Generalized class group actions on oriented elliptic curves with level structure

Sarah Arpin[1], Wouter Castryck[2], Jonathan Komada Eriksen[3], Gioella Lorenzon[2], and Frederik Vercauteren[2]

[1] Mathematics Institute, Universiteit Leiden, Leiden, The Netherlands and the Quantum Software Consortium of the Netherlands
[2] COSIC, ESAT, KU Leuven, Belgium
[3] Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Trondheim, Norway

Abstract. We study a large family of generalized class groups of imaginary quadratic orders O and prove that they act freely and (essentially) transitively on the set of primitively O-oriented elliptic curves over a field k (assuming this set is non-empty) equipped with appropriate level structure. This extends, in several ways, a recent observation due to Galbraith, Perrin and Voloch for the ray class group. We show that this leads to a reinterpretation of the action of the class group of a suborder $O' \subseteq O$ on the set of O'-oriented elliptic curves, discuss several other examples, and briefly comment on the hardness of the corresponding vectorization problems.

1 Introduction

A current trend in isogeny-based cryptography is to study elliptic curve isogenies that respect certain *level structure*, or additional information about the curves. This has two main catalysts. Firstly, the recently established rapid mixing properties of isogeny graphs of supersingular elliptic curves with a marked cyclic subgroup of order N (Γ_N^0-level structure) have led to improved security foundations, e.g., of the distributed generation of supersingular elliptic curves with unknown endomorphism ring [Arp22,BCC+23]; see [CL23b] for a generalization of these rapid mixing results to arbitrary level structure. Secondly, Robert's unconditional break of SIDH [Rob23a] has revealed that the problem of finding an isogeny between two elliptic curves with full Γ_N-level structure is dramatically easier than in the case of plain elliptic curves, at least for N smooth and large enough compared to the degree of the isogeny. The security of several recently proposed variants of SIDH [FMP23,BMP23] also reduces to leveled isogeny problems. Some of these can again be broken much more efficiently than in the unleveled case; see [FFP24] for a recent, systematic discussion.

In this paper we find explicit generalized class groups which act on the set of isomorphism classes of elliptic curves with various types of level structure. In doing so, we connect the study of isogenies between elliptic curves with level structure to the study of class group actions in the oriented framework of Colò–Kohel [CK20] and Onuki [Onu21]. Briefly recall that, for K an imaginary quadratic field, a K-orientation on an elliptic curve E over a field k, say of positive characteristic p, is an embedding $\iota : K \hookrightarrow \operatorname{End}^0(E)$ into the endomorphism algebra of E (assuming that such an embedding exists). For an order O of K, such an orientation is a primitive O-orientation if $O = \iota^{-1}\operatorname{End}(E)$. For a fixed order $O \subseteq K$, the set $\mathcal{E\ell\ell}_k(O)$

[*] This work was supported in part by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement ISOCRYPT - No. 101020788) and by CyberSecurity Research Flanders with reference number VR20192203.

of primitively O-oriented elliptic curves up to isomorphism naturally comes equipped with a free and (essentially) transitive action of the class group cl_O by isogenies, see Section 2.4 for more details. Isogenies arising from this class group action are called horizontal. For suitable parameters, this is considered a cryptographic group action, underpinning constructions like CRS [Cou06,RS06], CSIDH [CLM$^+$18,CD20] and SCALLOP [FFK$^+$23,CL23a].

Level structures have sneaked up in the oriented setting before, although the situation is more diffuse than in the non-oriented case. E.g., for N any prime different from p that splits in O, it is well-known that horizontal N-isogenies automatically preserve the two eigenspaces of any generator σ of O acting on the N-torsion [BF23,FFP24]; this can be seen as level structure amounting to the specification of two independent subgroups of order N. In [CS21], Chenu and Smith study ideal class groups acting on supersingular elliptic curves $E/\mathbb{F}_{p^2}$ together with an N-isogeny to their Frobenius conjugate; this can be viewed as Γ_N^0-level structure, see also [XZQ23]. However, our starting point is a recent observation due to Galbraith, Perrin and Voloch [GPV23] in the case of supersingular elliptic curves over $\mathbb{F}_p$, which is the setting of CSIDH: Just as $\mathrm{cl}_{\mathbb{Z}[\sqrt{-p}]}$ acts on the set of supersingular elliptic curves over $\mathbb{F}_p$ with $\mathbb{F}_p$-rational endomorphism ring $\mathbb{Z}[\sqrt{-p}]$, its ray class group for modulus (N) acts on supersingular elliptic curves over $\mathbb{F}_p$ with full Γ_N-level structure. In [GPV23], the authors observe that although using supersingular elliptic curves over $\mathbb{F}_p$ equipped with such level structure yields a larger key space for the usual CSIDH parameters, the security of such an enhanced protocol immediately reduces to that of the original CSIDH protocol, so this does not provide an advantage. We generalize this observation and contrast it with class group actions of suborders as in [FFK$^+$23].

Our goal is to analyze to what extent the observation by Galbraith et al. is part of a bigger story. Instead of starting from a type of level structure and trying to devise a corresponding class group action, we invert the viewpoint and start from the action of a *generalized class group*, subsequently finding the correct level structure in order to have a group action. In Section 2 we provide an overview of the relevant background on elliptic curves with level structure, orientations, and generalized class groups. Our main results are discussed in Section 3, where we study a large family of generalized class groups, study their properties, and show that they act freely and (essentially) transitively on oriented elliptic curves with suitable level structure. We discuss several interesting examples, one of which sheds a new light on actions by class groups of non-maximal orders. Finally, in Section 4, we discuss the hardness of the vectorization problem for our generalized class group actions.

Acknowledgments

We thank the anonymous reviewers of the International Workshop on the Arithmetic of Finite Fields 2024 for several helpful comments. When preparing the final version of this paper, we were informed that Derek Perrin has independently been working on related ideas [Per24].

2 Background

2.1 Elliptic Curves with Level Structure

In this section, fix an integer $N \geq 2$ and a field k such that $\mathrm{char}\, k \nmid N$, and let E be an elliptic curve over k. Let $E[N] \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ denote the N-torsion group of E.

Definition 1 (Level structure). *Let Γ be a subgroup of* $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$*. A Γ-level structure on an elliptic curve E is a choice of isomorphism $\Phi : \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \cong E[N]$, up to precomposition with an element of Γ. We denote this by the triple (E, Φ, Γ), just writing (E, Φ) when Γ is understood from context.*

Choosing such an isomorphism $\Phi : \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \cong E[N]$ amounts to specifying a basis $P, Q \in E[N]$ and considering it up to base change by matrices from the prescribed group $\Gamma \subseteq \mathrm{GL}_2(\mathbb{Z}/(N))$. An isogeny $\varphi : E_1 \to E_2$ respects the level structures P_1, Q_1 resp. P_2, Q_2 if and only if $\varphi(P_1) = Q_1$, $\varphi(P_2) = Q_2$, modulo the action of Γ. Commonly studied examples are

$$\Gamma_N^0 = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}, \quad \Gamma_N^{0,0} = \left\{ \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \right\}, \quad \Gamma_N^1 = \left\{ \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \right\}, \quad \Gamma_N = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

where the level structure corresponds to specifying a cyclic subgroup of order N, two independent cyclic subgroups of order N, a point of order N, or a basis of $E[N]$ (“full level structure”), respectively.

Example 1. Fix an isomorphism $\Phi : (\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}) \to E[N]$ and let $P = \Phi(1,0)$, $Q = \Phi(0,1)$. For any

$$h = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \Gamma_N^0,$$

$\Phi \circ h$ sends $(1,0) \mapsto aP$ and $(0,1) \mapsto bP + dQ$. The basis element $(0,1)$ can be sent anywhere in the group $E[N]$ via Γ_N^0, but the image of $(1,0)$ is always in $\langle P \rangle$. In this sense Φ fixes a choice of cyclic subgroup $\langle P \rangle$.

2.2 Congruence subgroups and generalized class groups

Our main references for this and the next section are [Cox13,KL22]. For O an order in an imaginary quadratic number field K, a *modulus in O* is a non-zero integral ideal $\mathfrak{m} \subseteq O$. We denote by I_O the group of proper fractional ideals in K, which we recall are lattices $\mathfrak{a} \subseteq K$ such that $\{ \alpha \in K \mid \alpha\mathfrak{a} \subseteq \mathfrak{a} \} = O$. Let P_O be the subgroup of principal fractional ideals, i.e., fractional ideals of the form αO with $\alpha \in K \setminus \{0\}$. Then the class group of O is the quotient $\mathrm{cl}_O = I_O/P_O$.

It can be shown that for any choice of modulus $\mathfrak{m}$, every class in cl_O contains an ideal $\mathfrak{a} \subseteq O$ that is coprime with $\mathfrak{m}$, i.e., $\mathfrak{a} + \mathfrak{m} = O$ [Cox13, Cor. 7.17]. Equivalently, if we define $I_O(\mathfrak{m}) \subseteq I_O$ to be the subgroup generated by all proper integral ideals that are coprime with $\mathfrak{m}$, and we let $P_O(\mathfrak{m}) = P_O \cap I_O(\mathfrak{m})$,[4] then the natural map $I_O(\mathfrak{m})/P_O(\mathfrak{m}) \to \mathrm{cl}_O : [\mathfrak{a}] \mapsto [\mathfrak{a}]$ is an isomorphism.

