Entanglement in the family of division fields of elliptic curves with complex multiplication

Campagna, Francesco; Pengo, Riccardo

Publication date:
2020

ENTANGLEMENT IN THE FAMILY OF DIVISION FIELDS OF ELLIPTIC CURVES WITH COMPLEX MULTIPLICATION

FRANCESCO CAMPAGNA AND RICCARDO PENGO

Abstract. For every CM elliptic curve E defined over a number field F containing the CM field K, we prove that the family of p^∞-division fields of E, with $p \in \mathbb{N}$ prime, becomes linearly disjoint over F after removing an explicit finite subfamily of fields. If $F = K$ and E is obtained as the base-change of an elliptic curve defined over $\mathbb{Q}$, we prove that this finite subfamily is never linearly disjoint over K as soon as it contains more than one element.

1. Introduction

Let E be an elliptic curve defined over a number field F, and let $\overline{F} \supseteq F$ be a fixed algebraic closure. The absolute Galois group $\mathrm{Gal}(\overline{F}/F)$ acts on the group $E_{\mathrm{tors}} := E(\overline{F})_{\mathrm{tors}}$ of all torsion points of E, giving rise to a Galois representation

$$\rho_E : \mathrm{Gal}(F(E_{\mathrm{tors}})/F) \hookrightarrow \mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}}) \cong \mathrm{GL}_2(\widehat{\mathbb{Z}})$$

where $F(E_{\mathrm{tors}})$ is the compositum of the family of fields $\{F(E[p^\infty])\}_p$ for $p \in \mathbb{N}$ prime. Each extension $F \subseteq F(E[p^\infty])$ is in turn defined as the compositum of the family $\{F(E[p^n])\}_{n \in \mathbb{N}}$, where, for every $N \in \mathbb{N}$, we denote by $F(E[N])$ the *division field* obtained by adjoining to F the coordinates of all the points belonging to the N-torsion subgroup $E[N] := E[N](\overline{F})$.

For an elliptic curve E without complex multiplication (CM), Serre's Open Image Theorem [25, Théorème 3] asserts that the image of ρ_E has finite index in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. However, explicitly describing this image is a non-trivial problem in general which is connected to the celebrated Uniformity Conjecture [25, § 4.3]. A first step in this direction is to study the *entanglement* of the family $\{F(E[p^\infty])\}_p$ for p prime, *i.e.* to describe the image of the natural inclusion

$$\mathrm{Gal}(F(E_{\mathrm{tors}})/F) \hookrightarrow \prod_p \mathrm{Gal}(F(E[p^\infty])/F) \tag{1}$$

where the product runs over all primes $p \in \mathbb{N}$. For each non-CM elliptic curve $E_{/F}$ this has been done in [7] by Stevenhagen and the first named author. They identify a finite set S of "bad primes" (depending on E and F) such that the map (1) induces an isomorphism

$$\mathrm{Gal}(F(E_{\mathrm{tors}})/F) \xrightarrow{\sim} \mathrm{Gal}(F(E[S^\infty])/F) \times \prod_{p \notin S} \mathrm{Gal}(F(E[p^\infty])/F)$$

where $F(E[S^\infty])$ denotes the compositum of the family of fields $\{F(E[p^\infty])\}_{p \in S}$. In this case one says that the family $\{F(E[S^\infty])\} \cup \{F(E[p^\infty])\}_p$ is *linearly disjoint* over F. The first goal of this paper is to prove the following analogous statement for CM elliptic curves.

Theorem 1.1. *Let F be a number field and $E_{/F}$ an elliptic curve with complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field $K \subseteq F$. Denote by $\mathfrak{b}_E := \mathfrak{f}_{\mathcal{O}}\, \Delta_F\, N_{F/\mathbb{Q}}(\mathfrak{f}_E)$ the product of the conductor $\mathfrak{f}_{\mathcal{O}} := |\mathcal{O}_K \colon \mathcal{O}|$ of the order $\mathcal{O}$, the absolute discriminant $\Delta_F \in \mathbb{Z}$ of the number field F and the norm $N_{F/\mathbb{Q}}(\mathfrak{f}_E) := |\mathcal{O}_F/\mathfrak{f}_E|$ of the conductor ideal $\mathfrak{f}_E \subseteq \mathcal{O}_F$.*

Date: June 2, 2020.
2020 *Mathematics Subject Classification.* Primary: 11G05, 14K22, 11G15; Secondary: 11S15, 11F80.
Key words and phrases. Elliptic curves, Complex multiplication, Division fields, Entanglement.

Then the map (1) *induces an isomorphism*

$$\mathrm{Gal}(F(E_{tors})/F) \xrightarrow{\sim} \mathrm{Gal}(F(E[S^\infty])/F) \times \prod_{p \notin S} \mathrm{Gal}(F(E[p^\infty])/F)$$

where $S \subseteq \mathbb{N}$ *denotes the finite set of primes dividing* $\mathfrak{b}_E$.

A key ingredient in the proof of Theorem 1.1 is Proposition 3.3, which can be seen as an explicit version of Deuring's analogue, for CM elliptic curves, of Serre's Open Image Theorem (see [25, § 4.5]). More precisely, if $E_{/F}$ is an elliptic curve with complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field K, the extension $F \subseteq F(E_{\mathrm{tors}})$ is abelian. This shows that the image of ρ_E has infinite index in $\mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}}) \cong \mathrm{GL}_2(\widehat{\mathbb{Z}})$, and in particular the conclusion of Serre's theorem does not hold in this setting. Nevertheless, the elements of $\mathrm{Gal}(\overline{F}/F)$ act on E_{tors} as $\mathcal{O}$-module automorphisms, so that the image of ρ_E is contained in the subgroup $\mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}) \subseteq \mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}})$. Then Proposition 3.3 says that $\rho_E(\mathrm{Gal}(F(E[p^n])/F)) = \mathrm{Aut}_{\mathcal{O}}(E[p^n])$ for every prime $p \notin S$ and every $n \in \mathbb{N}$. Hence one has the inclusion

$$\prod_{p \notin S} \mathrm{Aut}_{\mathcal{O}}(E[p^\infty]) \subseteq \mathrm{Im}(\rho_E) := \rho_E(\mathrm{Gal}\,(F(E_{\mathrm{tors}})/F))$$

which can be used to show, as Deuring did, that $\mathrm{Im}(\rho_E) \subseteq \mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}})$ has finite index. Proposition 3.3 is proved using some results concerning formal groups attached to CM elliptic curves, which are recalled in Section 2. We point out that another proof of Proposition 3.3 can also be deduced from previous work of Lozano-Robledo, as explained in Remark 3.4.

While Proposition 3.3 (combined with Lemma 3.1) gives the identification

$$\mathrm{Gal}(F(E[N])/F) \cong (\mathcal{O}/N\mathcal{O})^\times \tag{2}$$

for every $N \in \mathbb{N}$ coprime with $\mathfrak{b}_E$, we prove in Theorem 4.3 that, if the extension $K \subseteq F$ is abelian and $F(E_{\mathrm{tors}}) \subseteq K^{\mathrm{ab}}$, the isomorphism (2) does not hold for infinitely many $N \in \mathbb{N}$ not coprime with $\mathfrak{b}_E$. Theorem 4.3 extends results of Coates and Wiles (see [9, Lemma 3]) and Kuhman (see [14, Chapter II, Lemma 3]) using a class of abelian extensions of K which are constructed in Appendix A. These extensions are a generalisation both of the usual ray class fields for K (see [23, Chapter VI, § 6]) and of the ray class fields for orders defined in [33] and [34, § 4].

The condition $F(E_{\mathrm{tors}}) \subseteq K^{\mathrm{ab}}$ was introduced by Shimura in [28, Theorem 7.44]. The author also shows in [28, Page 217] that if K is an imaginary quadratic field with absolute discriminant $\Delta_K \not\equiv -1\,(3)$, then there exists an elliptic curve E defined over the Hilbert class field H_K with complex multiplication by $\mathcal{O}_K$ such that $H_K(E_{\mathrm{tors}}) \subseteq K^{\mathrm{ab}}$. We generalise Shimura's result in Theorem 4.6 by proving that, for every imaginary quadratic field K and any order $\mathcal{O} \subseteq K$, there exist infinitely many ellipic curves $E_{/H_{\mathcal{O}}}$ with complex multiplication by $\mathcal{O}$ such that the extension $K \subseteq H_{\mathcal{O}}(E_{\mathrm{tors}})$ is abelian. Here $H_{\mathcal{O}}$ denotes the *ring class field of* K *relative to* $\mathcal{O}$ (see [11, § 9]), which is an abelian extension of K coinciding with the Hilbert class field H_K when $\mathcal{O} = \mathcal{O}_K$.

We use Theorem 1.1 and Theorem 4.3 to prove Theorem 5.4, which provides a complete description of the image of (1) when $F = K$ is an imaginary quadratic field and $E_{/K}$ is the base-change of an elliptic curve defined over $\mathbb{Q}$.

The results contained in this article are applied by the authors in two different ways. The first named author uses Theorem 1.1 in [6] to study, jointly with Stevenhagen, cyclic reduction of CM elliptic curves. The second named author uses Theorem 1.1 in [24] to provide explicit planar models of CM elliptic curves defined over $\mathbb{Q}$ and to compute their Mahler measure.

2. Formal groups and elliptic curves

2.1. **Formal groups.** The aim of this subsection is to recall, following [30, Chapter IV], some of the main points of the theory of one dimensional, commutative formal group laws defined over a ring R, which we call *formal groups* for short. Roughly speaking, these are power series $\mathcal{F} \in R[\![z_1, z_2]\!]$ for which the association $x +_{\mathcal{F}} y := \mathcal{F}(x, y)$ behaves like an abelian group law.

Given a formal group $\mathcal{F} \in R[\![z_1, z_2]\!]$ we denote the set of endomorphisms of $\mathcal{F}$ by

$$\mathrm{End}_R(\mathcal{F}) := \{f \in tR[\![t]\!] \mid f(x +_{\mathcal{F}} y) = f(x) +_{\mathcal{F}} f(y)\}$$

which is a ring under the operations $(f +_{\mathcal{F}} g)(t) := \mathcal{F}(f(t), g(t))$ and $(g \circ f)(t) := g(f(t))$. We write $\mathrm{Aut}_R(\mathcal{F})$ for the unit group $\mathrm{End}_R(\mathcal{F})^\times$ and we denote by $[\cdot]_{\mathcal{F}}$ the unique ring homomorphism $\mathbb{Z} \to \mathrm{End}_R(\mathcal{F})$. For every $\phi \in \mathrm{End}_R(\mathcal{F})$ one has that $\phi \in \mathrm{Aut}_R(\mathcal{F})$ if and only if $\phi'(0) \in R^\times$ where $\phi'(t) := \frac{d}{dt}\phi \in R[\![t]\!]$ (see [30, Chapter IV, Lemma 2.4]). Moreover, every $\phi \in \mathrm{End}_R(\mathcal{F})$ is uniquely determined by $\phi'(0)$ whenever R is torsion-free. More precisely, there exist two power series $\exp_{\mathcal{F}}, \log_{\mathcal{F}} \in (R \otimes_{\mathbb{Z}} \mathbb{Q})[\![t]\!]$ such that

$$\phi(t) = \exp_{\mathcal{F}}(\phi'(0) \cdot \log_{\mathcal{F}}(t)) \tag{3}$$

as explained in [30, Chapter IV, § 5].

Let us now recall that if $(R, \mathfrak{m})$ is a complete local ring there is a well defined map

$$\mathfrak{m} \times \mathfrak{m} \xrightarrow{+_{\mathcal{F}}} \mathfrak{m}$$
$$(x, y) \mapsto \mathcal{F}(x, y)$$

endowing the set $\mathfrak{m}$ with the structure of an abelian group, which will be denoted by $\mathcal{F}(\mathfrak{m})$. We will sometimes refer to $\mathcal{F}(\mathfrak{m})$ as the *group of* $\mathfrak{m}$*-points of* $\mathcal{F}$. Every $\phi \in \mathrm{End}_R(\mathcal{F})$ induces an endomorphism $\phi_{\mathfrak{m}} \colon \mathcal{F}(\mathfrak{m}) \to \mathcal{F}(\mathfrak{m})$, and for every ideal $\Phi \subseteq \mathrm{End}_R(\mathcal{F})$ we define the Φ-torsion subgroup $\mathcal{F}(\mathfrak{m})[\Phi] \subseteq \mathcal{F}(\mathfrak{m})$ as

$$\mathcal{F}(\mathfrak{m})[\Phi] := \bigcap_{\phi \in \Phi} \ker(\phi_{\mathfrak{m}}).$$

These Φ-torsion subgroups generalise the usual N-torsion subgroups $\mathcal{F}(\mathfrak{m})[N] \subseteq \mathcal{F}(\mathfrak{m})$ defined for every $N \in \mathbb{Z}$. The following lemma provides some information about the behaviour of $\mathcal{F}(\mathfrak{m})[p^n]$ under finite extensions of local rings with residue characteristic p.

