psi \circ [n])(P) = (\tau \circ \psi)(O) = O \end{aligned}$$

since $\tau \circ \alpha = \alpha \circ \tau$ ($\text{End}(E)$ is commutative). □

Lemma 2.11. *Let \mathcal{O} be a quadratic imaginary order with $p \nmid d(\mathcal{O})$ with two integral, invertible ideals $\mathfrak{a}, \mathfrak{b} \leq \mathcal{O}$. Let further E be an Elliptic Curve with $\text{End}(E) \cong \mathcal{O}$. Identifying $\text{End}(E_{\mathfrak{a}})$ with \mathcal{O} by the canonical isomorphism $\Phi_{E, \mathfrak{a}} : \text{End}(E) \xrightarrow{\sim} \text{End}(E_{\mathfrak{a}})$, we have*

$$E_{\mathfrak{a}\mathfrak{b}} \cong (E_{\mathfrak{a}})_{\mathfrak{b}} \quad \text{and} \quad \phi_{E, \mathfrak{a}\mathfrak{b}} = \phi_{E_{\mathfrak{a}}, \mathfrak{b}} \circ \phi_{E, \mathfrak{a}}$$

¹By Prop. 2.4, this representation of an ideal \mathfrak{a} is well-defined and unique, as $\mathfrak{N}((p, \pi)) = p \nmid [\mathcal{O}_{\text{End}(E) \otimes \mathbb{Q}} : \text{End}(E)] \mid d(\text{End}(E))$.

Proof. First, we show that $\Phi_{E,\mathfrak{a}}(\pi_E) = \pi_{E_{\mathfrak{a}}}$ and so we can write $\pi \in \mathcal{O}$ for the unique element mapping to the Frobenius in $\text{End}(E)$ resp. $\text{End}(E_{\mathfrak{a}})$. We have that

$$\Phi_{E,\mathfrak{a}}(\pi_E) = \frac{1}{\deg(\phi_{E,\mathfrak{a}})} \phi_{E,\mathfrak{a}} \circ \pi_E \circ \hat{\phi}_{E,\mathfrak{a}}$$

and so

$$\phi_{E,\mathfrak{a}} \circ \hat{\phi}_{E,\mathfrak{a}} \circ \Phi_{E,\mathfrak{a}}(\pi_E) = \phi_{E,\mathfrak{a}} \circ \pi_E \circ \hat{\phi}_{E,\mathfrak{a}}$$

Counting separability degrees on both sides shows that $\Phi_{E,\mathfrak{a}}(\pi_E)$ is purely inseparable, thus must be the Frobenius $\pi_{E_{\mathfrak{a}}}$.

Now write $\mathfrak{a} = \tilde{\mathfrak{a}}(p, \pi)^r$ and $\mathfrak{b} = \tilde{\mathfrak{b}}(p, \pi)^s$. It is now the case that

$$\phi_{E,\mathfrak{a}\mathfrak{b}} = \phi_{E,\tilde{\mathfrak{a}}\tilde{\mathfrak{b}}}^{(p^{r+s})}$$

and

$$\phi_{E_{\mathfrak{a}},\mathfrak{b}} \circ \phi_{E,\mathfrak{a}} = (\phi_{E_{\mathfrak{a}},\tilde{\mathfrak{b}}} \circ \pi_r \circ \phi_{E,\tilde{\mathfrak{a}}})^{(p^s)} = (\phi_{E_{\mathfrak{a}},\tilde{\mathfrak{b}}} \circ \phi)^{(p^r)} = (\phi_{E_{\mathfrak{a}},\tilde{\mathfrak{b}}}^{(q/p^r)} \circ \phi_{E,\tilde{\mathfrak{a}}})^{(p^{r+s})}$$