A *ray* for modulus $\mathfrak{m}$ is a principal fractional ideal of the form

$$\alpha O \text{ with } \alpha \in K^* \text{ such that } \alpha \equiv 1 \bmod \mathfrak{m},$$

where a congruence $\alpha \equiv \beta \bmod \mathfrak{m}$ means that for any $\alpha_1, \alpha_2, \beta_1, \beta_2 \in O$ such that $\alpha = \alpha_1/\alpha_2$ and $\beta = \beta_1/\beta_2$ we have $\alpha_1\beta_2 - \alpha_2\beta_1 \in \mathfrak{m}$; see [KL22, Def. 4.2].

The rays form a subgroup $P_{O,1}(\mathfrak{m}) \subseteq P_O(\mathfrak{m})$ called the *ray group* for modulus $\mathfrak{m}$. Any group H such that $P_{O,1}(\mathfrak{m}) \subseteq H \subseteq I_O(\mathfrak{m})$ is then called a *congruence subgroup* for modulus

[4] Equivalently, $P_O(\mathfrak{m})$ is the subgroup of P_O generated by all principal integral ideals of O that are coprime with $\mathfrak{m}$; see [KL22, §4.3], or see [Cox13, Pf. of Prop. 7.19] for the case $\mathfrak{m} = fO$ with $f \in \mathbb{Z}_{>0}$.

$\mathfrak{m}$. The corresponding quotient $I_O(\mathfrak{m})/H$ is known as a *generalized class group*; such groups play a crucial role in the study of abelian extensions of K. In the extremal case $H = P_{O,1}(\mathfrak{m})$ one ends up with the ray class group $\mathrm{cl}_{O,1}(\mathfrak{m})$. It was observed by Galbraith et al. that $\mathrm{cl}_{\mathbb{Z}[\sqrt{-p}],1}(N\mathbb{Z}[\sqrt{-p}])$ acts freely on the set of supersingular elliptic curves with $\mathbb{F}_p$-rational endomorphism ring $\mathbb{Z}[\sqrt{-p}]$ equipped with full N-level structure [GPV23, Prop. 2.5], where N denotes an integer coprime to p; we will generalize this in Section 3, but first we discuss how class groups of non-maximal orders are related to generalized class groups of their superorders.

2.3 Class groups of suborders

Let $O' \subseteq O$ be orders in K. Then $O' = \mathbb{Z} + fO$ for a unique positive integer f called the *conductor* of O' relative to O. The following result shows that $\mathrm{cl}_{O'}$ can also be viewed as a generalized class group of O:

Theorem 1. *Let*

$$P_{O,\mathbb{Z}}(fO) = \{\, \alpha O \mid \alpha \in K^* \textit{ and } \alpha \equiv g \bmod fO \textit{ for some } g \in \mathbb{Z} \textit{ coprime with } f \,\}.$$

Then the map

$$\mathrm{cl}_{O'} \to I_O(fO)/P_{O,\mathbb{Z}}(fO) : [\mathfrak{a}] \mapsto [\mathfrak{a}O],$$

where it can be assumed that $[\mathfrak{a}]$ *is represented by an integral* O'*-ideal that is coprime with* fO'*, is an isomorphism of groups.*

Proof. This is the relative version of [Cox13, Prop. 7.22], with the same proof. □

The following classical exact sequence provides a foundational framework for working with generalized class groups of orders.

Theorem 2 ([KL22, Theorem 5.4]). *Let K be an imaginary quadratic number field with ring of integers O_K and orders $O' \subseteq O \subseteq O_K$. Let f be the conductor of O' relative to O. Then, the following sequence is exact:*

$$1 \longrightarrow O^\times/(O')^\times \longrightarrow (O/fO)^\times/(O'/fO)^\times \longrightarrow \mathrm{cl}_{O'} \longrightarrow \mathrm{cl}_O \longrightarrow 1.$$

Proof. This is a generalization of the classical exact sequences with $O = O_K$ [Neu99, Theorem I.12.12]. The proof follows from [KL22, Thm. 5.4] by choosing $\mathfrak{m} = O, \mathfrak{m}' = O', \mathfrak{d} = fO'$ (notice that the roles of O and O' are reversed). □

2.4 Class group actions on sets of elliptic curves

In this section, we assume to be working in characteristic $p > 0$ and let $k \subset \overline{\mathbb{F}_p}$. We describe the class group actions on certain sets of elliptic curves over finite fields. We begin following an approach of Waterhouse [Wat69], who provides such a group action for isomorphism classes of ordinary elliptic curves over finite fields. The endomorphism ring of an ordinary elliptic curve is isomorphic to an imaginary quadratic order O. The class group of the endomorphism ring is used to define a group action on the set of isomorphism classes of curves with isomorphic endomorphism rings. We write $\mathrm{End}(E)$ to denote the ring of all endomorphisms of E/k, defined over $\overline{k} = \overline{\mathbb{F}_p}$. When it arises, we write $\mathrm{End}_k(E)$ to specify the subring of endomorphisms of E defined over k.

Theorem 3 (**[Wat69, Theorem 4.5]**)**.** *Let E be an ordinary elliptic curve over a field $k \subset \overline{\mathbb{F}_p}$ having endomorphism ring $\operatorname{End}(E) \cong O$. Then the class group of O acts freely and transitively on the set of elliptic curves over k with endomorphism ring isomorphic to O.*

The ideal class group of $\operatorname{End}(E)$ acts on the set of isomorphism classes of ordinary elliptic curves with endomorphism rings isomorphic to the order O in the following sense:

Definition 2. *Let E/k be an elliptic curve over a field $k \subset \overline{\mathbb{F}_p}$ with commutative endomorphism ring $\operatorname{End}(E)$. Take a proper integral ideal I of $\operatorname{End}(E)$ with $N(I)$ coprime to p. Define*

$$E[I] := \bigcap_{\alpha \in I} \ker \alpha.$$

As I is a finitely generated $\mathbb{Z}$-module, the set $E[I]$ is a finite group. This finite group defines an isogeny $\varphi_I : E \to E/E[I]$ with kernel $E[I]$. Define

$$I * E := E/E[I].$$

Each ideal class contains an integral ideal representative which is of norm coprime to p. The principal ideals are generated by a single endomorphism, and so act trivially. In [Wat69, §3], Waterhouse establishes that, in the case where E is ordinary, this is a free and transitive group action on the set of elliptic curves with endomorphism ring isomorphic to $\operatorname{End}(E)$. The proof goes through showing that ideals of $\operatorname{End}(E)$ satisfy certain properties qualifying them as *kernel ideals.*

In the supersingular case, the situation is more complicated. If E is supersingular, then $\operatorname{End}(E)$ is a noncommutative ring in a quaternion algebra. In particular, $\operatorname{End}(E)$ does not have a class *group* of (left or right) ideals. There is a partial remedy and a full remedy. The partial remedy: if $k = \mathbb{F}_p$, then $\operatorname{End}_k(E)$ is isomorphic to an order in the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$. In this case, one can work with the class group of $\operatorname{End}_k(E)$ and use Definition 2, just as in the ordinary case. The group action will be free and transitive (modulo a minor subtlety highlighted in the proof of [Sch87, Thm. 4.5]). However, if $k = \mathbb{F}_{p^n}$ for $n > 1$ or $k = \overline{\mathbb{F}_p}$, we find ourselves in need of additional framework: orientations on supersingular elliptic curves are the full remedy. The remainder of this section deals with the supersingular case.

Let $k \subset \overline{\mathbb{F}_p}$ and consider a supersingular elliptic curve E/k. By [Sil09], the endomorphism ring $\operatorname{End}(E)$ is isomorphic to a maximal order in the quaternion algebra $B_{p,\infty} := \operatorname{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ ramified precisely at p and ∞. Any non-scalar element $\alpha \in \operatorname{End}(E) \setminus \mathbb{Z}$ generates an imaginary quadratic order. Let K be an imaginary quadratic field in which p does not split. This condition gives the existence of an embedding of K into $B_{p,\infty}$ [Voi21, Prop. 14.6.7].

Definition 3. *A K-orientation on an elliptic curve E is an embedding*

$$\iota : K \hookrightarrow \operatorname{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

For an order O of K such an embedding is called a primitive O-orientation if $\iota(O) = \iota(K) \cap \operatorname{End}(E)$. The pair (E, ι) is called a primitively O-oriented supersingular elliptic curve. We denote by $\mathcal{E\ell\ell}_k(O)$ the set of primitively O-oriented elliptic curves over k.

Remark 1. When E is supersingular as above, a K-orientation ι maps into a four-dimensional $\mathbb{Q}$-algebra. In the case where the endomorphism ring of E is commutative, Definition 3 can still apply: the map ι defines an isomorphism $O \cong \operatorname{End}(E)$. Note that in both cases we call such a map a primitive O-orientation on E, to unify notation.

Definition 4 (K-oriented isogeny). *A K-oriented isogeny is an isogeny $\varphi : (E_0, \iota_0) \to (E_1, \iota_\varphi)$ between K-oriented elliptic curves such that $\varphi : E_0 \to E_1$ as an isogeny of elliptic curves and $\iota_\varphi(-) = \frac{1}{\deg \varphi}\varphi \circ \iota_0(-) \circ \widehat{\varphi}$.*

An isomorphism of elliptic curves is likewise a K-oriented isomorphism if it is of degree-1 and satisfies the above properties.