Lemma 2.1 (see [30, Chapter IV, Exercise 4.6] and [31, Page 15])**.** *Let $R \subseteq S$ be a finite extension of complete discrete valuation rings of characteristic zero with maximal ideals $\mathfrak{m}_R \subseteq \mathfrak{m}_S$ and residue fields $\kappa_R \subseteq \kappa_S$. Let $p := \mathrm{char}(\kappa_R) > 0$ be the residue characteristic of R and S, and suppose that $\mathfrak{m}_R = pR$. Then for every formal group $\mathcal{F} \in R[\![z_1, z_2]\!]$ and every $x \in \mathcal{F}(\mathfrak{m}_S)[p^n] \setminus \mathcal{F}(\mathfrak{m}_S)[p^{n-1}]$ with $n \in \mathbb{Z}_{\geq 1}$ we have that*

$$v_S(x) \leq \frac{v_S(p)}{p^{h(n-1)} \cdot (p^h - 1)}$$

where v_S denotes the normalised valuation on S, and

$$h = \mathrm{ht}(\overline{\mathcal{F}}) := \max\left\{ n \in \mathbb{N} \,\middle|\, [p]_{\overline{\mathcal{F}}} \in \kappa_R[\![t^{p^n}]\!] \right\}$$

is the height of the reduced formal group $\overline{\mathcal{F}} \in \kappa_R[\![z_1, z_2]\!]$.

Proof. Using that $h = \mathrm{ht}(\overline{\mathcal{F}})$ and that $\mathfrak{m}_R = p \cdot R$ we see that there exist $f, g \in R[\![t]\!]$ such that $[p]_{\mathcal{F}} = f(t^{p^h}) + p\, g(t)$. We can assume that $f, g \in t\, R[\![t]\!]$ and $g'(0) = 1$ because $[p]_{\mathcal{F}} \in t\, R[\![t]\!]$ and $[p]'_{\mathcal{F}}(0) = p$. Now fix $x \in \mathcal{F}(\mathfrak{m}_S)[p^n] \setminus \mathcal{F}(\mathfrak{m}_S)[p^{n-1}]$ and proceed by induction on $n \in \mathbb{Z}_{\geq 1}$.

If $n = 1$ then $f(x^{p^h}) + p\, g(x) = [p]_{\mathcal{F}}(x) = 0$, hence $v_S(p) + v_S(g(x)) = v_S(f(x^{p^h}))$. Now $v_S(g(x)) = v_S(x)$ because $g(0) = 0$ and $g'(0) = 1$, and $v_S(f(x^{p^h})) \geq v_S(x^{p^h}) = p^h\, v_S(x)$ because $f(0) = 0$. Hence $v_S(p) \geq (p^h - 1) \cdot v_S(x)$, which is what we wanted to prove.

If $n \geq 2$ we know by induction that

$$\frac{v_S(p)}{p^{h(n-2)} \cdot (p^h - 1)} \geq v_S([p]_{\mathcal{F}}(x)) = v_S(f(x^{p^h}) + p\, g(x)) \geq \min(v_S(x^{p^h}), v_S(px))$$

because $[p]_{\mathcal{F}}(x) \in \mathcal{F}(\mathfrak{m}_S)[p^{n-1}] \setminus \mathcal{F}(\mathfrak{m}_S)[p^{n-2}]$. This implies that $\min(v_S(x^{p^h}), v_S(px)) = v_S(x^{p^h})$. Otherwise we would get the contradiction $v_S(p) \geq p^{h(n-2)} \cdot (p^h - 1) \cdot v_S(px) > v_S(p)$ because $n \geq 2$, $v_S(x) > 0$ and $h \geq 1$. Hence we have that

$$v_S(x) = \frac{v_S(x^{p^h})}{p^h} \leq \frac{v_S(p)}{p^h \cdot (p^{h(n-2)} \cdot (p^h - 1))} = \frac{v_S(p)}{p^{h(n-1)} \cdot (p^h - 1)}$$

which is what we wanted to prove. □

2.2. **Formal groups and elliptic curves.** Given an elliptic curve E defined over a number field F by an integral Weierstrass equation one can construct, following for example [30, Chapter IV], a formal group $\widehat{E} \in \mathcal{O}_F[\![z_1, z_2]\!]$ which can be thought of as the formal counterpart of the addition law on E. The association $E \mapsto \widehat{E}$ is functorial and in particular induces a map

$$\begin{aligned} \mathrm{End}_F(E) &\longrightarrow \mathrm{End}_F(\widehat{E}) \\ \phi &\mapsto \widehat{\phi} \end{aligned} \tag{4}$$

between the endomorphism rings of E and $\widehat{E}$. The power series lying in the image of (4) have integral coefficients, as proved in the following theorem, due to Streng.

Theorem 2.2 (see [35, Theorem 2.9]). *Let E be an elliptic curve defined over a number field F and let $\widehat{E} \in \mathcal{O}_F[\![z_1, z_2]\!]$ be the formal group law associated to a Weierstrass model of E with coefficients $a_1, \dots, a_6 \in \mathcal{O}_F$. Then for every $\phi \in \mathrm{End}_F(E)$ we have that $\widehat{\phi} \in \mathcal{O}_F[\![t]\!]$.*

Proof. One can show by induction that $\widehat{[n]_E} = [n]_{\widehat{E}} \in \mathbb{Z}[a_1, \dots, a_6][\![t]\!] \subseteq \mathcal{O}_F[\![t]\!]$ for every $n \in \mathbb{Z}$, where $[n]_E \in \mathrm{End}_F(E)$ denotes the multiplication-by-n map. This proves the theorem when $\mathrm{End}_F(E) \cong \mathbb{Z}$. Otherwise E has *complex multiplication* by [30, Chapter III, Corollary 9.4], and one can combine [29, Chapter II, Proposition 1.1] and [30, Chapter IV, Corollary 4.3] to see that there exists a unique isomorphism $[\cdot]_E \colon \mathcal{O} \xrightarrow{\sim} \mathrm{End}_F(E)$ such that $\widehat{[\alpha]}_E'(0) = \alpha$ for every $\alpha \in \mathcal{O}$ where $\mathcal{O}$ is an order in an imaginary quadratic field $K \subseteq F$.

Let $\{\psi_j\}_{j \in \mathbb{N}} \subseteq F[s]$ be the polynomials determined by the equality

$$\sum_{j=0}^{+\infty} \psi_j(s) \cdot t^j = \exp_{\widehat{E}}(s \cdot \log_{\widehat{E}}(t)) \in F[\![t, s]\!]$$

and observe that $\psi_j(\mathbb{Z}) \subseteq \mathcal{O}_F$ for every $j \in \mathbb{N}$ because (3) shows that

$$\sum_{j=0}^{+\infty} \psi_j(n) \cdot t^j = [n]_{\widehat{E}}(t) \in \mathcal{O}_F[\![t]\!]$$

for every $n \in \mathbb{Z}$.

To conclude it is sufficient to show that $\psi_j(\mathcal{O}) \subseteq \mathcal{O}_{F_{\mathfrak{P}}}$ for every $j \in \mathbb{N}$ and every prime $\mathfrak{P} \subseteq \mathcal{O}_F$, where $F_{\mathfrak{P}}$ denotes the completion of F at $\mathfrak{P}$. Indeed, in this case $\psi_j(\mathcal{O}) \subseteq \mathcal{O}_F$ for every $j \in \mathbb{N}$, and again (3) gives

$$\widehat{[\alpha]}_E(t) = \exp_{\widehat{E}}(\widehat{[\alpha]}_E'(0) \cdot \log_{\widehat{E}}(t)) = \exp_{\widehat{E}}(\alpha \cdot \log_{\widehat{E}}(t)) = \sum_{j=0}^{+\infty} \psi_j(\alpha) \cdot t^j \in \mathcal{O}_F[\![t]\!]$$

for every $\alpha \in \mathcal{O}$. The inclusion $\psi_j(\mathcal{O}) \subseteq \mathcal{O}_{F_{\mathfrak{P}}}$ is easily seen if $\mathfrak{P}$ lies above a rational prime $p \in \mathbb{N}$ which splits in K, because under this assumption $\mathcal{O} \subseteq \mathbb{Z}_p$ and $\psi_j(\mathbb{Z}_p) \subseteq \mathcal{O}_{F_{\mathfrak{P}}}$ since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$ and $\psi_j \colon F_{\mathfrak{P}} \to F_{\mathfrak{P}}$ is continuous with respect to the $\mathfrak{P}$-adic topology. For the remaining cases we refer the reader to the original proof contained in [35]. □

Let now $\mathfrak{P} \subseteq \mathcal{O}_F$ be a prime of F with residue field $\kappa_{\mathfrak{P}}$ and corresponding maximal ideal $\mathfrak{m}_{\mathfrak{P}} \subseteq \mathcal{O}_{F_{\mathfrak{P}}}$, where $F_{\mathfrak{P}}$ denotes the completion of F at $\mathfrak{P}$. Then [35, § 2] shows that there is a unique injective group homomorphism $\iota_{\mathfrak{P}} \colon \widehat{E}(\mathfrak{m}_{\mathfrak{P}}) \to E(F_{\mathfrak{P}})$ making the following diagram

$$\begin{tikzcd} \widehat{E}(\mathfrak{m}_{\mathfrak{P}}) \arrow[r, "\iota_{\mathfrak{P}}"] \arrow[d, "\widehat{\phi}_{\mathfrak{P}}"'] & E(F_{\mathfrak{P}}) \arrow[d, "\phi"] \\ \widehat{E}(\mathfrak{m}_{\mathfrak{P}}) \arrow[r, "\iota_{\mathfrak{P}}"] & E(F_{\mathfrak{P}}) \end{tikzcd} \tag{5}$$

commute for every $\phi \in \operatorname{End}_{F_{\mathfrak{P}}}(E)$, where $\widehat{\phi}_{\mathfrak{P}} := (\widehat{\phi})_{\mathfrak{m}_{\mathfrak{P}}}$ (see Section 2.1). Moreover [30, Chapter VII, Proposition 2.1 and Proposition 2.2] imply that $\iota_{\mathfrak{P}}$ fits in the following exact sequence

$$0 \to \widehat{E}(\mathfrak{m}_{\mathfrak{P}}) \xrightarrow{\iota_{\mathfrak{P}}} E(F_{\mathfrak{P}}) \xrightarrow{\pi_{\mathfrak{P}}} \widetilde{E}(\kappa_{\mathfrak{P}}) \to 0$$

in which $\widetilde{E}$ denotes the reduction of E modulo $\mathfrak{P}$ and $\pi_{\mathfrak{P}} \colon E(F_{\mathfrak{P}}) \twoheadrightarrow \widetilde{E}(\kappa_{\mathfrak{P}})$ is the canonical projection. Taking torsion and using (5) we get a left-exact sequence

$$0 \to \widehat{E}(\mathfrak{m}_{\mathfrak{P}})[\widehat{\Phi}] \xrightarrow{\iota_{\mathfrak{P}}} E(F_{\mathfrak{P}})[\Phi] \xrightarrow{\pi_{\mathfrak{P}}} \widetilde{E}(\kappa_{\mathfrak{P}})[\Phi] \tag{6}$$

for every ideal $\Phi \subseteq \operatorname{End}_{F_{\mathfrak{P}}}(E)$. Here $E(F_{\mathfrak{P}})[\Phi] \subseteq E(F_{\mathfrak{P}})$ is the Φ-torsion subgroup

$$E(F_{\mathfrak{P}})[\Phi] := \bigcap_{\phi \in \Phi} \ker(\phi)$$

and $\widetilde{E}(\kappa_{\mathfrak{P}})[\Phi]$ is defined analogously, noting that the map $\operatorname{End}_{F_{\mathfrak{P}}}(E) \to \operatorname{End}_{\kappa_{\mathfrak{P}}}(\widetilde{E})$ is injective (see [29, Chapter II, Proposition 4.4]). We remark that $\widehat{E}(\mathfrak{m}_{\mathfrak{P}})[\widehat{\Phi}]$ is well defined since $\widehat{\Phi} \subseteq \mathcal{O}_F[\![t]\!]$ by Theorem 2.2. Sequence (6) will be extensively used in the next section.