where $\pi_r : E_{\tilde{\mathfrak{a}}} \rightarrow E_{\tilde{\mathfrak{a}}}^{(p^r)}$ is the p^r -th power Frobenius and $\phi_{E_{\mathfrak{a}},\tilde{\mathfrak{b}}}$ is defined over \mathbb{F}_q . Note that $\phi_{E_{\mathfrak{a}},\tilde{\mathfrak{b}}}$ is the separable isogeny with kernel $E_{\mathfrak{a}}[\tilde{\mathfrak{b}}]$ and thus $\phi_{E_{\mathfrak{a}},\tilde{\mathfrak{b}}}^{(q/p^r)}$ is the separable isogeny with kernel $E_{\mathfrak{a}}^{(q/p^r)}[\tilde{\mathfrak{b}}] = E_{\tilde{\mathfrak{a}}}[\tilde{\mathfrak{b}}]$. In other words, find

$$\phi_{E_{\mathfrak{a}},\tilde{\mathfrak{b}}}^{(q/p^r)} = \phi_{E_{\tilde{\mathfrak{a}}},\tilde{\mathfrak{b}}}$$

and so it suffices to show the claim in the case that $\mathfrak{a} = \tilde{\mathfrak{a}}$, $\mathfrak{b} = \tilde{\mathfrak{b}}$ are integral, invertible ideals coprime to (p, π) .

Having reduced everything to the separable case, it now suffices to show that $\ker(\phi_{E_{\mathfrak{a}},\mathfrak{b}} \circ \phi_{E,\mathfrak{a}}) = E[\mathfrak{a}\mathfrak{b}]$. For simplicity of notation, write $\phi = \phi_{E,\mathfrak{a}}$ and $\psi = \phi_{E_{\mathfrak{a}},\mathfrak{b}}$. Hence, we want to show that $\ker(\psi \circ \phi) = E[\mathfrak{a}\mathfrak{b}]$.

The crucial point here is that our isomorphism $\text{End}(E) \cong \text{End}(E_{\mathfrak{a}})$ is given by Φ . Since the identification of $\text{End}(E)$ and $\text{End}(E_{\mathfrak{a}})$ would hide this, we will be explicit in this part and write

$$i : \mathcal{O} \rightarrow \text{End}(E) \quad \text{and} \quad i' : \mathcal{O} \rightarrow \text{End}(E')$$

for the isomorphisms. Note that $\Phi \circ i = i'$. We have

$$\begin{aligned} \ker(\psi \circ \phi) &= \phi^{-1}(\ker \psi) = \phi^{-1}(E'[\mathfrak{a}]) = \phi^{-1}\left(\bigcap_{\tau \in \mathfrak{a}} \ker(i'(\tau))\right) \\ &= \bigcap_{\tau \in \mathfrak{a}} \phi^{-1}(\ker(i'(\tau))) = \bigcap_{\tau \in \mathfrak{a}} \ker(i'(\tau) \circ \phi) \stackrel{(*)}{=} \bigcap_{\tau \in \mathfrak{a}} \ker(\phi \circ i(\tau)) \\ &= \bigcap_{\tau \in \mathfrak{a}} i(\tau)^{-1}(\ker \phi) = \bigcap_{\tau \in \mathfrak{a}} i(\tau)^{-1}(E[\mathfrak{b}]) = \bigcap_{\tau \in \mathfrak{a}, \rho \in \mathfrak{b}} i(\tau)^{-1}(\ker(i(\rho))) \\ &= \bigcap_{\tau \in \mathfrak{a}, \rho \in \mathfrak{b}} \ker(\underbrace{i(\rho) \circ i(\tau)}_{=i(\rho\tau) \in i(\mathfrak{a}\mathfrak{b})}) = E[\mathfrak{b}\mathfrak{a}] \end{aligned}$$

The equality at $(*)$ holds, since

$$i'(\tau) = (\Phi_* \circ i)(\tau) = \frac{1}{\deg(\phi)} \phi \circ i(\tau) \circ \hat{\phi} \quad \square$$

Lemma 2.12. *Let E be an ordinary curve and $\alpha \in \text{End}(E)$. Then α inseparable if and only if $\alpha \in (p, \pi)$.*

Proof. First, consider

$$\mathfrak{b} := \{\beta \in \text{End}(E) \mid \beta \text{ inseparable}\}$$

This is an ideal, as for two inseparable $\beta_1, \beta_2 \in \text{End}(E)$ have that they factor as

$$\begin{array}{ccccc} & & \beta_i & & \\ & \nearrow & & \searrow & \\ E & \xrightarrow{\pi_1} & E^{(p)} & \xrightarrow{\phi_i} & E \end{array}$$

with the p -th power Frobenius π_1 . Now $\beta_1 + \beta_2 = (\phi_1 + \phi_2) \circ \pi_1$ is inseparable, and clearly $\beta\gamma$ is inseparable for $\beta \in \mathfrak{b}$ and $\gamma \in \text{End}(E)$ (just compare separability degrees).