Via the Deuring lifting theorem, the theory of oriented supersingular elliptic curves is closely related to the theory of CM elliptic curves.

Definition 5. *There is an extension L' of the ring class field L of O and a prime $\mathfrak{p}$ above p in $O_{L'}$ such that every elliptic curve with CM by O has a representative defined over L' with good reduction at $\mathfrak{p}$. Let $\mathcal{E}\ell\ell_{L'}(O)$ denote the set of isomorphism classes of elliptic curves with endomorphism ring isomorphic to O and having good reduction over $\mathfrak{p}$. Let $\rho : \mathcal{E}\ell\ell_{L'}(O) \to \mathcal{E}\ell\ell_k(O)$ denote the reduction map modulo $\mathfrak{p}$.*

Definition 6. *Let $(E, \iota) \in \mathcal{E}\ell\ell_k(O)$ and take an ideal $\mathfrak{a}$ of O. Define the (group-theoretic) intersection:*

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

Let $\varphi_\mathfrak{a}$ denote a K-oriented isogeny of (E, ι) with kernel $E[\iota(\mathfrak{a})]$. Such an isogeny $\varphi_\mathfrak{a} : (E, \iota) \to (E_\mathfrak{a}, \iota_\mathfrak{a})$ is unique up to K-oriented automorphism on the codomain.
When $\#E[\iota(\mathfrak{a})] = N(\mathfrak{a})$, we define the action of $\mathfrak{a}$ on (E, ι) to be: $\mathfrak{a} * (E, \iota) = (E_\mathfrak{a}, \iota_\mathfrak{a})$.

Definition 6 is precisely the supersingular analogue of Definition 2 that we need. The principal ideals (β) of O are generated by endomorphisms of E, and thus act trivially on (E, ι) since $\beta \in O$ commutes with the image of ι in $\mathrm{End}(E)$. The following theorem of Onuki completes the picture by providing the supersingular analogue of Theorem 3.

Theorem 4 ([Onu21, Theorem 3.4]). *When p is not split in the imaginary quadratic field K and p is coprime to the conductor of the order O of K, then Definition 6 gives a free and transitive action of cl_O on $\rho(\mathcal{E}\ell\ell_{L'}(O))$.*

To understand when this gives a free and transitive action on the set $\mathcal{E}\ell\ell_k(O)$ of primitively O-oriented elliptic curves, we need to understand the relationship between the sets $\rho(\mathcal{E}\ell\ell_{L'}(O))$ and its superset $\mathcal{E}\ell\ell_k(O)$:

Corollary 1 ([Sch87, Theorem 4.5],[ACL+24, Theorem 4.4]). *If p is ramified in the imaginary quadratic field $O \otimes_\mathbb{Z} \mathbb{Q}$, then cl_O acts freely and transitively on the set of primitively O-oriented supersingular elliptic curves over $\overline{\mathbb{F}_p}$. If p is inert in the imaginary quadratic field $O \otimes_\mathbb{Z} \mathbb{Q}$, then cl_O has two orbits in the set of primitively O-oriented supersingular elliptic curves over $\overline{\mathbb{F}_p}$.*

Concretely, if p is not inert in the imaginary quadratic field K containing O, then cl_O acts freely and transitively on the set of isomorphism classes of primitively O-oriented elliptic curves $\mathcal{E}\ell\ell_k(O)$. If p is split in K, $\mathcal{E}\ell\ell_k(O)$ is a set of ordinary elliptic curves. If p is ramified, $\rho(\mathcal{E}\ell\ell_{L'}(O)) = \mathcal{E}\ell\ell_k(O)$ is a set of primitively O-oriented supersingular elliptic curves. If p is inert, cl_O acts on $\rho(\mathcal{E}\ell\ell_{L'}(O))$, which is again a set of primitively O-oriented supersingular elliptic curves.

3 Generalized class group actions

Let K be an imaginary quadratic number field and let O be an order in K. Let $k \subset \overline{\mathbb{F}_p}$. In this section, if p is inert in K, we fix the orbit $\rho(\mathcal{E}\ell\ell_{L'}(O))$ of cl_O and call it $\mathcal{E}\ell\ell_k(O)$ by an abuse of notation.

Let $\mathfrak{m}$ be a modulus in O. Let H be a congruence subgroup for $\mathfrak{m}$ that is contained in $P_O(\mathfrak{m})$. Let

$$\mathrm{cl}_H = I_O(\mathfrak{m})/H$$

be the corresponding generalized class group. Because $H \subseteq P_O(\mathfrak{m})$ the map

$$\mathrm{cl}_H \times \mathcal{E}\ell\ell_k(O) \to \mathcal{E}\ell\ell_k(O) : ([\mathfrak{a}], E) \mapsto \varphi_{\mathfrak{a}}(E) = E/E[\mathfrak{a}]$$

remains a well-defined group action. However, if $H \subsetneq P_O(\mathfrak{m})$ then this no longer yields a free group action: the class of any ideal $\mathfrak{a} \in P_O(\mathfrak{m}) \setminus H$ is a non-trivial element acting trivially. This creates room for an action of cl_H on elements of $\mathcal{E}\ell\ell_k(O)$ equipped with extra data, i.e., with $\mathfrak{m}$-*level structure*, which we now define.

3.1 $\mathfrak{m}$-level structures

Our starting observation is:

Lemma 1. *Let O be an imaginary quadratic order and let $E \in \mathcal{E}\ell\ell_k(O)$. Suppose $\mathfrak{m} \subseteq O$ is a proper ideal of norm coprime with p. Then*

$$E[\mathfrak{m}] \cong O/\mathfrak{m}$$

as O-modules; in particular, they are are also isomorphic as groups.

Proof. If O is a maximal order, then for $k \subseteq \mathbb{C}$ this is precisely [Sil94, Proposition II.1.4(b)], while for k finite one can use the Deuring lifting theorem to reduce to the case $k \subseteq \mathbb{C}$. To obtain the statement for arbitrary imaginary quadratic orders and over arbitrary base fields, we start by writing $\mathfrak{m} = NO + \alpha O$ with N the positive generator of $\mathfrak{m} \cap \mathbb{Z}$. We can assume that the norm of α is coprime with p. Indeed, this follows from the fact that $N(\mathfrak{m})$ equals the greatest common divisor of the norms of the elements of $\mathfrak{m}$ (because it is a proper ideal).

We rely on a result due to Lenstra [Len96, Lemma 2.1], stating that the lemma is true for principal ideals. Applying this to αO, we obtain an isomorphism

$$\phi : \frac{O}{\alpha O} \longrightarrow E[\alpha]$$

of O-modules. From this it readily follows that $O/\mathfrak{m} \cong E[\mathfrak{m}]$ as groups, because for any finite abelian group A we have $A/NA \cong A[N]$. However, our goal is to establish this isomorphism at the level of O-modules.

Proving this amounts to showing that for any δ such that $O = \mathbb{Z}[\delta]$ we can find a point $P \in E[\mathfrak{m}]$ such that

$$E[\mathfrak{m}] = \langle P, \delta(P) \rangle.$$

Indeed, this gives a well-defined map of O-modules given by

$$O/\mathfrak{m} \to E[\mathfrak{m}] : 1 \mapsto P,$$

which is clearly a surjective group homomorphism, hence bijective because we already know an isomorphism as groups.

We again use the fact that $\mathfrak{m}$ is proper, which implies that $\bar{\mathfrak{m}}\mathfrak{m} = N(\mathfrak{m})O$. We start with the curve $E_{\mathfrak{m}} := E/E[\mathfrak{m}]$. Note that $E_{\mathfrak{m}} \in \mathcal{E}\ell\ell_k(O)$ since the corresponding isogeny $\varphi_{\mathfrak{m}}$ is horizontal, so by abuse of notation we can view δ as an endomorphism of $E_{\mathfrak{m}}$. Again by Lenstra's theorem, there exists an isomorphism of O-modules

$$O/N(\mathfrak{m})O \to E_{\mathfrak{m}}[N(\mathfrak{m})].$$

Set $P \in E_{\mathfrak{m}}[N(\mathfrak{m})]$ to be the image of 1 under this isomorphism. This implies that $E_{\mathfrak{m}}[N(\mathfrak{m})] = \langle P, \delta(P)\rangle$. Then

$$E[\mathfrak{m}] = \langle \varphi_{\bar{\mathfrak{m}}}(P), \varphi_{\bar{\mathfrak{m}}}(\delta(P))\rangle = \langle \varphi_{\bar{\mathfrak{m}}}(P), \delta(\varphi_{\bar{\mathfrak{m}}}(P))\rangle,$$

where the first equality follows from the fact that $\varphi_{\bar{\mathfrak{m}}} = \widehat{\varphi_{\mathfrak{m}}}$, and the second follows from the fact that δ "commutes" with horizontal isogenies. Thus we have constructed our basis in the correct form. □

Remark 2. Lemma 1 covers all cases of interest to this paper, but it holds more generally: e.g., from the proof, it is immediate that the statement remains true if $\mathfrak{m}$ is principal and generated by a separable endomorphism, or whenever $\mathfrak{m}$ contains a separable element and $E[\mathfrak{m}]$ is cyclic. However, not all conditions can be dropped: one clearly runs into issues as soon as $\varphi_{\mathfrak{m}}$ is inseparable, while a more subtle counterexample is $O = \mathbb{Z}[\ell\sqrt{-1}]$ and $\mathfrak{m}$ the O-ideal generated by ℓ^2 and $\ell \cdot \ell\sqrt{-1}$ (where ℓ denotes any prime number different from p).