3. Division fields of CM elliptic curves: ramification and entanglement

The goal of this section is to prove Theorem 1.1 by studying the ramification properties of primes in division field extensions associated to CM elliptic curves, as described in Proposition 3.2 and Proposition 3.3. The proof of these results is an application to the CM case of the theory of formal groups outlined in Section 2. We work in a fixed algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$.

Let $F \subseteq \overline{\mathbb{Q}}$ be a number field and let $E_{/F}$ be an elliptic curve with *complex multiplication* by an order $\mathcal{O}$ in an imaginary quadratic field K, which means that $\operatorname{End}_{\overline{\mathbb{Q}}}(E) \cong \mathcal{O}$. One can always fix, combining [29, Chapter II, Proposition 1.1] and [30, Chapter IV, Corollary 4.3], a unique isomorphism $[\cdot]_E \colon \mathcal{O} \xrightarrow{\sim} \operatorname{End}_{\overline{\mathbb{Q}}}(E)$ normalised in such a way that $\widehat{[\alpha]}_E'(0) = \alpha$ for every $\alpha \in \mathcal{O}$, where $\widehat{[\alpha]}_E \in \operatorname{End}_{\overline{\mathbb{Q}}}(\widehat{E})$ denotes the endomorphism of the formal group $\widehat{E}$ associated to $[\alpha]_E$ by (4). We will assume throughout this section that the field of definition F contains the CM field K. This assumption implies in particular that all the endomorphisms of E are already defined over F, as proved in [27, Chapter II, Proposition 30].

For any field extension $F \subseteq L \subseteq \overline{\mathbb{Q}}$ and any ideal $I \subseteq \mathcal{O}$ we write

$$E(L)[I] := \{P \in E(L) : [\alpha]_E(P) = 0 \text{ for all } \alpha \in I\}$$

for the set of I-torsion points of E defined over L, which is naturally a module over $\mathcal{O}/I$. When $I = \alpha \cdot \mathcal{O}$ for some $\alpha \in \mathcal{O}$ we write $E(L)[\alpha] := E(L)[I]$ and $E[\alpha] := E(\overline{\mathbb{Q}})[\alpha]$. For any ideal $I \subseteq \mathcal{O}$ the groups $E[I] := E(\overline{\mathbb{Q}})[I]$ are always finite and they give rise to finite extensions $F \subseteq F(E[I])$ obtained by adjoining to F the coordinates of every I-torsion point. We refer to the number field $F(E[I])$ as the *I-division field* of $E_{/F}$. The next result summarises the main properties of the extension $F \subseteq F(E[I])$ when I is invertible (see [23, Chapter I, § 12]).

Lemma 3.1. *Let F be a number field and $E_{/F}$ an elliptic curve with complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field $K \subseteq F$. Then for every ideal $I \subseteq \mathcal{O}$ the extension $F \subseteq F(E[I])$ is Galois and there is a canonical inclusion $\mathrm{Gal}(F(E[I])/F) \hookrightarrow \mathrm{Aut}_{\mathcal{O}}(E[I])$. Moreover, if I is invertible, the group $E[I]$ has a natural structure of free $\mathcal{O}/I$-module of rank one and, after choosing a generator, one gets an injective group homomorphism*

$$\rho_{E,I} \colon \mathrm{Gal}(F(E[I])/F) \hookrightarrow (\mathcal{O}/I)^{\times}$$

which will be denoted by $\rho_{E,N}$ when $I = N \cdot \mathcal{O}$ for some $N \in \mathbb{Z}$. Under the further assumption that I is coprime to the ideal $\mathfrak{f}_{\mathcal{O}} \cdot \mathcal{O}$ generated by the conductor $\mathfrak{f}_{\mathcal{O}} := |\mathcal{O}_K \colon \mathcal{O}|$ of the order $\mathcal{O}$, one has that $\mathcal{O}/I \cong \mathcal{O}_K/I\mathcal{O}_K$.

Proof. Since F contains the CM field K, the endomorphisms of E are all defined over F and this implies that $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ acts on $E[I]$ by $\mathcal{O}$-module automorphisms. In particular $F \subseteq F(E[I])$ is Galois and there is a canonical inclusion $\mathrm{Gal}(F(E[I])/F) \hookrightarrow \mathrm{Aut}_{\mathcal{O}}(E[I])$. If I is invertible, $E[I]$ has the structure of free $\mathcal{O}/I$-module of rank one by [5, Lemma 2.4], and the choice of a generator induces an isomorphism $\mathrm{Aut}_{\mathcal{O}}(E[I]) \cong (\mathcal{O}/I)^{\times}$ which gives the map $\rho_{E,I}$ appearing in the statement. The last assertion follows from [11, Proposition 7.20]. □

With the next proposition we start our study concerning the ramification properties of the extensions $F \subseteq F(E[I])$ by finding an explicit finite set of primes outside which these are unramified.

Proposition 3.2. *Let F be a number field and $E_{/F}$ an elliptic curve with complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field $K \subseteq F$. Denote by $\mathfrak{f}_{\mathcal{O}} := |\mathcal{O}_K \colon \mathcal{O}|$ the conductor of the order $\mathcal{O}$ and by $\mathfrak{f}_E \subseteq \mathcal{O}_F$ the conductor ideal of the elliptic curve E. Then for every ideal $I \subseteq \mathcal{O}$ coprime with $\mathfrak{f}_{\mathcal{O}}$ the extension $F \subseteq F(E[I])$ is unramified at all primes not dividing $(I \cdot \mathcal{O}_F) \cdot \mathfrak{f}_E$.*

Proof. Since I is coprime with the conductor of the order $\mathcal{O}$, it can be uniquely factored into a product of invertible prime ideals of $\mathcal{O}$ (see [11, Proposition 7.20]). The field $F(E[I])$ is then the compositum of all the division fields $F(E[\mathfrak{p}^n])$ with $\mathfrak{p}^n$ the prime power factors of I in $\mathcal{O}$. Hence it suffices to prove that for every invertible prime ideal $\mathfrak{p} \subseteq \mathcal{O}$ and $n \in \mathbb{N}$, the field extension $F \subseteq F(E[\mathfrak{p}^n])$ is unramified at every prime of F not dividing $(\mathfrak{p}\,\mathcal{O}_F) \cdot \mathfrak{f}_E$.

Fix an invertible prime $\mathfrak{p} \subseteq \mathcal{O}$ and write $L := F(E[\mathfrak{p}^n])$. Let $\mathfrak{q} \nmid (\mathfrak{p}\,\mathcal{O}_F) \cdot \mathfrak{f}_E$ be a prime of F and fix a prime $\mathfrak{Q} \subseteq \mathcal{O}_L$ lying above $\mathfrak{q}$, with residue field κ. Since $\mathfrak{q}$ does not divide the conductor $\mathfrak{f}_E$ of the elliptic curve, E has good reduction $\widetilde{E}$ modulo $\mathfrak{q}$ and we then denote by $\pi \colon E(L) \to \widetilde{E}(\kappa)$ the reduction map. Take $\sigma \in I(\mathfrak{Q}/\mathfrak{q})$, where $I(\mathfrak{Q}/\mathfrak{q}) \subseteq \mathrm{Gal}(L/F)$ denotes the inertia subgroup of $\mathfrak{q} \subseteq \mathfrak{Q}$, and fix a torsion point $Q \in E[\mathfrak{p}^n] = E(L)[\mathfrak{p}^n]$. By definition of inertia σ acts trivially on the residue field κ, hence

$$\pi(Q^{\sigma} - Q) = \pi(Q^{\sigma}) - \pi(Q) = \pi(Q) - \pi(Q) = 0 \tag{7}$$

i.e. the point $Q^{\sigma} - Q$ is in the kernel of the reduction map π. We are going to use the exact sequence (6) to show that the only $\mathfrak{p}^n$-torsion point contained in this kernel is 0. To this aim, we embed L in its $\mathfrak{Q}$-adic completion $L_{\mathfrak{Q}}$ with ring of integers $\mathcal{O}_{L_{\mathfrak{Q}}}$ and maximal ideal $\mathfrak{m}_{\mathfrak{Q}}$. Notice that the set $(\mathfrak{p}^n \cap \mathcal{O}) \setminus (\mathfrak{Q} \cap \mathcal{O})$ is non-empty because $\mathfrak{p} \nmid \mathfrak{f}_{\mathcal{O}}$ and $\mathfrak{q} \nmid (\mathfrak{p}\,\mathcal{O}_F)$. Consider then the formal group $\widehat{E} \in \mathcal{O}_F[\![z_1, z_2]\!]$ associated to an integral Weierstrass model of E, and let $\alpha \in (\mathfrak{p}^n \cap \mathcal{O}) \setminus (\mathfrak{Q} \cap \mathcal{O})$. The endomorphism $\widehat{[\alpha]}_E \in \mathrm{End}_F(\widehat{E})$ corresponding to $[\alpha]_E \in \mathrm{End}_F(E)$ via (4) becomes an automorphism over $L_{\mathfrak{Q}}$, because $\widehat{[\alpha]}_E'(0) = \alpha \in \mathcal{O}_{L_{\mathfrak{Q}}}^{\times}$. Hence taking $\Phi = [\mathfrak{p}^n]_E$ in (6) shows that $E[\mathfrak{p}^n] \cap \ker(\pi) \subseteq E[\alpha] \cap \ker(\pi) = \{0\}$, where the last equality holds because $\widehat{E}(\mathfrak{m}_{\mathfrak{Q}})\widehat{[\alpha]}_E = 0$. Combining this with (7) we see that $Q^{\sigma} = Q$ for every $Q \in E[\mathfrak{p}^n]$ and $\sigma \in I(\mathfrak{Q}/\mathfrak{q})$.

Since L is generated over F by the elements of $E[\mathfrak{p}^n]$, we deduce that the inertia group $I(\mathfrak{Q}/\mathfrak{q})$ is trivial. In particular, $F \subseteq L$ is unramified at every prime not dividing $(\mathfrak{p} \cdot \mathcal{O}_F)\,\mathfrak{f}_E$, as wanted. □

We now turn to the study of the primes which ramify in $F \subseteq F(E[I])$. To do this it suffices to restrict our attention to the case $I = \mathfrak{p}^n$ for some prime $\mathfrak{p} \subseteq \mathcal{O}$ and some $n \in \mathbb{N}$, as we do in the following proposition.

Proposition 3.3. *Let F be a number field and $E_{/F}$ an elliptic curve with complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field $K \subseteq F$. Denote by $\mathfrak{d}_E := \mathfrak{f}_{\mathcal{O}}\, \Delta_F\, N_{F/\mathbb{Q}}(\mathfrak{f}_E)$ the product of the conductor $\mathfrak{f}_{\mathcal{O}} := |\mathcal{O}_K \colon \mathcal{O}|$ of the order $\mathcal{O}$, the absolute discriminant $\Delta_F \in \mathbb{Z}$ of the number field F and the norm $N_{F/\mathbb{Q}}(\mathfrak{f}_E) := |\mathcal{O}_F/\mathfrak{f}_E|$ of the conductor ideal $\mathfrak{f}_E \subseteq \mathcal{O}_F$. Then for any $n \in \mathbb{N}$ and any prime ideal $\mathfrak{p} \subseteq \mathcal{O}$ coprime with $\mathfrak{d}_E\,\mathcal{O}$ the extension $F \subseteq F(E[\mathfrak{p}^n])$ is totally ramified at each prime dividing $\mathfrak{p}\,\mathcal{O}_F$. Moreover, the Galois representation*

$$\rho_{E,\mathfrak{p}^n} \colon \operatorname{Gal}(F(E[\mathfrak{p}^n])/F) \hookrightarrow (\mathcal{O}/\mathfrak{p}^n)^\times \cong (\mathcal{O}_K/\mathfrak{p}^n\mathcal{O}_K)^\times$$

defined in Lemma 3.1 is an isomorphism.

Proof. The statement is trivially true if $n = 0$, hence we assume that $n \geq 1$. Fix $\widehat{E} \in \mathcal{O}_F[\![z_1, z_2]\!]$ to be the formal group associated to an integral Weierstrass model of E, and let $\mathfrak{p} \subseteq \mathcal{O}$ be as in the statement. The hypothesis of coprimality with $\mathfrak{d}_E\,\mathcal{O}$ implies that $\mathfrak{p}$ is invertible in $\mathcal{O}$ and that it lies above a rational prime $p \in \mathbb{N}$ that is unramified in K. We divide the proof according to the splitting behaviour of p in $\mathcal{O}$, which is the same as the splitting behaviour in K, since $p \nmid \mathfrak{f}_{\mathcal{O}}$.