Furthermore, p and π are inseparable, so $(p, \pi) \subseteq \mathfrak{b}$. Note that in the imaginary quadratic order $\text{End}(E)$, every prime ideal is maximal. Since $\mathfrak{N}((p, \pi)) = p \perp d(\text{End}(E))$, Prop. 2.4 shows that (p, π) is prime, and thus $(p, \pi) = \mathfrak{b}$ (clearly, $\mathfrak{b} \neq \text{End}(E)$). \square

Lemma 2.13. *Let E be an ordinary curve and $\mathfrak{a}, \mathfrak{b} \leq \text{End}(E)$ two integral, invertible ideals. Then $E_{\mathfrak{a}} \cong E_{\mathfrak{b}}$ if and only if $[\mathfrak{a}] = [\mathfrak{b}] \in \text{Cl}(\text{End}(E))$ are in the same ideal class.*

Proof. First, we show the direction \Leftarrow . By assumption, there are $\alpha, \beta \in \mathcal{O}$ such that $\alpha\mathfrak{a} = \beta\mathfrak{b}$. Thus $E_{\alpha\mathfrak{a}} = E_{\beta\mathfrak{b}}$ and it suffices to show that for any Elliptic Curve E and $\alpha \in \text{End}(E)$, have $E_{(\alpha)} \cong E$.

Write $(\alpha) = (p, \pi)^r \mathfrak{a}$ and assume that E is defined over \mathbb{F}_{p^s} . Then $(\alpha)(p)^{\lceil r/s \rceil s - r} = (\pi)^{\lceil r/s \rceil}(\alpha')$ since $(p) = (p, \pi)(p, \pi - t)$ and $(p, \pi)^s = (\pi)$ by an easy computation. Furthermore, $\alpha' \notin (p, \pi)$. Now note that for any curve E , have $E_{(\pi)} = E^{(p^s)} \cong E$ and $E_{(p)} \cong E$, where the latter holds, since in the ordinary case, p factors as

$$\begin{array}{ccccc} & & [p] & & \\ & \nearrow & & \searrow & \\ E & \xrightarrow{\pi_1} & E^{(p)} & \xrightarrow{\phi} & E \end{array}$$

with the p -th power Frobenius π_1 and ϕ is separable with $\ker(\phi) = E[p] = \ker([p]) \cap \ker(\pi - t)$. Thus we see that $E_{(\alpha)} \cong E_{(\alpha')}$ and can assume wlog that $\alpha = \alpha' \notin (p, \pi)$.

By Lemma 2.12, we now see that α is separable, and so clearly $\ker(\alpha) = E[(\alpha)]$. Since $\alpha : E \rightarrow E$ is the separable isogeny on E with kernel $E[(\alpha)]$, we see that $E_{(\alpha)} = E/E[(\alpha)] \cong E$.

Now we consider the other direction \Rightarrow . Again, write $\mathfrak{a} = \tilde{\mathfrak{a}}(p, \pi)^r$ and assume that E is defined over \mathbb{F}_{p^s} . Then we have as before that $\mathfrak{a}(p)^{\lceil r/s \rceil s - r} = (\pi)^{\lceil r/s \rceil} \mathfrak{a}'$ for the ideal $\mathfrak{a}' = \tilde{\mathfrak{a}}(p, \pi - t)^{\lceil r/s \rceil s - r}$. Now clearly $[\mathfrak{a}] = [\mathfrak{a}']$ are in the same ideal class and $\mathfrak{a}' \perp (p, \pi)$. Furthermore, by the direction \Leftarrow , have $E_{\mathfrak{a}} \cong E_{\mathfrak{a}'}$. Doing the same with \mathfrak{b} , we can assume wlog that $\mathfrak{a} = \mathfrak{a}'$ and $\mathfrak{b} = \mathfrak{b}'$ are ideals coprime to (p, π) .