Applying Lemma 1 to $\mathfrak{m} = NO$ for some integer N coprime to $\operatorname{char} k$, we recover the well-known fact that

$$E[N] \cong O/NO \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$$

as groups, where upon writing $O = \mathbb{Z}[\sigma]$ for some generator σ, an instance of the last isomorphism is given by $1 \mapsto (1, 0)$, $\sigma \mapsto (0, 1)$. This motivates the following generalization of Definition 1.

Definition 7. *Let $\mathfrak{m} \subseteq O$ be a proper ideal coprime to* $\operatorname{char} k$*. Let $\Gamma \subseteq \mathrm{GL}(O/\mathfrak{m})$ be a subgroup and let E be an elliptic curve primitively oriented by O. A Γ-level structure on E is then a group isomorphism*

$$\Phi : O/\mathfrak{m} \to E[\mathfrak{m}]$$

defined up to pre-composition with an element $\gamma \in \Gamma$ and post-composition with a K-oriented automorphism. We denote by Y_Γ the set of primitively O-oriented elliptic curves equipped with a Γ-level structure, up to K-oriented isomorphisms. If Γ consists of O-module automorphisms, then we denote by $Z_\Gamma \subseteq Y_\Gamma$ the subset for which the level structure is an isomorphism of O-modules.

The reason for highlighting the subset Z_Γ will become apparent in Section 3.2.

Remark 3. Considering Γ-level structures up to K-oriented automorphisms amounts to identifying (E, Φ) and $(E, \iota(u) \circ \Phi)$ for every $u \in O^\times$; here ι denotes the implicit embedding of O in $\mathrm{End}(E)$. However, in most cases this can be ignored because it is already taken care of by the Γ-level structure. E.g., this is true if $O^\times = \{\pm 1\}$ and Γ is closed under negation.

More concretely, in view of the lemma below, defining a Γ-level structure amounts to specifying a point P of order $a_{\mathfrak{m}}$ and a point Q of order $b_{\mathfrak{m}}$ such that $\frac{a_{\mathfrak{m}}}{b_{\mathfrak{m}}}P, Q$ is a basis of $E[b_{\mathfrak{m}}]$, considered up to "base changes" as specified by the subgroup Γ.

Lemma 2. *Let $\mathfrak{m} \subseteq O$ be a proper ideal. Then there exist unique $a_{\mathfrak{m}}, b_{\mathfrak{m}} \in \mathbb{Z}$ such that $\operatorname{char} k \nmid b_{\mathfrak{m}} \mid a_{\mathfrak{m}}$ and*

$$E[\mathfrak{m}] \cong \frac{\mathbb{Z}}{(a_{\mathfrak{m}})} \times \frac{\mathbb{Z}}{(b_{\mathfrak{m}})}$$

for all $E \in \mathcal{E}\ell\ell_k(O)$.

Proof. This is standard: every finite subgroup of E admits such a decomposition, and the independence of E follows because any two such curves are connected by a horizontal isogeny of norm coprime with $\mathfrak{m}$. □

In order to motivate the next sections, let us conclude by restating (a slightly extended version of) the observation made by Galbraith, Perrin, and Voloch [GPV23] in the context of CSIDH. Here one considers $\mathfrak{m} = NO$ and $\Gamma = \{\mathrm{id}\}$; for simplicity we will just write Y_N, Z_N instead of $Y_{\{\mathrm{id}\}}, Z_{\{\mathrm{id}\}}$. Putting an $\{\mathrm{id}\}$-level structure on a curve $E \in \mathcal{E}\ell\ell_k(O)$ just amounts to choosing a basis $P, Q \in E[N]$, i.e., a full level-N structure. Writing $O = \mathbb{Z}[\sigma]$, elements of $Z_N \subseteq Y_N$ correspond to bases of the form $P, \sigma(P)$; it is a consequence of Lemma 1 that such bases indeed exist.

Theorem 5. *Let N be a positive integer coprime to $\operatorname{char} k$. Then the ray class group*

$$\mathrm{cl}_{O,1}(NO) = I_O(NO)/P_{O,1}(NO)$$

acts freely on both Y_N and Z_N; in the latter case, the action is also transitive.

Proof. This is a special case of Theorem 6 below. □

3.2 A family of congruence subgroups

The goal of this section (and of this paper) is to embed Theorem 5 in a more general story. We concentrate on congruence subgroups of the form

$$P_{O,\Lambda}(\mathfrak{m}) = \{\, \alpha O \mid \alpha \in K^\times \text{ and } \alpha \equiv \lambda \bmod \mathfrak{m} \text{ for some } \lambda \in \Lambda \text{ coprime to } N(\mathfrak{m}) \,\},$$

where Λ is a multiplicatively closed subset of O. This covers the aforementioned congruence subgroups $P_{O,\mathbb{Z}}(fO)$ and $P_{O,1}(\mathfrak{m}) = P_{O,\{1\}}(\mathfrak{m})$ as special cases, yet it also introduces several interesting new examples.

Remark 4. Notice that Λ and $\pm\Lambda$ or more generally $O^\times \Lambda$ define the same congruence subgroup, as one can always change the generator α of a principal ideal accordingly. Thus it would make sense to impose $O^\times \subseteq \Lambda$. However, we refrain from doing this, in order to keep covering standard notation such as $P_{O,\mathbb{Z}}(fO)$; also the exact sequence from Proposition 1 is affected by this, see Remark 6.

Now, to such a congruence subgroup $P_{O,\Lambda}(\mathfrak{m})$ we can naturally associate the subgroup

$$\Gamma_{O,\Lambda}(\mathfrak{m}) = \{\, \mu_\alpha \ \mid \alpha O \in P_{O,\Lambda}(\mathfrak{m}) \,\} = \{\, \mu_\lambda \mid \lambda \in O^\times \Lambda \,\} \subseteq \mathrm{GL}(O/\mathfrak{m})$$

where μ_α refers to the action of multiplication by α on $O/\mathfrak{m}$. By definition of $P_{O,\Lambda}(\mathfrak{m})$, this is a multiplicative subset of the finite group $\mathrm{GL}(O/\mathfrak{m})$, hence indeed a subgroup. Note that the μ_α's are O-module automorphisms, so both $Y_{\Gamma_{O,\Lambda}(\mathfrak{m})}$ and $Z_{\Gamma_{O,\Lambda}(\mathfrak{m})}$ are well-defined.

Theorem 6. *Let $\mathfrak{m} \subseteq O$ be a proper ideal, and let $H = P_{O,\Lambda}(\mathfrak{m})$ be as above. Then*

$$[\mathfrak{a}] \star (E, \Phi) = (\varphi_{\mathfrak{a}}(E), \varphi_{\mathfrak{a}} \circ \Phi) \tag{1}$$

is a well-defined free action of cl_H on $Z_{\Gamma_{O,\Lambda}(\mathfrak{m})}$. Moreover, this action is transitive. If $\Lambda \subseteq O^\times\mathbb{Z}$ then this extends to a free action of cl_H on $Y_{\Gamma_{O,\Lambda}(\mathfrak{m})}$.

Proof. Since $\deg \varphi_{\mathfrak{a}} = N(\mathfrak{a})$ is assumed coprime with $\mathfrak{m}$, it follows readily that the right-hand side of (1) is an element of $Y_{\Gamma_{O,\Lambda}(\mathfrak{m})}$. Using that $\varphi_{\mathfrak{a}}$ is K-oriented, we also see that it concerns an element of $Z_{\Gamma_{O,\Lambda}(\mathfrak{m})}$ as soon as (E, Φ) is.

Now assume $(E, \Phi) \in Z_{\Gamma_{K,\Lambda}(\mathfrak{m})}$ and let $\mathfrak{a} = \alpha O$ be the principal ideal generated by some $\alpha \in O$. Then

$$\varphi_{\mathfrak{a}} \circ \Phi = \Phi \circ \mu_\alpha \tag{2}$$

because Φ is an isomorphism of O-modules. It follows that Φ and $\varphi_{\mathfrak{a}} \circ \Phi$ define the same $\Gamma_{O,\Lambda}(\mathfrak{m})$-level structure on E if and only if $\alpha O \in P_{O,\Lambda}(\mathfrak{m})$. But this implies that the action is well-defined and free. As for the transitivity, it suffices to argue that if

$$\Phi_1, \Phi_2 : O/\mathfrak{m} \to E[\mathfrak{m}]$$

are two isomorphisms as O-modules, then there exists $\alpha \in O$ such that $\Phi_2 = \varphi_{\alpha O} \circ \Phi_1$. This is evident from the fact that we are dealing with free rank-1 modules over $O/\mathfrak{m}$.