First, assume that p is inert in K, so that $\mathfrak{p} = p\mathcal{O}$. In this case, $L := F(E[\mathfrak{p}^n])$ coincides with the p^n-division field $F(E[p^n])$. The injectivity of the Galois representation

$$\rho_{E,p^n} \colon \operatorname{Gal}(L/F) \hookrightarrow (\mathcal{O}/p^n\mathcal{O})^\times \cong (\mathcal{O}_K/p^n\mathcal{O}_K)^\times$$

shows that the degree of the extension $F \subseteq L$ is bounded as

$$[L : F] \leq |(\mathcal{O}_K/p^n\mathcal{O}_K)^\times| = p^{2(n-1)}(p^2 - 1).$$

Let $\mathfrak{P} \subseteq \mathcal{O}_L$ be a prime of L lying above p and denote by $L_{\mathfrak{P}}$ the $\mathfrak{P}$-adic completion of L with ring of integers $\mathcal{O}_{L_{\mathfrak{P}}}$, maximal ideal $\mathfrak{m}_{\mathfrak{P}}$ and residue field $\kappa_{\mathfrak{P}}$. We want to determine the ramification index $e(\mathfrak{P}/(\mathfrak{P} \cap \mathcal{O}_F))$.

Since p is inert in K, the reduced elliptic curve $\widetilde{E}$ is supersingular by [15, § 14, Theorem 12], hence $\widetilde{E}(\kappa_{\mathfrak{P}})[p^n] = 0$. Taking $\Phi = [p^n]_E$ in (6), we see that the group $\widehat{E}(\mathfrak{m}_{\mathfrak{P}})$ contains a non-zero point of exact order p^n. We can now use Lemma 2.1 and the hypothesis $p \nmid \Delta_F$ to get

$$p^{h(n-1)}(p^h - 1) \leq v_{L_{\mathfrak{P}}}(p) = e(\mathfrak{P}/p) = e(\mathfrak{P}/(\mathfrak{P} \cap \mathcal{O}_F)) \leq [L \colon F] \leq p^{2(n-1)}(p^2 - 1). \tag{8}$$

where $h \in \mathbb{N}$ denotes the height of the reduction modulo $\mathfrak{P}$ of the formal group $\widehat{E}$. Since the latter is precisely the formal group associated to $\widetilde{E}$, we have that $h = 2$ by [30, Chapter V, Theorem 3.1]. Thus all the inequalities appearing in (8) are actually equalities, and we see at once that $e(\mathfrak{P}/(\mathfrak{P} \cap \mathcal{O}_F)) = [L \colon F] = p^{2(n-1)}(p^2 - 1)$, which implies that ρ_{E,p^n} is an isomorphism and that $\mathfrak{P} \cap \mathcal{O}_F$ is totally ramified in L. This concludes the proof of the inert case.

Suppose now that p splits in K, so that $p\mathcal{O} = \mathfrak{p}\overline{\mathfrak{p}}$, where $\overline{\mathfrak{p}}$ is the image of $\mathfrak{p}$ under the unique non-trivial automorphism of K. If we put again $L := F(E[\mathfrak{p}^n])$, the injectivity of $\rho_{E,\mathfrak{p}^n}$ gives

$$[L : F] \leq |(\mathcal{O}_K/\mathfrak{p}^n\mathcal{O}_K)^\times| = p^{n-1}(p - 1).$$

It is convenient in this case to work inside the bigger division field $\widetilde{F} := F(E[p^n])$, which contains both L and $L' := F(E[\,\overline{\mathfrak{p}}^n\,])$. We then fix $\mathfrak{P}, \overline{\mathfrak{P}} \subseteq \mathcal{O}_{\widetilde{F}}$ two primes of $\widetilde{F}$ lying respectively above $\mathfrak{p}\mathcal{O}_K$ and $\overline{\mathfrak{p}}\mathcal{O}_K$, and we denote by $\mathcal{P} := \mathfrak{P} \cap \mathcal{O}_L$ and $\overline{\mathcal{P}} := \overline{\mathfrak{P}} \cap \mathcal{O}_L$ the corresponding primes in L. For every prime ideal $\mathfrak{q} \in \{\mathfrak{P}, \overline{\mathfrak{P}}\}$ we denote by $\widetilde{F}_{\mathfrak{q}}$ the $\mathfrak{q}$-adic completion of $\widetilde{F}$ with ring of integers $\mathcal{O}_{\widetilde{F}_{\mathfrak{q}}}$ and residue field $\kappa_{\mathfrak{q}}$, and by $\widetilde{E}_{\mathfrak{q}}$ the reduction of $E_{/\widetilde{F}}$ modulo $\mathfrak{q}$. We use analogous notation for $\mathcal{P}$ and $\overline{\mathcal{P}}$. The goal is to compute the ramification index $e(\mathcal{P}/\mathcal{P} \cap \mathcal{O}_F)$, and we divide our argument in three steps.

$\boxed{\textbf{Step 1}}$ First of all, we prove that the reduction map $E[\mathfrak{p}^n] \longrightarrow \widetilde{E}_{\overline{\mathfrak{P}}}(\kappa_{\overline{\mathfrak{P}}})$ is injective. This is equivalent to say that $\ker(\pi_{\overline{\mathcal{P}}}) \cap E(L_{\overline{\mathcal{P}}})[\mathfrak{p}^n] = 0$, where

$$\pi_{\overline{\mathcal{P}}} \colon E(L_{\overline{\mathcal{P}}}) \twoheadrightarrow \widetilde{E}_{\overline{\mathcal{P}}}(\kappa_{\overline{\mathcal{P}}}) \subseteq \widetilde{E}_{\overline{\mathfrak{P}}}(\kappa_{\overline{\mathfrak{P}}})$$

denotes the reduction modulo $\overline{\mathcal{P}}$. Since p is coprime with the conductor of the order $\mathcal{O}$ by assumption, it is possible to find $\alpha \in \mathfrak{p}^n$ such that $\alpha \notin \overline{\mathfrak{p}}$. The endomorphism $\widehat{[\alpha]}_E \in \mathrm{End}_F(\widehat{E})$ corresponding to $[\alpha]_E \in \mathrm{End}_F(E)$ via (4) becomes an automorphism over $L_{\overline{\mathcal{P}}}$, because $\widehat{[\alpha]}_E'(0) = \alpha \in \mathcal{O}_{L_{\overline{\mathcal{P}}}}^\times$. Hence taking $\Phi = [\mathfrak{p}^n]_E$ in (6) shows that

$$\ker(\pi_{\overline{\mathcal{P}}}) \cap E(L_{\overline{\mathcal{P}}})[\mathfrak{p}^n] \subseteq \ker(\pi_{\overline{\mathcal{P}}}) \cap E(L_{\overline{\mathcal{P}}})[\alpha] = 0$$

where the last equality holds because $\widehat{E}(\mathfrak{m}_{\overline{\mathcal{P}}})[\widehat{\alpha}]_E = 0$. In exactly the same way, using L' in place of L, one shows that the reduction map $E[\overline{\mathfrak{p}}^n] \longrightarrow \widetilde{E}_{\mathfrak{P}}(\kappa_{\mathfrak{P}})$ is injective.

$\boxed{\textbf{Step 2}}$ We now claim that $\ker(\pi_{\mathfrak{P}}) \cap E[p^n] = E[\mathfrak{p}^n]$ where $\pi_{\mathfrak{P}} : E(\widetilde{F}) \longrightarrow \widetilde{E}_{\mathfrak{P}}(\kappa_{\mathfrak{P}})$ denotes the reduction modulo $\mathfrak{P}$. Since $p\mathcal{O} = \mathfrak{p}\overline{\mathfrak{p}}$, there is a decomposition of the group $E[p^n]$ into the direct sum of $E[\,\mathfrak{p}^n\,]$ and $E[\,\overline{\mathfrak{p}}^n\,]$, which are cyclic groups of order p^n by Lemma 3.1. In particular, there exists $A \in E[\mathfrak{p}^n]$ and $B \in E[\overline{\mathfrak{p}}^n]$ such that every p^n-torsion point $Q \in E[p^n]$ can be written as

$$Q = [a](A) + [b](B)$$

for unique $a, b \in \{0, \dots, p^n - 1\}$. If $\pi_{\mathfrak{P}}(Q) = 0$ then

$$\pi_{\mathfrak{P}}([b](B)) = \pi_{\mathfrak{P}}([-a](A)) \in \widetilde{E}_{\mathfrak{P}}[\,\mathfrak{p}^n\,] \cap \widetilde{E}_{\mathfrak{P}}[\,\overline{\mathfrak{p}}^n\,] = \{0\}$$

where the last equality follows from the fact that $\mathfrak{p}^n$ and $\overline{\mathfrak{p}}^n$ are coprime in $\mathcal{O}$. In particular, $[b](B)$ is in the kernel of the reduction map $E[\overline{\mathfrak{p}}^n] \longrightarrow \widetilde{E}_{\mathfrak{P}}(\kappa_{\mathfrak{P}})[p^n]$, which is the restriction of $\pi_{\mathfrak{P}}$ to $E[\overline{\mathfrak{p}}^n]$ and is injective by **Step 1**. Hence we have $Q = [a](A) \in E[\mathfrak{p}^n]$, and this shows the inclusion $\ker(\pi_{\mathfrak{P}}) \cap E[p^n] \subseteq E[\mathfrak{p}^n]$. To prove the other inclusion first notice that the restriction of $\pi_{\mathfrak{P}}$ to $E[p^n]$ gives rise to a surjection $E[p^n] \twoheadrightarrow \widetilde{E}_{\mathfrak{P}}(\kappa_{\mathfrak{P}})[p^n]$ because $E[\overline{\mathfrak{p}}^n] \longrightarrow \widetilde{E}_{\mathfrak{P}}(\kappa_{\mathfrak{P}})[p^n]$ is injective and the elliptic curve $\widetilde{E}_{\mathfrak{P}}$ is ordinary by [15, § 14, Theorem 12]. This gives

$$\frac{E[p^n]}{\ker(\pi_{\mathfrak{P}}) \cap E[p^n]} \cong \widetilde{E}_{\mathfrak{P}}(\kappa_{\mathfrak{P}})[p^n]$$

which in turn shows that

$$|\ker(\pi_{\mathfrak{P}}) \cap E[p^n]| = \frac{|E[p^n]|}{|\widetilde{E}_{\mathfrak{P}}(\kappa_{\mathfrak{P}})[p^n]|} = \frac{p^{2n}}{p^n} = p^n = |E[\mathfrak{p}^n]|.$$

We conclude that $\ker(\pi_{\mathfrak{P}}) \cap E[p^n] = E[\mathfrak{p}^n]$.

$\boxed{\textbf{Step 3}}$ Using (6) with $\Phi = [p^n]_E$ and **Step 2**, after recalling that $\mathfrak{P}$ lies over $\mathcal{P}$, one can see that the group $\widehat{E}(\mathfrak{m}_{\mathcal{P}})$ contains a point of exact order p^n. We now apply Lemma 2.1 and the hypothesis $p \nmid \Delta_F$ to get

$$p^{h(n-1)}(p^h - 1) \leq v_{L_{\mathcal{P}}}(p) = e(\mathcal{P}/p) = e(\mathcal{P}/(\mathcal{P} \cap \mathcal{O}_F)) \leq [L \colon F] \leq p^{n-1}(p-1). \tag{9}$$

where $h \in \mathbb{N}$ denotes the height of the reduction modulo $\mathcal{P}$ of the formal group $\widehat{E}$. Since the latter is precisely the formal group associated to the ordinary elliptic curve $\widetilde{E}_{\mathcal{P}}$, we have that $h = 1$ by [30, Chapter V, Theorem 3.1]. Thus all the inequalities appearing in (9) are actually equalities, and we see at once that $e(\mathcal{P}/(\mathcal{P} \cap \mathcal{O}_F)) = [L \colon F] = p^{n-1}(p-1)$, which implies that $\rho_{E,\mathfrak{p}^n}$ is an isomorphism and that $\mathcal{P} \cap \mathcal{O}_F$ is totally ramified in L. This concludes the proof. □

Remark 3.4. As we already stated in the introduction, Proposition 3.3 can be obtained by combining various results of Lozano-Robledo. More precisely, see [18, Proposition 5.6] for the inert case and the proof of [19, Theorem 6.10] for the split case. The arguments used by Lozano-Robledo for the inert case involve a formula for the valuation of the coefficient of t^p in the power series $[p]_{\widehat{E}}(t) \in \mathcal{O}_F[\![t]\!]$ (see [17, Theorem 3.9]), and the study of the split case goes through a detailed investigation of Borel subgroups of $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ (see [19, Section 4]). Our proof of Proposition 3.3, which concerns only CM elliptic curves and prime ideals not dividing $\mathfrak{b}_E \mathcal{O}$, appears to be shorter because it uses the same techniques to deal with the split and inert case. Notice as well that our discussion is explicitly written for general imaginary quadratic orders, whereas [19, Theorem 6.10] is stated and proved only for maximal orders. We observe however that [19, Remark 6.12] points out that the proof of [19, Theorem 6.10] carries over to the general case.