Therefore, the isogenies $\phi_{E, \mathfrak{a}}$ and $\phi_{E, \mathfrak{b}}$ are separable. Write $E' := E_{\mathfrak{a}} = E_{\mathfrak{b}}$. Choose $N > 0$ such that $[N]^{-1}(E[\mathfrak{a}]) \supseteq E[\mathfrak{b}]$. Now the isogeny $[N] \circ \phi_{E, \mathfrak{a}}$ factors through $\phi_{E, \mathfrak{b}}$, i.e. we get a commutative diagram

$$\begin{array}{ccccc} & & \phi_{E, \mathfrak{a}} & \rightarrow & E' \\ & \nearrow & & & \searrow [N] \\ E & & & & E' \\ & \searrow & \phi_{E, \mathfrak{b}} & \rightarrow & E' \\ & & & & \nearrow \psi \end{array}$$

for some endomorphism $\psi : E' \rightarrow E'$. Clearly the isogenies $[N]$ and ψ are given by the ideals (N) resp. (ψ) , and so we find

$$(N)\mathfrak{a} = (\psi)\mathfrak{b}$$

and the claim follows. \square

Theorem 2.14. *Let \mathcal{O} be an imaginary quadratic order with $p \nmid d(\mathcal{O})$ and denote by $\text{Ell}(\mathcal{O})$ the set of isomorphism classes of all Elliptic Curves E over \mathbb{F}_p with $\text{End}(E) \cong \mathcal{O}$. Then there is a free and transitive group action*

$$\text{Cl}(\mathcal{O}) \times \text{Ell}(\mathcal{O}) \rightarrow \text{Ell}(\mathcal{O}), \quad ([\mathfrak{a}], E) \mapsto E_{\mathfrak{a}}$$

where \mathfrak{a} is an integral, invertible ideal representative of the ideal class $[\mathfrak{a}]$.

Proof. Well-definedness and freeness follow from all the previous lemmas. \square

A similar class group action exists in many other cases, since it is really founded in the theory of abelian varieties, see [Wat69]. Notable examples are the CSIDH class group action for supersingular curves defined over \mathbb{F}_p (see [Cas+18]), its generalization to so-called oriented curves (see [CK20]), and the very classical class group action of Elliptic Curves with complex multiplication (over \mathbb{C}). More concretely, if we consider an order \mathcal{O} in a quadratic imaginary number field and write $\text{Ell}(\mathcal{O})$ for the set of (isomorphism classes of) curves over \mathbb{C} with endomorphism ring \mathcal{O} (these are said to have *complex multiplication*), then there is a free and transitive class group action

$$\text{Cl}(\mathcal{O}) \times \text{Ell}(\mathcal{O}) \rightarrow \text{Ell}(\mathcal{O}), \quad ([\mathfrak{a}], E) \rightarrow E/E[\mathfrak{a}]$$

where we choose \mathfrak{a} to be an integral ideal representative of $[\mathfrak{a}]$. Note that for ideals $\mathfrak{a} \perp (p, \pi)$, this is analogous to our action defined above. However, since the Frobenius has trivial kernel, one needs some addition in the finite field case.

Note that one can still keep the simpler definition

$$\mathrm{Cl}(\mathcal{O}) \times \mathrm{Ell}(\mathcal{O}) \rightarrow \mathrm{Ell}(\mathcal{O}), \quad ([\mathfrak{a}], E) \rightarrow E/E[\mathfrak{a}]$$

also in the finite field case, if we require \mathfrak{a} to be an (integral) ideal representative of $[\mathfrak{a}]$ that is coprime to (p, π) . Clearly, every ideal class has such a representative, since we can multiply with the principal ideal $(p) = (p, \pi)(p, \pi - t)$ and divide out the principal ideal $(\pi) = (p, \pi)^s$. However, some sources do not explicitly mention that \mathfrak{a} must be chosen coprime to (p, π) , which caused me some confusion.

2.3 Vulcanoes

3 Supersingular isogeny graphs

4 Generating supersingular curves