Finally, we need to show that if $\Lambda \subseteq O^\times\mathbb{Z}$, then we still have a well-defined and free action on all of $Y_{\Gamma_{O,\Lambda}(\mathfrak{m})}$. By ignoring post-compositions with K-oriented automorphisms, we can in fact assume $\Lambda \subseteq \mathbb{Z}$. For this we need to show that

$$\varphi_{\alpha O} \circ \Phi = \Phi \circ \mu_{\alpha'}$$

for some $\alpha' O \in P_{O,\Lambda}(\mathfrak{m})$ if and only if $\alpha O \in P_{O,\Lambda}(\mathfrak{m})$. Since we are working modulo $\mathfrak{m}$, this amounts to saying that

$$\varphi_{\alpha O} \circ \Phi = \Phi \circ \mu_\lambda = [\lambda] \circ \Phi$$

for some $\lambda \in \Lambda$ if and only if $\alpha O \in P_{O,\Lambda}(\mathfrak{m})$; the last equality follows because Φ is a group homomorphism. If $\alpha O \in P_{O,\Lambda}(\mathfrak{m})$ then the existence of such a λ is clear. On the other hand, if such a λ exists then from [Sil09, Cor. III.4.11] it follows that $\alpha \equiv \lambda \bmod \mathfrak{m}$, as wanted. (Note that, in the above reasoning, we have used that we can ignore units, in view of Remark 3.) □

In general, the action of the generalized class group cl_H on $Y_{\Gamma_{O,\Lambda}(\mathfrak{m})}$ is far from transitive. E.g., recall from Theorem 5 that the ray class group acts freely on

$$Y_{\Gamma_N} = \{\, (E, P, Q) \mid E \in \mathcal{E}\ell\ell_k(O),\ P, Q \text{ basis of } E[N] \,\},$$

but when writing $O = \mathbb{Z}[\sigma]$, it is easy to see that if P happens to be an eigenvector of σ, this can never be "undone" by acting with a ray class. There are two natural ways to make the action more transitive:

- Restricting to a subset of $Y_{\Gamma_{O,\Lambda}(\mathfrak{m})}$; this is exactly what we did above when studying $Z_{\Gamma_{O,\Lambda}}$, which seems to be the most natural option.
- Further identifying elements of $Y_{\Gamma_{O,\Lambda}}$ by working with a bigger group $\Gamma \supseteq \Gamma_{O,\Lambda}$.

We now analyse the action of cl_H on a set defined by $\Gamma \supseteq \Gamma_{O,\Lambda}(\mathfrak{m})$. First, note that we are free to chose any such set, as the following lemma shows.

Lemma 3. *Assume $\Lambda \subseteq \mathbb{Z}$, let $H = P_{O,\Lambda}(\mathfrak{m})$ and consider the free action of cl_H on $Y_{\Gamma_{O,\Lambda}}$ from above. Then this descends to a well-defined action of cl_H on Y_Γ for any $\Gamma \supseteq \Gamma_{O,\Lambda}(\mathfrak{m})$.*

Proof. The set Y_Γ consists of equivalence classes of elements of $Y_{\Gamma_{O,\Lambda}}$. Thus, we only need to show that if $(E, \Phi) \sim (E, \Phi')$, i.e. $\Phi' = \Phi \circ T$ for some $T \in \Gamma$, then $(\varphi_{\mathfrak{a}}(E), \varphi_{\mathfrak{a}} \circ \Phi) \sim (\varphi_{\mathfrak{a}}(E), \varphi_{\mathfrak{a}} \circ \Phi')$ for all $[\mathfrak{a}] \in \mathrm{cl}_H$. But this is clearly true, since we still have $\varphi_{\mathfrak{a}} \circ \Phi' = \varphi_{\mathfrak{a}} \circ \Phi \circ T$. □

3.3 A generalised exact sequence

Recall that $H \subseteq P_O(\mathfrak{m})$. Thus, the class group cl_H surjects onto cl_O, and as the action of cl_O is well understood, we aim to study the action of the kernel of this surjection. To do this, we start by slightly generalising the exact sequence from Theorem 2:

Proposition 1. *Let $\mathfrak{m}, \Lambda$ and O be as above. Let $H = P_{O,\Lambda}(\mathfrak{m})$. Then Λ defines a subgroup of $(O/\mathfrak{m})^\times$, defined as $\Delta := \phi(\Lambda) \cap (O/\mathfrak{m})^\times$, where ϕ denotes the natural surjection from O to $O/\mathfrak{m}$. Then, there is an exact sequence*

$$1 \to O^\times/(O^\times \cap (\Lambda + \mathfrak{m})) \to (O/\mathfrak{m})^\times/\Delta \to \mathrm{cl}_H \to \mathrm{cl}_O \to 1$$

Proof. The proof closely follows the proof from Cox [Cox13, Theorem 7.24], which proves the special case where $\Lambda = \mathbb{Z}$, $\mathfrak{m} = (f)$ and $O = O_K$.

We prove this from the right to left. The surjection $\pi : \mathrm{cl}_H \to \mathrm{cl}_O$ is obtained from the natural map sending $[\mathfrak{a}] \in I_O(\mathfrak{m})/P_{O,\Lambda}(\mathfrak{m})$ to the class of $\mathfrak{a}$ in $I_O(\mathfrak{m})/P_O(\mathfrak{m}) \cong \mathrm{cl}_O$. The kernel is therefore exactly $P_O(\mathfrak{m})/P_{O,\Lambda}(\mathfrak{m})$. Next, we show that there is a surjection

$$(O/\mathfrak{m})^\times/\Delta \to P_O(\mathfrak{m})/P_{O,\Lambda}(\mathfrak{m})$$

obtained by sending $[[\alpha]] \in (O/\mathfrak{m})^\times/\Delta$ to αO (we will use the notation $[\gamma]$ for elements of $(O/\mathfrak{m})^\times$, and $[[\gamma]]$ for elements of $(O/\mathfrak{m})^\times/\Delta$). The ideal αO is clearly in $P_O(\mathfrak{m})$. Further, let $[\alpha] = [\beta][\delta]$, for some $\delta \in \Lambda$, i.e. α and β are in the same class of $(O/\mathfrak{m})^\times/\Delta$. Then, unraveling the definitions, there exists some $u \in O$ such that $u\alpha \equiv u\beta\delta \equiv 1 \pmod{\mathfrak{m}}$. Further, we can choose some $\delta' \in \Lambda$ such that $[\delta'] \equiv [\delta]^{-1}$. Thus, we have that

$$\alpha O \cdot u\beta\delta O = \beta O \cdot u\alpha\delta^{-1} O,$$

which shows that the map is a well defined group homomorphism, since $u\beta\delta O \in P_{O,1}(\mathfrak{m}) \subseteq P_{O,\Lambda}(\mathfrak{m})$, and $u\alpha\delta^{-1} O \in P_{O,\Lambda}(\mathfrak{m})$.

Next, we show that the map is surjective. Let $\gamma O \in P_O(\mathfrak{m})$. Obviously, if $\gamma \in O$, then $[[\gamma]]$ maps to γO. In general, γ can be written as $\gamma_1 \gamma_2^{-1}$ for $\gamma_1, \gamma_2 \in O$, which both are coprime to $\mathfrak{m}$. Let N be the norm of γ_2. Since N is coprime to $\mathfrak{m}$, there exists a $k \in \mathbb{Z}$ such that $kN \equiv 1$ mod $\mathfrak{m}$. Since $N\gamma_2^{-1} = \overline{\gamma_2}$, we have that the class $[[\gamma_1][k\overline{\gamma_2}]]$ maps to $k\gamma_1\overline{\gamma_2}O = \gamma O \cdot kNO$, and since $kN \equiv 1 \mod \mathfrak{m}$, we have $kNO \in P_{O,1}(\mathfrak{m}) \subseteq P_{O,\Lambda}(\mathfrak{m})$, proving that the map is surjective.

Finally, assume $[[\alpha]] \in (O/\mathfrak{m})^\times/\Delta$ satisfies $\alpha O \in P_{O,\Lambda}(\mathfrak{m})$. Thus, we have that $\alpha O = \beta\gamma^{-1}O$, for some β, γ satisfying $[\beta'][\gamma]^{-1} \in \Delta$, and that $\alpha = \mu\beta\gamma^{-1}$ for some $\mu \in O^\times$. This in turn means that $[\alpha] = [\mu][\beta][\gamma]^{-1}$, and since $[\beta][\gamma]^{-1} \in \Delta$, we see that $[[\alpha]] = [[\mu]]$, i.e. $[[\alpha]]$ is in the image of the natural homomorphism $O^\times \to (O/\mathfrak{m})^\times/\Delta$, whose kernel is in turn exactly $O^\times \cap (\Lambda + \mathfrak{m})$. □

Remark 5. We can compare Proposition 1 with both the classical $O = O_K$ version of Theorem 2 and the formula for computing the size of the ray class group from [Coh12, Theorem 3.2.4]: Specialising to $\Lambda = \mathbb{Z}$ and $\mathfrak{m} = (f)$, and writing $O := \mathbb{Z} + fO_K$, we immidiately see that

$$O_K^\times \cap (\Lambda + \mathfrak{m}) = O_K^\times \cap (\mathbb{Z} + fO_K) = O^\times,$$

and similarily, $\Delta = \phi(\mathbb{Z}) \cap (O_K/fO_K)^\times = (\mathbb{Z} + fO_K/fO_K)^\times = (O/fO_K)^\times$, recovering the exact sequence from Theorem 2.