We also remark that, if $\mathcal{O} = \mathcal{O}_K$ is a maximal order of class number 1 and $F = K$, Proposition 3.3 is proved by Coates and Wiles in [9, Lemma 5] (see also [1, Lemma 3] and [10, Proposition 47]). The main tool used in their proof is Lubin-Tate theory.

Remark 3.5. Let $E_{/F}$ be any elliptic curve (not necessarily with complex multiplication) which has good supersingular reduction at a prime $\mathfrak{p} \subseteq \mathcal{O}_F$ lying above a prime $p \in \mathbb{N}$ which does not ramify in $\mathbb{Q} \subseteq F$. Then one can use the same argument provided in the first part of the proof of Proposition 3.3 to show that the ramification index $e(\mathfrak{P}/\mathfrak{p})$ is bounded from below by $p^{2(n-1)}(p^2-1)$, where $\mathfrak{P} \subseteq F(E[p^n])$ is any prime lying above $\mathfrak{p}$. This result has already been proved by Lozano-Robledo in [18, Proposition 5.6] and by Smith in [32, Theorem 2.1].

We are now ready to prove Theorem 1.1. Recall that a family $\mathcal{F} = \{F_s\}_{s\in\mathcal{S}}$ of Galois extensions of a number field F, indexed over any set $\mathcal{S}$, is called *linearly disjoint* over F if the natural inclusion map

$$\mathrm{Gal}(L/F) \hookrightarrow \prod_{s\in\mathcal{S}} \mathrm{Gal}(F_s/F)$$

is an isomorphism, where L denotes the compositum of the fields F_s. Otherwise the family is called *entangled* over F.

Proof of Theorem 1.1. The family $\{F(E[p^\infty])\}_{q\notin S} \cup \{F(E[S^\infty])\}$ appearing in the statement of Theorem 1.1 is linearly disjoint over F if and only if $F(E[p^n]) \cap F(E[m]) = F$ for every prime $p \notin S$, every $n \in \mathbb{N}$ and every $m \in \mathbb{Z}$ coprime with p. To prove this latter statement, we first show that every non-trivial subextension of $\widetilde{F} := F(E[p^n])$ is ramified at some prime dividing p.

When p is inert in K, this follows immediately from Proposition 3.3. Suppose then that p is split in K, with $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$. The division field $\widetilde{F}$ is the compositum over F of the extensions $F_{\mathfrak{p}} := F(E[\mathfrak{p}^n])$ and $F_{\overline{\mathfrak{p}}} := F(E[\overline{\mathfrak{p}}^n])$. By Proposition 3.3 the extension $F \subseteq F_{\mathfrak{p}}$ (respectively $F \subseteq F_{\overline{\mathfrak{p}}}$) is totally ramified at every prime of F lying over $\mathfrak{p}$ (resp. $\overline{\mathfrak{p}}$). Let $\mathfrak{P}$ be a prime of F lying above $\mathfrak{p}$, and denote by $I(\mathfrak{P}) \subseteq \mathrm{Gal}(\widetilde{F}/F)$ its inertia group and by $e(\mathfrak{P})$ its ramification index in the extension $F \subseteq \widetilde{F}$. If $F \subsetneq L$ is a subextension of $F \subseteq \widetilde{F}$ in which $\mathfrak{P}$ does not ramify, then L must be contained in the inertia field $T = (\widetilde{F})^{I(\mathfrak{P})}$ relative to $\mathfrak{P}$. Notice that the latter also contains $F_{\overline{\mathfrak{p}}}$, since by Proposition 3.2 the extension $F \subseteq F_{\overline{\mathfrak{p}}}$ is unramified at $\mathfrak{P}$. On the other hand, the fact that $F \subseteq F_{\mathfrak{p}}$ is totally ramified at $\mathfrak{P}$ gives the chain of inequalities

$$[F_{\overline{\mathfrak{p}}} \colon F] \leq [T \colon F] = \frac{[\widetilde{F} \colon F]}{|I(\mathfrak{P})|} = \frac{[\widetilde{F} \colon F]}{e(\mathfrak{P})} \leq \frac{[F_{\mathfrak{p}} \colon F] \cdot [F_{\overline{\mathfrak{p}}} \colon F]}{e(\mathfrak{P})} \leq [F_{\overline{\mathfrak{p}}} \colon F]$$

which shows that $T = F_{\overline{\mathfrak{p}}}$. Hence Proposition 3.3 implies that any extension $F \subsetneq L$ which is unramified at every prime above $\mathfrak{p}$ is totally ramified at every prime above $\overline{\mathfrak{p}}$.

Now it is easy to conclude that $\widetilde{F} \cap F(E[m]) = F$, since otherwise $F \subsetneq F(E[m])$ would ramify at some prime of F dividing p, contradicting Proposition 3.2. □

Remark 3.6. Let F be a number field and E be a CM elliptic curve defined over F. Then, even when $K \not\subseteq F$, we have that $K \subseteq F(E[N])$ for every $N > 2$. This has been showed in [22, Lemma 6] for $F = \mathbb{Q}$ and in [4, Lemma 3.15] for arbitrary F. In particular, the statement of Theorem 1.1 does not hold when $K \not\subseteq F$.

The description of the set of primes S in Theorem 1.1 is actually redundant, since all the primes p dividing the conductor $\mathfrak{f}_O$, with the possible exception of $p = 2$, also divide the absolute discriminant Δ_F of the field of definition of E. This can be seen as follows: since $K \subseteq F$, the field F always contains the field $K(j(E))$, obtained by adjoining to K the j-invariant $j(E)$ of the elliptic curve E. Despite its definition, $H_O := K(j(E))$ does not depend on E but only on its CM order O, and is called the *ring class field* of K relative to the order O. The extension $K \subseteq H_O$ is always abelian and it is possibly ramified only at primes of K dividing the conductor $\mathfrak{f}_O$ (see [11, § 9.A]). If $O = O_K$, the field H_{O_K} coincides with the *Hilbert class field* of K, *i.e.* the maximal abelian extension of K which is unramified everywhere. The initial assertion now follows from the following proposition.

Proposition 3.7. *Let O be an order of conductor $\mathfrak{f}_O := |O_K : O|$ in an imaginary quadratic field K. Then the extension $\mathbb{Q} \subseteq H_O$ is ramified at all the odd primes dividing $\mathfrak{f}_O$. Moreover if $4 \mid \mathfrak{f}_O$ the same extension is also ramified at 2.*

Proof. If $\mathfrak{f}_O = 1$ there is nothing to prove. Otherwise let $\mathfrak{f}_O = p_1^{a_1} \cdots p_n^{a_n}$ be the prime factorisation of $\mathfrak{f}_O$, and observe that, for every $i \in \{1, \dots, n\}$, one has the chain of inclusions

$$K \subseteq H_{O_K} \subseteq H_{O_i} \subseteq H_O$$

given by the *Anordnungsatz* for ring class fields (see Remark A.3), where O_i denotes the order of conductor $p_i^{a_i}$. Now, the class number formula [11, Theorem 7.24] yields

$$[H_{O_i} : H_{O_K}] = \frac{[H_{O_i} : K]}{[H_{O_K} : K]} = \frac{h_{O_i}}{h_K} = \frac{p_i^{a_i}}{|O_K^\times : O_i^\times|} \left(1 - \left(\frac{\Delta_K}{p_i} \right) \frac{1}{p_i} \right). \tag{10}$$

where $h_{O_i} := [H_{O_i} : K] = |\mathrm{Pic}(O_i)|$ and analogously $h_K := [H_{O_K} : K] = |\mathrm{Pic}(O_K)|$. Since either $p_i \geq 3$ or $p_i = 2$ and $a_i \geq 2$, we see from (10) that $H_{O_i} \neq H_{O_K}$ except when $p_i = 3$, $a_i = 1$ and $K = \mathbb{Q}(\sqrt{-3})$. In this last case the extension $\mathbb{Q} \subseteq K$ is ramified at $p_i = 3$. Otherwise the extension $H_{O_K} \subsetneq H_{O_i}$ is ramified at some prime dividing p_i. Indeed, $H_{O_K} \subsetneq H_{O_i}$ is ramified at some prime because $K \subseteq H_{O_i}$ is abelian and H_{O_K} is the Hilbert class field of K, and this suffices to conclude because $K \subseteq H_{O_i}$ can ramify only at primes lying above p_i. □

Remark 3.8. If $2 \mid \mathfrak{f}_O$ but $4 \nmid \mathfrak{f}_O$ the extension $\mathbb{Q} \subseteq H_O$ could still be unramified at 2. This happens, for instance, if $\mathfrak{f}_O = 2$ and 2 splits in K, because in this case the ring class field H_O is equal to the Hilbert class field H_{O_K}.

Proposition 3.7 shows that the set S in Theorem 1.1 could be replaced by the set S' of primes dividing $2 \cdot \Delta_F \cdot \mathrm{N}_{F/\mathbb{Q}}(\mathfrak{f}_E)$, even if this results in a slightly weaker statement. However, choosing the set S' instead of the set S allows to draw a comparison with a result of Lombardo on the image of p-adic Galois representations attached to CM elliptic curves, which is shown in [16, Theorem 6.6]. In this paper Lombardo proves the isomorphism

$$\mathrm{Gal}(F(E[p^\infty])/F) \cong (O \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times$$

for every prime $p \nmid \Delta_F \cdot \mathrm{N}_{F/\mathbb{Q}}(\mathfrak{f}_E)$. If moreover $p \geq 3$, *i.e.* $p \notin S'$, this isomorphism follows also from Proposition 3.3 by taking inverse limits. The methods used in [16] are different from ours and generalise also to higher dimensional abelian varieties.

4. Minimality of division fields

We have seen in Proposition 3.3 that for every CM elliptic curve E defined over a number field F with $\mathrm{End}_F(E) \cong \mathcal{O}$ for some order $\mathcal{O}$ in an imaginary quadratic field $K \subseteq F$, the division fields $F(E[N])$ are *maximal* for all integers N coprime with a fixed integer $\mathfrak{b}_E \in \mathbb{N}$. This is to say that the associated Galois representation $\rho_{E,N}$ given by Lemma 3.1 is surjective. When E is defined over the ring class field $H_{\mathcal{O}}$ of K relative to $\mathcal{O}$, the division fields $H_{\mathcal{O}}(E[N])$ always contain a special abelian extension $H_{N,\mathcal{O}} \subseteq K^{\mathrm{ab}}$ called the *ray class field modulo N relative to the order $\mathcal{O}$*. If the division field $H_{\mathcal{O}}(E[N])$ is maximal and $N > 2$ then the containment $H_{N,\mathcal{O}} \subseteq H_{\mathcal{O}}(E[N])$ is strict. In this section we want to study for which integers N the division fields are *minimal*, in the sense that $H_{\mathcal{O}}(E[N]) = H_{N,\mathcal{O}}$. Theorem 4.3, which is the main result of Section 4, provides an explicit set of integers $N \in \mathbb{N}$ for which such an equality occurs. This will be used in Section 5 to detect entanglement in families of division fields. We point out that Theorem 4.3 is formulated in a wider setting, with the integer N replaced by a general invertible ideal $I \subseteq \mathcal{O}$. The study of the ray class fields $H_{I,\mathcal{O}}$ associated to these ideals is the content of Appendix A. We begin instead this section with a summary of some basic facts on lattices in number fields which will be used in the proof of Theorem 4.3. Our exposition follows [15, Chapter 8].

Let F be a number field. A *lattice* $\Lambda \subseteq F$ is an additive subgroup of F which is free of rank $[F : \mathbb{Q}]$ over $\mathbb{Z}$. Given a pair of lattices $\Lambda_1, \Lambda_2 \subseteq F$ we can form their sum $\Lambda_1 + \Lambda_2 \subseteq F$, their product $\Lambda_1 \cdot \Lambda_2 \subseteq F$ and their quotient $(\Lambda_1 \colon \Lambda_2) := \{x \in F \mid x \cdot \Lambda_2 \subseteq \Lambda_1\} \subseteq F$. Moreover, it is possible to define an action of the idèle group of F on the set $\{\Lambda \subseteq F : \Lambda \text{ lattice}\}$, as we are going to describe.