The size of the ray class group can be computed from the exact sequence when $\Lambda = \{1\}$, in which case one finds that $\Delta = \{[1]\}$, and thus

$$\#\,\mathrm{cl}_H = h(O_K)\frac{\#(O_K/\mathfrak{m})^\times}{\frac{O_K^\times}{O_K^\times \cap (1+\mathfrak{m})}} = h(O_K)\frac{\#(O_K/\mathfrak{m})^\times}{[O_K^\times : O_{K,\mathfrak{m}}^\times]}$$

where $O_{K,\mathfrak{m}}^\times$ is the group of units congruent to $1 \bmod \mathfrak{m}$. This same remark applies in the relative case, $O' \subseteq O \subseteq O_K$.

Remark 6. Recall from Remark 4 that switching from Λ to $O^\times\Lambda$ does not affect the congruence subgroup $P_{O,\Lambda}(\mathfrak{m})$, and therefore it does not change the generalized class group either. Also, it does not affect the subgroup $\Gamma_{O,\Lambda}(\mathfrak{m})$. However, it is interesting to observe that it can slightly reorganize the terms in the exact sequence from Proposition 1. Indeed, switching from Λ to $O^\times\Lambda$ has the effect of folding the exact sequence, which is of the form

$$1 \to G_1 \to G_2 \xrightarrow{f} G_3 \to G_4 \to 1, \qquad \text{into} \qquad 1 \to \frac{G_2}{\ker f} \to G_3 \to G_4 \to 1.$$

Since we know that cl_O acts freely on the set of primitively O-oriented curves, we use the surjection $\pi : \mathrm{cl}_H \to \mathrm{cl}_O$ from the exact sequence above, and study the action of $\ker\pi$. By Proposition 1, The elements of $\ker\pi$ are principal ideals, which can be identified by elements of $O/\mathfrak{m}$ up to multiplication by Δ and $O^\times$. In particular, they are endomorphisms, leaving the curve fixed, and acting on the different Γ-level structures, which in turn can be identified (by definition) with left cosets of $\Gamma \subset \mathrm{GL}(O/\mathfrak{m})$, up to K-oriented isomorphisms. This action is fairly easy to describe explicitly, as the following lemma shows.

Corollary 2. *Let $O, \mathfrak{m}, \Lambda \subseteq \mathbb{Z}$ and the map π be as before. Let $\Gamma \supseteq \Gamma_{O,\Lambda}(\mathfrak{m})$. Then,* $\ker\pi$ *acts on the set*

$$X_\Gamma := \{M\Gamma \mid M \in \mathrm{GL}(O/\mathfrak{m})\}/\sim$$

where $\sim$ is the equivalence relation obtained by identifying cosets up to left multiplication by μ_u for $u \in O^\times$.

Proof. As we have seen, $\ker \pi$ can be identified with elements $[\alpha] \in (O/\mathfrak{m})^\times$, up to multiplication by Λ and $O^\times$. We show that the natural action of sending the left coset $M\Gamma$ to $\mu_\alpha M\Gamma$ is well defined. This is clearly a well defined action by $(O/\mathfrak{m})^\times$, so it suffices to show that multiplication by elements of Λ and $O^\times$ act trivially. Since $\lambda \in \Lambda \subseteq \mathbb{Z}$, it is clear that

$$\mu_\lambda M\Gamma = M\mu_\lambda\Gamma = M\Gamma,$$

and further, for $u \in O^\times$, μ_u acts trivially by definition of X_Γ. □

3.4 Suborder class group actions

As one of our main examples, let us concentrate on the case where $\Lambda = \mathbb{Z}$ and $\mathfrak{m} = fO$ for some prime number f different from $\operatorname{char} k$. Pick $\sigma \in O$ such that $O = \mathbb{Z}[\sigma]$. Write $H = P_{O,\mathbb{Z}}(fO)$ and observe that $\Gamma := \Gamma_{O,\mathbb{Z}}(fO) \subseteq \mathrm{GL}(O/fO)$ is just the group of multiplications μ_λ by an integer λ that is not divisible by f. Thus we have

$$Y_\Gamma = \{\,(E, P, Q) \mid E \in \mathcal{E}\ell\ell_k(O),\ P, Q \text{ basis of } E[f]\}/\sim$$

where $(E, P, Q) \sim (E, \lambda P, \lambda Q)$ for any scalar $\lambda \in (\mathbb{Z}/f\mathbb{Z})^\times$. The action of cl_H on Y_Γ is not transitive. Recall that there are two approaches towards turning this into a "more transitive" action:

- Instead of Y_Γ, we can act on Z_Γ, i.e., we can require that the isomorphism

  $$\Phi : O/fO \to E[f]$$

  is an isomorphism of O-modules. This amounts to picking a basis of $E[f]$ of the form $P, \sigma(P)$. Note that it suffices to specify P in this case, and because of the scaling we are in fact specifying a cyclic subgroup $C \subseteq E$ of order f. However, since $P, \sigma(P)$ must be a basis, the subgroups we thus obtain are those that are *not* eigenspaces of σ acting on $E[f]$. In other words, we can identify

  $$Z_\Gamma = \{\,(E, C) \mid E \in \mathcal{E}\ell\ell_k(O),\ C \subseteq E \text{ kernel of descending } f\text{-isogeny}\}. \tag{3}$$

  Thanks to Theorem 6 we know that cl_H acts freely and transitively on this set.
- Alternatively, we can apply the idea of making the action of cl_H on Y_Γ more transitive by enlarging Γ. In this case it is natural to consider

  $$\Gamma_N^0 = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \supseteq \Gamma,$$

  where the last inclusion makes sense upon identification of $\mathrm{GL}(O/fO)$ with $(\mathbb{Z}/f\mathbb{Z})^2$. Thus by Lemma 3 we also have a natural action of cl_H on

  $$Y_N^0 = Y_{\Gamma_N^0} = \{\,(E, C) \mid E \in \mathcal{E}\ell\ell_k(O),\ C \subseteq E \text{ cyclic subgroup of order } f\,\}.$$

  However, unless f is inert, this action is neither free nor transitive: any eigenspace of σ acting on $E[f]$ is fixed by every element of cl_H. To turn this into a free and transitive action one has to discard the eigenspaces; as such one again arrives at Z_Γ.

Now let $O' = \mathbb{Z} + fO$ be a suborder of relative conductor f and recall from Theorem 1 that the natural map

$$\mathrm{cl}_{O'} \to \mathrm{cl}_H : [\mathfrak{a}] \mapsto [\mathfrak{a}O] \tag{4}$$

is an isomorphism. In fact, more generally, it is easy to check that the exact sequence from Proposition 1 fits in an isomorphism of exact sequences

$$\begin{tikzcd}
1 \arrow[r] & \frac{O^\times}{O'^\times} \arrow[r] \arrow[d] & \frac{(O/fO)^\times}{(O'/fO)^\times} \arrow[r] \arrow[d] & \mathrm{cl}_{O'} \arrow[r] \arrow[d] & \mathrm{cl}_O \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \frac{O^\times}{O^\times \cap (\mathit{\Lambda} + fO)} \arrow[r] & \frac{(O/fO)^\times}{\mathit{\Delta}} \arrow[r] & \mathrm{cl}_H \arrow[r] & \mathrm{cl}_O \arrow[r] & 1
\end{tikzcd}$$

where the vertical maps are the natural maps, and where the sequence on top is the exact sequence from Theorem 2.

Now recall from Section 2.4 that we have a free and transitive action of $\mathrm{cl}_{O'}$ on $\mathcal{E}\ell\ell_k(O')$. On the other hand, as we have just discussed, there is also a free and transitive action of cl_H on Z_Γ. Finally, we have the isomorphism (4) connecting $\mathrm{cl}_{O'}$ to cl_H, as well as a natural bijection

$$Z_\Gamma \to \mathcal{E}\ell\ell_k(O') : (E, C) \mapsto \pi(E, C) := E/C.$$

It can be argued that all these maps are compatible with each other:

Lemma 4. *For every ideal class $[\mathfrak{a}] \in \mathrm{cl}_{O'}$ we have*

$$[\mathfrak{a}] \star \pi(E, C) = \pi([\mathfrak{a}O] \star (E, C)),$$

where the left action is that of $\mathrm{cl}_{O'}$ on $\mathcal{E}\ell\ell_k(O')$, while the right action is that of cl_H on Z_Γ.

Proof. Write $E_1 = \pi(E, C)$ and let $E_1' = \varphi_\mathfrak{a}(E_1)$. Then $E \in \mathcal{E}\ell\ell_k(O)$ lies above E_1 via an ascending isogeny φ with kernel $E_1[f, f\sigma]$. Likewise, there is an elliptic curve $E' \in \mathcal{E}\ell\ell_k(O)$ above E_1', which is the codomain of an ascending isogeny φ' with kernel $E_1'[f, f\sigma]$. It is easy to check that we obtain a commuting diagram

$$\begin{tikzcd}
E \arrow[r, "\varphi_{\mathfrak{a}O}"] & E' \\
E_1 \arrow[u, "\varphi"] \arrow[r, "\varphi_\mathfrak{a}"] & E_1' \arrow[u, "\varphi'"']
\end{tikzcd}$$

showing that $[\mathfrak{a}O] \star E = E'$, an equality which refers to the action of cl_O on $\mathcal{E}\ell\ell_k(O)$; see also the proof of [Sut13, Lem. 6]. It is then immediate that $C = \ker \hat{\varphi}$ is mapped via $\varphi_{\mathfrak{a}O}$ to $C' := \ker \hat{\varphi}'$, from which the statement follows. □

Remark 7. From the commutativity of the above diagram it follows that

$$\hat{\varphi}' \circ \varphi_{\mathfrak{a}O} \circ \varphi = \hat{\varphi}' \circ \varphi' \circ \varphi_\mathfrak{a} = [f] \circ \varphi_\mathfrak{a},$$

showing that this is the horizontal isogeny corresponding to the ideal $f\mathfrak{a}$. Since the natural map $\mathrm{cl}_{O'} \to \mathrm{cl}_O$ is not injective, one can also wonder what ideal we end up with when first choosing an isogeny $\psi : E \to E'$ and considering the horizontal isogeny $\hat{\varphi}' \circ \psi \circ \varphi$. One particular case is where $E = E'$, as in the case of SCALLOP. In this case the ideals corresponding to $\hat{\varphi}' \circ \varphi$ have a particularly nice interpretation: they correspond to O'-ideals of norm f^2, of the form $\mathfrak{a}_{\alpha,\beta} = (f^2, f(\alpha+\beta\sigma))$, for some $\alpha+\beta\sigma \in O$ such that $N_{K/\mathbb{Q}}(\alpha+\beta\sigma) \not\equiv 0 \bmod f$. Indeed, there is in this case a free and transitive action of $\ker(\mathrm{cl}_{O'} \to \mathrm{cl}_O)$ on the set of all $E/C \in \mathcal{E}\ell\ell_k(O')$ over cyclic f-subgroups C that are not eigenspaces of σ acting on $E[f]$, which corresponds to the free and transitive action of $\mathrm{cl}_{O'}$ on Z_Γ as in Theorem 6. It can be proven that ideal classes $[\mathfrak{a}_{\alpha,\beta}]$ in $\mathrm{cl}_{O'}$ are in bijection with $(\alpha : \beta) \in \mathbb{P}^1(\mathbb{F}_f)$ such that $N_{K/\mathbb{Q}}(\alpha+\beta\sigma) \not\equiv 0 \bmod f$, and that they constitute all of $\ker(\mathrm{cl}_{O'} \to \mathrm{cl}_O)$ (see also [BLS12, Lemma 3.2]). Once we fix a subgroup $C = \ker\hat{\varphi}$, the action of such classes is explicitly given by: $[\mathfrak{a}_{\alpha,\beta}] \star \pi(E,C) = \pi(E,(\alpha+\beta\iota(\bar\sigma))(C))]$, where $\bar\sigma$ is the complex conjugate of σ. This follows from Lemma 4 and the fact that $[\mathfrak{a}_{\alpha,\beta}] = [(N_{K/\mathbb{Q}}(\alpha+\beta\sigma), f(\alpha+\beta\bar\sigma))]$, hence $[\mathfrak{a}_{\alpha,\beta}O] = [(\alpha+\beta\bar\sigma)]$.

3.5 Further examples

Cyclic torsion. Assume that $O/\mathfrak{m}$ is cyclic, i.e., $b_\mathfrak{m} = 1$ in Lemma 2. Then we can observe

- that every $\alpha \in O$ is congruent to an integer mod $\mathfrak{m}$; in particular it can be assumed without loss of generality that $\Lambda \subseteq \mathbb{Z}$,
- every group isomorphism $\Phi : O/\mathfrak{m} \to E[\mathfrak{m}]$ is necessarily an isomorphism of O-modules, i.e., $Y_\Gamma = Z_\Gamma$ for any $\Gamma \subseteq \mathrm{GL}(O/\mathfrak{m})$.

As a more concrete example, take $\Lambda = \{1\}$ and let f be a prime number such that $fO = \mathfrak{m}\cdot\overline{\mathfrak{m}}$ for some prime ideal $\mathfrak{m} \subseteq O$. By Theorem 6 the ray class group $I_O(\mathfrak{m})/P_{O,1}(\mathfrak{m})$ acts freely and transitively on the set $Z_{\Gamma_{O,1}(\mathfrak{m})}$ of O-oriented elliptic curves E/k equipped with an eigenvector of σ acting on $E[f]$. For instance, if $K = \mathbb{Q}(\sqrt{-p})$, f is odd and $p \equiv 1 \bmod f$ as in CSIDH, then we can take $\mathfrak{m} = (f, \sqrt{-p}-1)$ and this consists of supersingular elliptic curves over $\mathbb{F}_p$ with a distinguished $\mathbb{F}_p$-rational point of order f (up to negation).

Scaling by n-th powers. Let O be an order and $\mathfrak{m} = (f)$ an ideal such that $f \equiv 1 \pmod 4$ is prime in O. Let $\Lambda = \mathbb{Z}^2 := \{\alpha^2 \mid \alpha \in \mathbb{Z}\}$, and assume further that $O^\times = \{\pm 1\}$, such that $O^\times \subset \Lambda + f\mathbb{Z}$ (here we use $f \equiv 1 \pmod 4$). Observe that $H := P_{O,\Lambda}(\mathfrak{m})$ is thus the set of principal ideals generated by elements that are equivalent to integers that are squares mod $\mathfrak{m}$, and then it follows from 1, that $\#\,\mathrm{cl}_H = 2(f+1)h(O)$. As in the situation in Subsection 2.4, we get the set $Z_{\Gamma_{O,\Lambda}(\mathfrak{m})}$ consists of elements of the form $(E, P, \sigma(P))$, where $P \in E[f]$, and where we identify $(E,P,\sigma(P)) \sim (E,Q,\sigma(Q))$ if and only if $P = [\lambda]Q$ for some $\lambda \in \mathbb{Z}$ that is a square $\bmod f$. Thus, the situation here is a fine-grained version the action of $\mathrm{cl}_{\mathbb{Z}+fO}$ on $(E, \langle P\rangle)$ from Subsection 2.4: The slightly larger class group acts on the set that can be recognized as curves, together with one of two points of order f for each subgroup of order f, and where the two points differ by multiplication by a non-square.

This example easily generalizes to $\Lambda = \mathbb{Z}^n$ for any $n \mid f-1$, such that $O^\times \subset \Lambda + f\mathbb{Z}$.

The full class group. If $\Lambda = O$, then $P_{O,\Lambda}(\mathfrak{m}) = P_O(\mathfrak{m})$ is the group of all fractional principal ideals coprime to $\mathfrak{m}$, and we end up with the standard action of cl_O on $\mathcal{E}\ell\ell_k(O)$, which indeed naturally coincides with Z_Γ where $\Gamma = \Gamma_{K,O_K}(\mathfrak{m})$. Note that in general we do not have a well-defined action of cl_O on the larger set Y_Γ; indeed the condition $\Lambda \subseteq O^\times\mathbb{Z}$ from Theorem 6 is violated. Nevertheless it makes sense to study Y_Γ as a set; e.g., when $\mathfrak{m} = NO$ then it parametrizes O-oriented elliptic curves E together with a basis of $E[N]$, where two bases are identified if and only if they can be transformed into one another via an endomorphism in $\iota(O)$.

4 Security reductions and non-reductions

Although we do not have cryptographic applications in mind, it is natural to extend the central question of [GPV23] to our generalized setting: given

$$(E_1, \Phi_1),\ (E_2, \Phi_2)\ \in\ Z_{\Gamma_{O,\Lambda}(\mathfrak{m})},$$

how hard is it to find a generalized ideal class $[\mathfrak{a}] \in I_O(\mathfrak{m})/P_{O,\Lambda}(\mathfrak{m})$ such that $[\mathfrak{a}](E_1, \Phi_1) = (E_2, \Phi_2)$? This problem is known as the vectorization problem [Cou06], which quantum computers can solve in sub-exponential time $L_h(1/2)$, with h denoting the size of the generalized class group.

Unsurprisingly, the main conclusion from [GPV23, Alg. 2] also applies here: despite the generalized ideal class group being larger, there is an immediate reduction to the vectorization problem for cl_O, potentially at the cost of a discrete logarithm computation (which may be hard classically, but succumbs to Shor's algorithm quantumly). Indeed, after finding an ideal $\mathfrak{a} \in I_O(\mathfrak{m})$ such that $\varphi_{\mathfrak{a}} : E_1 \to E_2$, one can find $\alpha \in O$ such that $\alpha\mathfrak{a}$ moreover maps Φ_1 to Φ_2, via the computation of Weil pairings and discrete logarithms.

Remark 8. It is worth contrasting this with actions by class groups of suborders $O' \subseteq O$. From Section 3.4 we know that the action of $\mathrm{cl}_{O'}$ on $\mathcal{E}\ell\ell_k(O')$ is a generalized class group action in disguise. However, it would be wrong to apply the previous discussion and conclude that the corresponding vectorization problem reduces to that of cl_O acting on $\mathcal{E}\ell\ell_k(O)$ at the cost of discrete logarithm computations. There is again a reduction, but it proceeds by walking to $\mathcal{E}\ell\ell_k(O)$ via isogenies; in other words, the "disguise" is crucial for security. An extreme case is SCALLOP [FFK$^+$23,CL23a], where cl_O is the trivial group, but here the isogenies are of very large prime degree, hence infeasible to compute.