For a place $w \in M_F$ denote by F_w the completion of the number field F at w and by $\mathcal{O}_{F_w}$ its ring of integers. Let $\mathbb{A}_F$ be the *adèle ring* of F, defined by the restricted product

$$\mathbb{A}_F := \prod_{w \in M_F}{}' F_w = \left\{ s = (s_w)_{w \in M_F} \in \prod_{w \in M_F} F_w \;\middle|\; s_w \in \mathcal{O}_{F_w} \text{ for almost all } w \in M_F \right\}.$$

The discussion on [23, Page 371] shows that the adèle ring of F can be obtained from the rational adèle ring by extending scalars, *i.e.* there is a ring isomorphism $\mathbb{A}_F \cong \mathbb{A}_{\mathbb{Q}} \otimes_{\mathbb{Q}} F$. This enables us to talk, for a place $p \in M_{\mathbb{Q}}$, of the *p-component* $s_p \in F_p := \mathbb{Q}_p \otimes_{\mathbb{Q}} F$ of an adèle $s \in \mathbb{A}_F$; in particular if $p = \infty$ is the unique infinite place of $\mathbb{Q}$ we have the *infinity component* $s_\infty \in \mathbb{R} \otimes_{\mathbb{Q}} F$. Hence $s \in \mathbb{A}_F$ can be alternatively written as

$$s = (s_w)_{w \in M_F} \quad \text{or} \quad s = (s_p)_{p \in M_{\mathbb{Q}}} \tag{11}$$

and of course the same is true if $s \in \mathbb{A}_F^\times$ belongs to the *idèle group* $\mathbb{A}_F^\times$. In what follows, we will often confuse finite places $p \in M_{\mathbb{Q}}^0$ and rational primes $p \in \mathbb{N}$.

Now, for a lattice $\Lambda \subseteq F$ and a prime $p \in \mathbb{N}$, denote by $\Lambda_p := \Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_p$ the completion of the lattice Λ at p. Given an idèle $s = (s_p)_{p \in M_{\mathbb{Q}}} \in \mathbb{A}_F^\times$ there exists a unique lattice $s \cdot \Lambda \subseteq F$ with the property that $(s \cdot \Lambda)_p = s_p \cdot \Lambda_p$ for every prime $p \in \mathbb{N}$. This defines an action of the idèle group $\mathbb{A}_F^\times$ on the set of lattices in F, given by $(s, \Lambda) \mapsto s \cdot \Lambda$. We remark that the notation $s \cdot \Lambda$, although evocative of a multiplication between an idèle and a lattice, is purely formal and should not be confused with the notation $\Lambda_1 \cdot \Lambda_2$ for the usual product of lattices. Nevertheless, it is easy to see from the definitions that $(s \cdot \Lambda_1) \cdot \Lambda_2 = s \cdot (\Lambda_1 \cdot \Lambda_2)$ for every pair of lattices $\Lambda_1, \Lambda_2 \subseteq F$. Using the action just described, it is also possible to define a *multiplication by s* map $F/\Lambda \xrightarrow{s \cdot} F/(s \cdot \Lambda)$

by means of the following commutative diagram

$$\begin{tikzcd} \frac{F}{\Lambda} \arrow[r, "s\cdot"] \arrow[d, "\wr"'] & \frac{F}{s\cdot\Lambda} \arrow[d, "\wr"'] \\ \bigoplus_{p\in M_{\mathbb{Q}}^0} \frac{F_p}{\Lambda_p} \arrow[r, "(s_p\cdot)_p"] & \bigoplus_{p\in M_{\mathbb{Q}}^0} \frac{F_p}{s_p\Lambda_p} \end{tikzcd}$$

where the vertical maps are the obvious isomorphisms induced by the inclusions $F \hookrightarrow F_p$ and the bottom map is given by $(x_p)_p \mapsto (s_p\, x_p)_p$.

An essential ingredient in the proof of Theorem 4.3 is Theorem 4.1, which describes the action of complex automorphisms on torsion points of a CM elliptic curve in terms of its analytic parametrisation. The statement of the result involves the *global Artin map* and the notion of *Hecke character*. The first one is defined for every number field F and is a surjective, continuous group homomorphism $[\cdot, F] \colon \mathbb{A}_F^\times \twoheadrightarrow \mathrm{Gal}(F^{\mathrm{ab}}/F)$ such that $F^\times \cdot F_\infty^\times \subseteq \ker([\cdot, F])$, where $F^\times \subseteq \mathbb{A}_F^\times$ via the diagonal inclusion and $F_\infty^\times := \prod_{w|\infty} F_w^\times$ is the product of the unit groups of all the Archimedean completions of M (see [23, Chapter VI, § 5] and [2, Chapter IX]). Recall moreover that an *Hecke character* on a number field F is a continuous group homomorphism

$$\psi : \mathbb{A}_F^\times \to \mathbb{C}^\times$$

such that $\psi(F^\times) = 1$. Given a Hecke character ψ we denote by $\mathfrak{f}_\psi \subseteq \mathcal{O}_F$ its conductor, as defined in [13, Chapter 16, Definition 5.7]. For every place $w \in M_F$ we denote by $\psi_w \colon F_w^\times \to \mathbb{C}^\times$ the group homomorphism $\psi_w := \psi \circ \iota_w$, where $\iota_w \colon F_w^\times \hookrightarrow \mathbb{A}_F^\times$ is the natural inclusion. Similarly, for every rational prime $p \in \mathbb{N}$ we denote by $\psi_p \colon F_p^\times \to \mathbb{C}^\times$ the group homomorphism $\psi_p := \psi \circ \iota_p$ where $\iota_p \colon F_p^\times \hookrightarrow \mathbb{A}_F^\times$ is the analogous inclusion induced by the decomposition (11).

Theorem 4.1. *Let $F \subseteq \mathbb{C}$ be a number field, $E_{/F}$ be an elliptic curve such that $\mathrm{End}_F(E) \cong \mathcal{O}$ for some order $\mathcal{O}$ inside an imaginary quadratic field $K \subseteq F$. Let $K \subseteq M \subseteq F$ be a subfield such that $F(E_{tors}) \subseteq M^{ab} \cdot F$. Then there exist $[M^{ab} \cap F \colon M]$ group homomorphisms $\alpha \colon \mathbb{A}_M^\times \to K^\times \subseteq \mathbb{C}^\times$ such that:*

- *the map $\varphi \colon \mathbb{A}_M^\times \to \mathbb{C}^\times$ defined as $\varphi(s) := \alpha(s) \cdot \mathrm{N}_{M/K}(s)_\infty$ is a Hecke character, where $\mathrm{N}_{M/K} \colon \mathbb{A}_M^\times \to \mathbb{A}_K^\times$ is the idelic norm map described for example in [23, Chapter VI, § 2];*
- *for every lattice $\Lambda \subseteq K \subseteq \mathbb{C}$, every analytic isomorphism $\xi \colon \mathbb{C}/\Lambda \xrightarrow{\sim} E(\mathbb{C})$ and every $s \in M^\times \cdot \mathrm{N}_{F/M}(\mathbb{A}_F^\times) \subseteq \mathbb{A}_M^\times$ we have that $(\alpha(s) \cdot \mathrm{N}_{M/K}(s)^{-1}) \cdot \Lambda = \Lambda$ and the following diagram*

$$\begin{tikzcd} K/\Lambda \arrow[r, "(\alpha(s)\cdot \mathrm{N}_{M/K}(s)^{-1})\cdot"] \arrow[d, "\xi"'] & K/\Lambda \arrow[d, "\xi"] \\ E(M^{ab}\cdot F) \arrow[r, "\tau"'] & E(M^{ab}\cdot F) \end{tikzcd}$$

commutes, where $\tau \in \mathrm{Gal}(M^{ab}\cdot F/F)$ is the unique automorphism such that $\tau|_{M^{ab}} = [s, M]$.

Proof. Combine [28, Proposition 7.40] and [28, Proposition 7.41] when $M = F$ and use [28, Theorem 7.44] for the general case. Notice that, by class field theory, for every $s \in M^\times \cdot \mathrm{N}_{F/M}(\mathbb{A}_F^\times)$ the restriction $[s, M]|_{M^{\mathrm{ab}} \cap F}$ is trivial. This gives a unique $\tau \in \mathrm{Gal}(M^{\mathrm{ab}} \cdot F/F)$ such that $\tau|_{M^{\mathrm{ab}}} = [s, M]$. Moreover, fixing an embedding $F \subseteq \mathbb{C}$ automatically fixes an embedding $M^{\mathrm{ab}} \cdot F \subseteq \mathbb{C}$, hence $E(M^{\mathrm{ab}} \cdot F) \subseteq E(\mathbb{C})$, which gives a meaning to the vertical arrows in the diagram. □

Remark 4.2. If $K \subseteq M \subseteq M' \subseteq F$ and $F(E_{\mathrm{tors}}) \subseteq M^{\mathrm{ab}}$ then $M \subseteq F$ is abelian and Theorem 4.1 gives us $[M^{\mathrm{ab}} \cap F \colon M] = [F \colon M]$ Hecke characters $\varphi \colon \mathbb{A}_M^\times \to \mathbb{C}^\times$ and $[(M')^{\mathrm{ab}} \cap F \colon M'] = [F \colon M']$ Hecke characters $\widetilde{\varphi} \colon \mathbb{A}_{M'}^\times \to \mathbb{C}^\times$. We can observe that

$$\frac{[M^{\mathrm{ab}} \cap F \colon M]}{[(M')^{\mathrm{ab}} \cap F \colon M']} = \frac{[F \colon M]}{[F \colon M']} = [M' \colon M] \in \mathbb{N}$$

and that for every Hecke character $\widetilde{\varphi} \colon \mathbb{A}_{M'}^\times \to \mathbb{C}^\times$ given by Theorem 4.1 there are exactly $[M' \colon M]$ Hecke characters $\varphi \colon \mathbb{A}_M^\times \to \mathbb{C}^\times$ such that $\widetilde{\varphi} = \varphi \circ \mathrm{N}_{M'/M}$. If $K = M$ and $F = M'$ then we have a unique Hecke character $\widetilde{\varphi} \colon \mathbb{A}_F^\times \to \mathbb{C}^\times$ which coincides with the usual Hecke character associated to elliptic curves with complex multiplication, defined for example in [29, Chapter II, § 9] and [15, Chapter 10, Theorem 9].

We can now state the main theorem of this section, recalling that for every order $\mathcal{O}$ contained in an imaginary quadratic field K and every ideal $I \subseteq \mathcal{O}$ we denote by $H_{I,\mathcal{O}}$ the ray class field of K modulo I relative to the order $\mathcal{O}$, as defined in Appendix A.

Theorem 4.3. *Let $F \subseteq \mathbb{C}$ be a number field and let $E_{/F}$ be an elliptic curve such that $\mathrm{End}_F(E) \cong \mathcal{O}$ for some order $\mathcal{O}$ inside an imaginary quadratic field $K \subseteq F$. Suppose that $F(E_{tors}) \subseteq K^{ab}$. Let $H := H_{\mathcal{O}}$ the ring class field of $\mathcal{O}$, and fix $\alpha \colon \mathbb{A}_K^\times \to \mathbb{C}^\times$ as in Theorem 4.1, with $M = K$. Then we have that $F(E[I]) = F \cdot H_{I,\mathcal{O}}$ for every invertible ideal $I \subseteq \mathcal{O}$ such that $I \subseteq \mathfrak{f}_\varphi \cap \mathcal{O}$, where $\mathfrak{f}_\varphi \subseteq \mathcal{O}_K$ is the conductor of the Hecke character $\varphi \colon \mathbb{A}_K^\times \to \mathbb{C}^\times$ defined by $\varphi(s) := \alpha(s) \cdot s_\infty$.*

Proof. The containment $H_{I,\mathcal{O}} \subseteq F(E[I])$ is given by Theorem A.7. Observe moreover that $K \subseteq F$ is an abelian extension, since $F \subseteq F(E_{\mathrm{tors}}) \subseteq K^{\mathrm{ab}}$ by assumption. Hence to prove that $F(E[I]) \subseteq F \cdot H_{I,\mathcal{O}}$ it is sufficient to show that every I-torsion point of E is fixed by $[s, K]$, for any $s \in \mathbb{A}_K^\times$ such that $[s, K]\big|_{H_{I,\mathcal{O}}} = \mathrm{Id}$. Moreover, it suffices to consider only those $s \in \mathbb{A}_K^\times$ such that $s_\infty = 1$ and $s \in U_{I,\mathcal{O}}$, where $U_{I,\mathcal{O}} \leq \mathbb{A}_K^\times$ is the subgroup defined in (18). This follows from the fact that $[U_{I,\mathcal{O}}, K] = \mathrm{Gal}(K^{\mathrm{ab}}/H_{I,\mathcal{O}})$ and $K^\times \cdot K_\infty^\times \subseteq \ker([\cdot, K])$ where $K_\infty = \mathbb{C}$ is the completion of K at its unique Archimedean prime.