Cases where vectorization becomes easier In view of the attacks on SIDH, the extra level structure may in fact make the vectorization problem much easier. E.g., in the case of the ray class group for scalar modulus $\mathfrak{m} = NO$, an attacker has access to a basis P_1, Q_1 of $E_1[N]$ along with their images under the secret isogeny $\varphi_{\mathfrak{a}} : E_1 \to E_2$. Assuming we are given a bound on $\deg \varphi_{\mathfrak{a}} = N(\mathfrak{a})$ and assuming that N is large enough and smooth, we can recover $\deg \varphi_{\mathfrak{a}}$ and run the algorithm from [Rob23b] to solve the vectorization problem in classical polynomial time. Another interesting case is the generalized class group action from Section 3.4, where we have a free and transitive action on oriented elliptic curves together with the kernel of a descending f-isogeny, see (3). Thus, here one is given access to such a kernel $C_1 \subseteq E_1[f]$ along with its image $C_2 \subseteq E_2[f]$. But then one also knows that $\sigma(C_1)$ is connected to $\sigma(C_2)$ via the same unknown scalar: the vectorization problem becomes an instance of the M-SIDH problem [FMP23], which can again be broken in overstretched cases. Moreover, if f splits then we also know that the action preserves the eigenspaces of σ acting on the f-torsion; as such we have access to *four* subgroups together with their images, and we can reduce to the case of SIDH via [FP22, Lem. 1].

Supergroups of $P_O(\mathfrak{m})$ Finally, let us drop the overall assumption made at the beginning of Section 3, namely that $H \subseteq P_O(\mathfrak{m})$: what if, conversely, our congruence subgroup H is a supergroup of $P_O(\mathfrak{m})$? In this case the generalized class group $\mathrm{cl}_H = I_O(\mathfrak{m})/H$ naturally acts on subsets $\{\, [\mathfrak{h}]E \mid \mathfrak{h} \in H \,\} \subseteq \mathcal{E}\ell\ell_k(O)$ of oriented elliptic curves that can be connected via an ideal in H. In theory, this gives a reduction from the vectorization problem for cl_O to that of the smaller group cl_H: first find the class connecting $\{ [\mathfrak{h}]E_1 \mid \mathfrak{h} \in H \}$ and $\{ [\mathfrak{h}]E_2 \mid \mathfrak{h} \in H \}$ and then solve a vectorization problem for $H/P_O(\mathfrak{m})$. If this were possible, then this could be converted into a Pohlig–Hellman type reduction for class group actions. But unfortunately (or fortunately), it is unclear how to work with the sets $\{ [\mathfrak{h}]E \mid \mathfrak{h} \in H \}$; e.g., when merely working with a representant, one lacks tools for equality testing (which amounts to deciding whether or not two O-oriented elliptic curves E_1, E_2 are connected via an ideal in H).

References

ACL$^+$24. Sarah Arpin, Mingjie Chen, Kristin E. Lauter, Renate Scheidler, Katherine E. Stange, and Ha T.N. Tran. Orientations and cycles in supersingular isogeny graphs. In *Research Directions in Number Theory: Women in Numbers V*, pages 25–86. Springer International Publishing Cham, 2024.

Arp22. Sarah Arpin. *Supersingular Elliptic Curve Isogeny Graphs.* PhD thesis, University of Colorado Boulder, 2022.

BCC$^+$23. Andrea Basso, Giulio Codogni, Deirdre Connolly, Luca De Feo, Tako Boris Fouotsa, Guido Maria Lido, Travis Morrison, Lorenz Panny, Sikhar Patranabis, and Benjamin Wesolowski. Supersingular curves you can trust. In *EUROCRYPT (2)*, volume 14005 of *Lecture Notes in Computer Science*, pages 405–437. Springer, 2023.

BF23. Andrea Basso and Tako Boris Fouotsa. New SIDH countermeasures for a more efficient key exchange. In *ASIACRYPT (8)*, volume 14445 of *Lecture Notes in Computer Science*, pages 208–233. Springer, 2023.

BLS12. Reinier Bröker, Kristin Lauter, and Andrew V. Sutherland. Modular polynomials via isogeny volcanoes. *Mathematics of Computation*, 81(278):1201–1231, 2012.

BMP23. Andrea Basso, Luciano Maino, and Giacomo Pope. FESTA: fast encryption from supersingular torsion attacks. In *Advances in cryptology—ASIACRYPT 2023. Part VII*, volume 14444 of *Lecture Notes in Comput. Sci.*, pages 98–126. Springer, Singapore, [2023] ©2023.

CD20. Wouter Castryck and Thomas Decru. CSIDH on the surface. In *PQCrypto*, volume 12100 of *Lecture Notes in Computer Science*, pages 111–129. Springer, 2020.

CK20. Leonardo Colò and David Kohel. Orienting supersingular isogeny graphs. *J. Math. Cryptol.*, 14(1):414–437, 2020.

CL23a. Mingjie Chen and Antonin Leroux. SCALLOP-HD: group action from 2-dimensional isogenies. *IACR Cryptol. ePrint Arch.*, page 1488, 2023.

CL23b. Giulio Codogni and Guido Lido. Spectral theory of isogeny graphs, 2023.

CLM$^+$18. Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: an efficient post-quantum commutative group action. In *Advances in cryptology—ASIACRYPT 2018. Part III*, volume 11274 of *Lecture Notes in Comput. Sci.*, pages 395–427. Springer, Cham, 2018.

Coh12. Henri Cohen. *Advanced topics in computational number theory*, volume 193. Springer Science & Business Media, 2012.

Cou06. Jean Marc Couveignes. Hard homogeneous spaces. *IACR Cryptol. ePrint Arch.*, page 291, 2006.

Cox13. David A. Cox. *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication.* Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. Wiley, 2013.

CS21. Mathilde Chenu and Benjamin Smith. Higher-degree supersingular group actions. *Math. Cryptology*, 1(1):1–15, 2021.

FFK$^+$23. Luca De Feo, Tako Boris Fouotsa, Péter Kutas, Antonin Leroux, Simon-Philipp Merz, Lorenz Panny, and Benjamin Wesolowski. SCALLOP: scaling the CSI-FiSh. In *Public-Key Cryptography - PKC 2023 Part I*, volume 13940 of *Lecture Notes in Computer Science*, pages 345–375. Springer, 2023.

FFP24. Luca De Feo, Tako Boris Fouotsa, and Lorenz Panny. Isogeny problems with level structure. In *EUROCRYPT 2024 (to appear)*. Springer-Verlag, 2024.

FMP23. Tako Boris Fouotsa, Tomoki Moriya, and Christophe Petit. M-SIDH and MDSIDH: countering SIDH attacks by masking information. In *EUROCRYPT (5)*, volume 14008 of *Lecture Notes in Computer Science*, pages 282–309. Springer, 2023.

FP22. Tako Boris Fouotsa and Christophe Petit. A new adaptive attack on SIDH. In *Topics on Cryptology – CT-RSA*, volume 13161 of *Lecture Notes in Computer Science*, pages 322–344. Springer, 2022.

GPV23. Steven D. Galbraith, Derek Perrin, and José Felipe Voloch. CSIDH with level structure. *IACR Cryptol. ePrint Arch.*, page 1726, 2023.

KL22. Gene S. Kopp and Jeffrey C. Lagarias. Class field theory for orders of number fields, 2022.

Len96. Hendrik W. Lenstra. Complex multiplication structure of elliptic curves. *Journal of Number Theory*, 56(2):227–241, 1996.

Neu99. Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

Onu21. Hiroshi Onuki. On oriented supersingular elliptic curves. *Finite Fields Their Appl.*, 69:101777, 2021.

Per24. Derek Perrin. Ordinary isogeny graphs with level structure. Article in preparation, 2024.

Rob23a. Damien Robert. Breaking SIDH in polynomial time. In *EUROCRYPT (5)*, volume 14008 of *Lecture Notes in Computer Science*, pages 472–503. Springer, 2023.

Rob23b. Damien Robert. Breaking SIDH in polynomial time. In Carmit Hazay and Martijn Stam, editors, *Advances in Cryptology - EUROCRYPT 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part V*, volume 14008 of *Lecture Notes in Computer Science*, pages 472–503. Springer, 2023.

RS06. Alexander Rostovtsev and Anton Stolbunov. Public-key cryptosystem based on isogenies. Cryptology ePrint Archive, Paper 2006/145, 2006. https://eprint.iacr.org/2006/145.

Sch87. René Schoof. Nonsingular plane cubic curves over finite fields. *J. Combin. Theory Ser. A*, 46(2):183–211, 1987.

Sil94. Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151. Springer, 1994.

Sil09. Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, second edition, 2009.

Sut13. Andrew V. Sutherland. Isogeny volcanoes. In *ANTS-X*, volume 1 of *Open Book Series*, pages 507–530. MSP, 2013.

Voi21. John Voight. *Quaternion algebras*, volume 288 of *Graduate Texts in Mathematics*. Springer, Cham, [2021] ©2021.

Wat69. William C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. Ecole Norm. Sup.*, 2:521–560, 1969.

XZQ23. Guanju Xiao, Zijian Zhou, and Longjiang Qu. Oriented supersingular elliptic curves and Eichler orders, 2023.