Fix then such an $s \in U_{I,\mathcal{O}}$ with $s_\infty = 1$. Notice that $s \in K^\times \cdot \mathrm{N}_{H/K}(\mathbb{A}_H^\times)$: indeed Remark A.3 gives the containment of fields $H \subseteq H_{I,\mathcal{O}}$, which implies that $[U_{I,\mathcal{O}}, K] \subseteq [\mathrm{N}_{H/K}(\mathbb{A}_H^\times), K]$. Hence

$$U_{I,\mathcal{O}} \subseteq \mathrm{N}_{H/K}(\mathbb{A}_H^\times) \cdot \ker([\cdot, K]) = \mathrm{N}_{H/K}(\mathbb{A}_H^\times) \cdot K^\times \cdot K_\infty^\times$$

which, combined with the fact that $s_\infty = 1$, implies that $s \in K^\times \cdot \mathrm{N}_{H/K}(\mathbb{A}_H^\times)$.

To study the action of $[s, K]$ on $E[I]$, we fix an invertible ideal $\mathfrak{a} \subseteq \mathcal{O} \subseteq \mathbb{C}$ and a complex uniformisation $\xi \colon \mathbb{C}/\mathfrak{a} \xrightarrow{\sim} E(\mathbb{C})$, which exists by [28, Proposition 4.8]. Take a torsion point $P \in E[I]$, and let $z \in (\mathfrak{a} \colon I)$ be any element such that $\xi(\overline{z}) = P$, where $\overline{z} \in (\mathfrak{a} \colon I)/\mathfrak{a}$ denotes the image of z in the quotient. Since $s \in K^\times \cdot \mathrm{N}_{H/K}(\mathbb{A}_H^\times)$, we have that

$$P^{[s,K]} = \xi(\overline{z})^{[s,K]} = \xi\left((\alpha(s)\, s^{-1}) \cdot \overline{z}\right)$$

which follows from applying Theorem 4.1 with $M = K$.

To conclude, it suffices to show that $s^{-1} \cdot \overline{z} = \overline{z}$ and $\alpha(s) = 1$. Notice that $s^{-1} \cdot \mathfrak{a} = \mathfrak{a}$ because $\mathfrak{a} \subseteq \mathcal{O}$ is invertible and $s_p \in \mathcal{O}_p^\times$ for every rational prime $p \in \mathbb{N}$. The equality $s^{-1} \cdot \overline{z} = \overline{z}$ then follows from the fact that, for every prime $p \in \mathbb{N}$, we have $s_p^{-1} z - z \in \mathfrak{a}_p$ because $z \in (\mathfrak{a} \colon I)$ and $s_p^{-1} \in 1 + I\,\mathcal{O}_p$. To prove the equality $\alpha(s) = 1$, notice that for every prime $p \in \mathbb{N}$ we have

$$1 + I\,\mathcal{O}_p \subseteq \prod_{\substack{w \mid p \\ w \in M_K^0}} (1 + \mathfrak{f}_\varphi\, \mathcal{O}_{K_w})$$

since $I \subseteq \mathfrak{f}_\varphi \cap \mathcal{O}$ by assumption. This implies that $\varphi_p(s_p) = 1$ for every prime $p \in \mathbb{N}$. Indeed $s_p \in 1 + I\,\mathcal{O}_p$ by the definition of $U_{I,\mathcal{O}}$ and for every $w \in M_K^0$ we have that $\varphi_w(1 + \mathfrak{f}_\varphi\, \mathcal{O}_{K_w}) = 1$

because $\mathfrak{f}_\varphi$ is the conductor of φ. Since $s_\infty = 1$ we get that $\alpha(s) = \varphi(s) = 1$, as was to be shown. □

Remark 4.4. Theorem 4.3 has been proved by Coates and Wiles (see [9, Lemma 3]) if $\mathcal{O} = \mathcal{O}_K$ is a maximal order of class number one. Their result has been generalised in the PhD thesis of Kuhman (see [14, Chapter II, Lemma 3]) to maximal orders $\mathcal{O} = \mathcal{O}_K$, under the hypothesis that $F \subseteq H_{I,\mathcal{O}_K}$.

Theorem 4.3 has a partial converse, as we show in the following proposition.

Proposition 4.5. *Let $\mathcal{O}$ be an order in an imaginary quadratic field K and $F \supseteq K$ be an abelian extension. Let $E_{/F}$ be an elliptic curve with complex multiplication by the order $\mathcal{O}$. Suppose that there exists an invertible ideal $I \subseteq \mathcal{O}$ such that $F(E[I]) = F \cdot H_{I,\mathcal{O}}$ and $I \cap \mathbb{Z} = N\mathbb{Z}$ with $N > 2$ if $j(E) \neq 0$ or $N > 3$ if $j(E) = 0$. Then $F(E_{tors}) = K^{ab}$.*

Proof. It is sufficient to prove that $F(E_{\text{tors}}) \subseteq K^{\text{ab}}$, since the other inclusion follows from the class field theory of imaginary quadratic fields and the fact that $K \subseteq F$ is abelian.

Fix an embedding $K \hookrightarrow \mathbb{C}$ and let $\xi : \mathbb{C}/\Lambda \xrightarrow{\sim} E(\mathbb{C})$ be a complex parametrization for E, where $\Lambda \subseteq K$ is a lattice. Take $\sigma \in \text{Aut}(\mathbb{C}/K^{\text{ab}})$. By [28, Theorem 5.4] with $s = 1$, there exists a complex parametrization $\xi' : \mathbb{C}/\Lambda \xrightarrow{\sim} E(\mathbb{C})$ such that the following diagram

$$\begin{tikzcd} E(\mathbb{C}) \arrow[rr, "\sigma"] & & E(\mathbb{C}) \\ & K/\Lambda \arrow[ul, "\xi"] \arrow[ur, "\xi'"'] & \end{tikzcd}$$

commutes. This means that σ acts on E_{tors} as an automorphism $\gamma = \xi' \circ \xi^{-1} \in \text{Aut}(E) \cong \mathcal{O}^\times$. In particular, for any point $P \in E[I]$ we have

$$\gamma(P) = \sigma(P) = P \tag{12}$$

since by assumption $F(E[I]) = F \cdot H_{I,\mathcal{O}} \subseteq K^{\text{ab}}$. Notice now that if $j(E) \neq 0, 1728$ we have $\text{Aut}(E) = \{\pm 1\}$ and equality (12) can occur for $\gamma = -1$ only when $I \cap \mathbb{Z} = 2\mathbb{Z}$. Similarly, if $j(E) = 1728$ or $j(E) = 0$ one sees that a non-trivial element of $\text{Aut}(E)$ can possibly fix only points of $E[2]$ or points of $E[2] \cup E[3]$, respectively. Our assumptions on I allow then to conclude that γ must be the identity on E.

We have shown that every complex automorphism which fixes the maximal abelian extension of K fixes also the torsion points of E. We conclude that $F(E_{\text{tors}}) \subseteq K^{\text{ab}}$ and this finishes the proof. □

We have seen that, for a CM elliptic curve E defined over an abelian extension F of the CM field K, having a minimal division field is essentially equivalent to the property that torsion points of E generate abelian extensions of K (and not only of F). It seems then natural to ask whether for a fixed order $\mathcal{O}$ in an imaginary quadratic field K there exists any elliptic curve E with complex multiplication by $\mathcal{O}$ and defined over the ring class field $H_\mathcal{O}$ (the smallest possible field of definition for E) with the property that $H_\mathcal{O}(E_{\text{tors}}) = K^{\text{ab}}$. This question is discussed by Shimura in [28, Page 217]. Here the author proves that, if $\mathcal{O} = \mathcal{O}_K$ is a maximal order whose discriminant is a square mod 3, then there exists an elliptic curve $E_{/H_\mathcal{O}}$ such that $H_\mathcal{O}(E_{\text{tors}}) = K^{\text{ab}}$. The next theorem generalises this result to arbitrary imaginary quadratic orders.

Theorem 4.6. *Let $\mathcal{O}$ be an order in an imaginary quadratic field K and let $j \in H_\mathcal{O}$ be the j-invariant of any elliptic curve with complex multiplication by $\mathcal{O}$. Then there exist infinitely many elliptic curves $E_{/H_\mathcal{O}}$ with $j(E) = j$ but non-isomorphic over $H_\mathcal{O}$, and such that $H_\mathcal{O}(E_{tors}) = K^{ab}$.*

Proof. When $\mathcal{O}$ has class number 1 the statement is trivially true. We may then assume that $\mathrm{Pic}(\mathcal{O}) \neq \{1\}$, and in particular that $j \neq 0, 1728$.

Let $E_{0/H_\mathcal{O}}$ be any elliptic curve with $j(E) = j$, and let $p \in \mathbb{N}$ be a prime satisfying

$\boxed{1}$ $p \equiv 3 \bmod 4$;

$\boxed{2}$ p does not divide $\mathfrak{f}_\mathcal{O} \cdot N_{H_\mathcal{O}/\mathbb{Q}}(\mathfrak{f}_{E_0})$, where $\mathfrak{f}_\mathcal{O} := |\mathcal{O}_K \colon \mathcal{O}|$ denotes the conductor of the order $\mathcal{O}$ and $\mathfrak{f}_{E_0} \subseteq \mathcal{O}_{H_\mathcal{O}}$ is the conductor ideal of the elliptic curve E_0;

$\boxed{3}$ p splits completely in K.

There are infinitely many such primes. Indeed, it clearly suffices to show that there are infinitely many primes satisfying conditions $\boxed{1}$ and $\boxed{3}$, which are equivalent to

$$\left(\frac{-4}{p}\right) = -1 \quad \text{and} \quad \left(\frac{\Delta_K}{p}\right) = 1$$

respectively; here $\Delta_K \in \mathbb{Z}$ denotes the absolute discriminant of the imaginary quadratic field K. The existence of an infinity of primes such that the above conditions hold then follows from Dirichlet's theorem on primes in arithmetic progression (see [23, Chapter VII, Theorem 5.14]), noticing that $\Delta_K \neq -4, -8$ by the assumption $\mathrm{Pic}(\mathcal{O}) \neq \{1\}$.

Let $\mathfrak{p} \subseteq \mathcal{O}$ be a prime ideal lying over p and note that $\mathfrak{p}$ is invertible by condition $\boxed{2}$. We define a new elliptic curve $E_\mathfrak{p}$ over $H_\mathcal{O}$ as follows: consider the division field $H_\mathcal{O}(E_0[\mathfrak{p}])$. By Proposition 3.3 there is an isomorphism

$$\mathrm{Gal}(H_\mathcal{O}(E_0[\mathfrak{p}])/H_\mathcal{O}) \cong (\mathcal{O}/\mathfrak{p}\mathcal{O})^\times \cong \mathbb{F}_p^\times$$

where the last isomorphism follows from the fact that p splits in K. In particular, the group $\mathrm{Gal}(H_\mathcal{O}(E_0[\mathfrak{p}])/H_\mathcal{O})$ is cyclic of order $p-1$, so $H_\mathcal{O} \subseteq H_\mathcal{O}(E_0[\mathfrak{p}])$ contains unique sub-extensions of degree $(p-1)/2$ and of degree 2 over $H_\mathcal{O}$. The first one is necessarily the ray class field $H_{\mathfrak{p},\mathcal{O}}$ (see Theorem A.7), the second one is of the form $H_\mathcal{O}(\sqrt{\alpha})$ for some element $\alpha = \alpha_\mathfrak{p} \in H_\mathcal{O}^\times$. By condition $\boxed{1}$, the integer $p-1$ is not divisible by 4, hence these two extensions must be linearly disjoint over $H_\mathcal{O}$. We deduce that $H_\mathcal{O}(E_0[\mathfrak{p}]) = H_{\mathfrak{p},\mathcal{O}}(\sqrt{\alpha})$. We set $E_\mathfrak{p} := E_0^{(\alpha)}$, where $E_0^{(\alpha)}$ denotes the twist of E_0 by $\alpha \in H_\mathcal{O}^\times$.

By Proposition 5.1, which will be proved in the next section, the Galois representation

$$\rho_{E_\mathfrak{p},\mathfrak{p}} : \mathrm{Gal}(H_\mathcal{O}(E_\mathfrak{p}[\mathfrak{p}])/H_\mathcal{O}) \hookrightarrow (\mathcal{O}/\mathfrak{p}\mathcal{O})^\times$$

is not surjective. This in particular implies that $H_\mathcal{O}(E_\mathfrak{p}[\mathfrak{p}]) = H_{\mathfrak{p},\mathcal{O}}$. It follows from Proposition 4.5 that $H_\mathcal{O}((E_\mathfrak{p})_{\text{tors}}) = K^{\text{ab}}$.

To conclude the proof, we want to show that the infinitely many elliptic curves $E_\mathfrak{p}$ with $\mathfrak{p} \subseteq \mathcal{O}$ chosen as above, are pairwise non-isomorphic over $H_\mathcal{O}$. To do so, it suffices to prove that the fields $H_\mathcal{O}(\sqrt{\alpha_\mathfrak{p}})$ associated to the quadratic twists are pairwise distinct. But this follows from Proposition 3.2 and Proposition 3.3, which show that the extension $H_\mathcal{O} \subseteq H_\mathcal{O}(\sqrt{\alpha_\mathfrak{p}})$ is ramified at all primes of $H_\mathcal{O}$ lying above $\mathfrak{p}$ and unramified at all primes of $H_\mathcal{O}$ which do not divide $\mathfrak{p} \cdot \mathfrak{f}_{E_\mathfrak{p}} \cdot \mathcal{O}_{H_\mathcal{O}}$, because $H_\mathcal{O}(\sqrt{\alpha_\mathfrak{p}}) \subseteq H_\mathcal{O}(E_0[\mathfrak{p}])$. This finishes the proof. □

We conclude this section by remarking that not all CM elliptic curves $E_{/H_\mathcal{O}}$ with $j(E) = j$ as in Theorem 4.6 have the property that $H_\mathcal{O}(E_{\text{tors}}) = K^{\text{ab}}$. This is already pointed out by Shimura in [28, Pages 217-218], where he shows that counterexamples can be obtained by twisting an elliptic curve $E_{/H_\mathcal{O}}$ with the desired property by an element $\alpha \in H_\mathcal{O}^\times$ whose square roots do not belong to K^{ab}.

5. Entanglement in the family of division fields of CM elliptic curves over $\mathbb{Q}$

Let $E_{/\mathbb{Q}}$ be an elliptic curve with complex multiplication by an order in an imaginary quadratic field K. The aim of this section is to explicitly determine the image of the natural map

$$\mathrm{Gal}(K(E_{\mathrm{tors}})/K) \hookrightarrow \prod_q \mathrm{Gal}(K(E[q^\infty])/K) \tag{13}$$

where the product runs over all rational primes $q \in \mathbb{N}$ and $K(E[q^\infty])$ denotes the compositum of the q-power division fields of $E_{/K}$. In other words, we want to analyse the entanglement in the family of Galois extensions $\{K(E[q^\infty])\}_q$ over K. The conclusion of this study will be Theorem 5.4, which provides a complete description of the image of (13) for all CM elliptic curves $E_{/\mathbb{Q}}$ such that $j(E) \notin \{0, 1728\}$.

Observe that there is essentially no difference in considering the division fields of the elliptic curve $E_{/\mathbb{Q}}$ and of its base change $E_{/K}$, because $\mathbb{Q}(E[n]) = K(E[n])$ for every $n > 2$ as explained in Remark 3.6. In particular, the family of division fields $\{\mathbb{Q}(E[q^\infty])\}_q$ is always entangled over $\mathbb{Q}$, but there are elliptic curves for which it is linearly disjoint over K, as we will see in Theorem 5.4.

We briefly outline the strategy of our proof: since E is defined over $\mathbb{Q}$ we have that $|\mathrm{Pic}(\mathcal{O})| = [\mathbb{Q}(j(E)) \colon \mathbb{Q}] = 1$ (see [11, Proposition 13.2]) which implies that the elliptic curve E has complex multiplication by one of the thirteen imaginary quadratic orders $\mathcal{O}$ of class number 1, listed in [11, Theorem 7.30]. For each of these orders $\mathcal{O}$, we first find an elliptic curve $E_{0/\mathbb{Q}}$ with complex multiplication by $\mathcal{O}$ such that $|\mathfrak{f}_{E_0}| \in \mathbb{N}$ is minimal among all the conductors[1] of elliptic curves defined over $\mathbb{Q}$ which have complex multiplication by $\mathcal{O}$. We then proceed to compute the full entanglement in the family of division fields of $E_{0/K}$, using Theorem 1.1, Theorem 4.3, and Proposition 5.2. Since $\mathcal{O}$ is an order of class number 1 and $j(E) \notin \{0, 1728\}$, we have that E is a quadratic twist of E_0. We then use Proposition 5.1, which describes how Galois representations attached to CM elliptic curves behave under quadratic twisting, to determine the complete entanglement in the family of division fields of $E_{/K}$.

In order to state Proposition 5.1 we introduce the following notation: given an elliptic curve E defined over a number field F and an element $\alpha \in F^\times$, we denote by $E^{(\alpha)}$ the *twist* of E by α, as described in [30, Chapter X, § 5]. We recall that two twists $E^{(\alpha)}$ and $E^{(\alpha')}$ are isomorphic over F if and only if α and α' represent the same class in $F^\times/(F^\times)^2$, *i.e.* if and only if $F(\sqrt{\alpha}) = F(\sqrt{\alpha'})$.

Proposition 5.1. *Let $\mathcal{O}$ be an order of discriminant $\Delta_{\mathcal{O}} < -4$ in an imaginary quadratic field K, and let $H_{\mathcal{O}}$ be the ring class field of K relative to the order $\mathcal{O}$. Consider an elliptic curve $E_{/H_{\mathcal{O}}}$ with complex multiplication by $\mathcal{O}$ and fix $\alpha \in H_{\mathcal{O}}^\times$. Then for every invertible ideal $I \subsetneq \mathcal{O}$ the surjectivity of the Galois representation $\rho_{E,I}$ defined in Lemma 3.1 determines the surjectivity of $\rho_{E^{(\alpha)},I}$ as follows:*

1. *if $\rho_{E,I}$ is surjective, then $\rho_{E^{(\alpha)},I}$ is surjective if and only if*
$$H_{\mathcal{O}}(E[I]) \neq H_{I,\mathcal{O}}(\sqrt{\alpha})$$
where $H_{I,\mathcal{O}}$ is the ray class field of K modulo I relative to $\mathcal{O}$, defined in Definition A.1;
2. *if $\rho_{E,I}$ is not surjective, then $\rho_{E^{(\alpha)},I}$ is surjective if and only if*
$$H_{\mathcal{O}}(E[I]) \cap H_{\mathcal{O}}(\sqrt{\alpha}) = H_{\mathcal{O}}.$$

Proof. First of all, observe that $\rho_{E,I}$ (respectively $\rho_{E^{(\alpha)},I}$) has maximal image if and only if there exists $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/H_{\mathcal{O}})$ such that $\rho_{E,I}(\sigma) = -1 \in (\mathcal{O}/I)^\times$ (respectively $\rho_{E^{(\alpha)},I}(\sigma) = -1$). Indeed, $H_{\mathcal{O}}(E[I])$ contains the ray class field $H_{I,\mathcal{O}}$, which is generated over $H_{\mathcal{O}}$ by the values of the Weber

[1] The symbol $|\mathfrak{f}_A| \in \mathbb{N}$ denotes the positive generator of the conductor ideal $\mathfrak{f}_A \subseteq \mathbb{Z}$ of an elliptic curve $A_{/\mathbb{Q}}$

function $\mathfrak{h}_E \colon E \twoheadrightarrow E/\mathrm{Aut}(E) \cong \mathbb{P}^1$ at I-torsion points (see Theorem A.7). Since $\mathfrak{h}_E([\varepsilon](P)) = \mathfrak{h}_E(P)$ for every $P \in E[I]$ and $\varepsilon \in \{\pm 1\} = \mathcal{O}^\times \cong \mathrm{Aut}(E)$, we see that $\rho_{E,I}$ induces the identification

$$\mathrm{Gal}(H_{\mathcal{O}}(E[I])/H_{I,\mathcal{O}}) \cong \mathrm{Im}(\pi_I^\times) \cap \mathrm{Im}(\rho_{E,I}) = \{\pm 1\} \cap \mathrm{Im}(\rho_{E,I}) \subseteq (\mathcal{O}/I)^\times \tag{14}$$

where $\pi_I^\times \colon \mathcal{O}^\times \longrightarrow (\mathcal{O}/I)^\times$ denotes the map induced by the quotient $\pi_I \colon \mathcal{O} \twoheadrightarrow \mathcal{O}/I$. Hence $\rho_{E,I}$ is surjective if and only if $-1 \in \mathrm{Im}(\rho_{E,I})$, and the same holds for $\rho_{E^{(\alpha)},I}$. Moreover $\rho_{E^{(\alpha)},I}$ is linked to $\rho_{E,I}$, after choosing compatible generators of $E[I]$ and $E^{(\alpha)}[I]$ as $\mathcal{O}/I$-modules, by the formula

$$\rho_{E^{(\alpha)},I} = \rho_{E,I} \cdot \chi_\alpha \tag{15}$$

where $\chi_\alpha \colon \mathrm{Gal}(\overline{\mathbb{Q}}/H_{\mathcal{O}}) \longrightarrow \{\pm 1\} \subseteq (\mathcal{O}/I)^\times$ is the quadratic character associated to $H_{\mathcal{O}}(\sqrt{\alpha})$.

To prove $\boxed{1}$ suppose that $\rho_{E,I}$ has maximal image. First, assume that $H_{\mathcal{O}}(E[I]) \neq H_{I,\mathcal{O}}(\sqrt{\alpha})$. Then, either $H_{\mathcal{O}}(\sqrt{\alpha}) \cap H_{\mathcal{O}}(E[I]) = H_{\mathcal{O}}$ or we have $H_{\mathcal{O}}(\sqrt{\alpha}) \subseteq H_{I,\mathcal{O}}$. In the first case, we can certainly find $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/H_{\mathcal{O}})$ acting trivially on $H_{\mathcal{O}}(\sqrt{\alpha})$ and such that $\rho_{E,I}(\sigma) = -1$. Hence we can use (15) to see that $\rho_{E^{(\alpha)},I}(\sigma) = \rho_{E,I}(\sigma) \cdot \chi_\alpha(\sigma) = -1$. This implies, by the initial discussion, that $\rho_{E^{(\alpha)},I}$ has maximal image. In the second case, any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/H_{\mathcal{O}})$ with $\rho_{E,I}(\sigma) = -1$ will act trivially on $H_{I,\mathcal{O}} \supseteq H_{\mathcal{O}}(\sqrt{\alpha})$ by (14). As before, we can use (15) to conclude that $\rho_{E^{(\alpha)},I}$ has maximal image.

Assume now that $H_{\mathcal{O}}(E[I]) = H_{I,\mathcal{O}}(\sqrt{\alpha})$. This implies that the extensions $H_{\mathcal{O}} \subseteq H_{\mathcal{O}}(\sqrt{\alpha})$ and $H_{\mathcal{O}} \subseteq H_{I,\mathcal{O}}$ are linearly disjoint over $H_{\mathcal{O}}$, because $\rho_{E,I}$ has maximal image. In particular

$$\mathrm{Gal}(H_{\mathcal{O}}(E[I])/H_{\mathcal{O}}) \cong \mathrm{Gal}(H_{I,\mathcal{O}}/H_{\mathcal{O}}) \times \mathrm{Gal}(H_{\mathcal{O}}(\sqrt{\alpha})/H_{\mathcal{O}}).$$

We deduce that any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/H_{\mathcal{O}})$ with $\rho_{E,I}(\sigma) = -1$, being the identity on $H_{I,\mathcal{O}}$ by (14), must act non-trivially on $H_{\mathcal{O}}(\sqrt{\alpha})$. Then (15) gives

$$\rho_{E^{(\alpha)},I}(\sigma) = \rho_{E,I}(\sigma) \cdot \chi_\alpha(\sigma) = 1$$

and this suffices to see that $\rho_{E^{(\alpha)},I}$ is non-maximal. This concludes the proof of $\boxed{1}$.

The proof of $\boxed{2}$ can be carried out in a similar fashion. First of all, notice that the non-maximality of $\rho_{E,I}$ and (14) imply that $H_{I,\mathcal{O}} = H_{\mathcal{O}}(E[I])$. Now, by (15) the only possibility for $\rho_{E^{(\alpha)},I}$ to be surjective in this case is to find an automorphism $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/H_{\mathcal{O}})$ with $\rho_{E,I}(\sigma) = 1$ and $\chi_\alpha(\sigma) = -1$, which is clearly impossible if $H_{\mathcal{O}}(\sqrt{\alpha}) \subseteq H_{\mathcal{O}}(E[I]) = H_{I,\mathcal{O}}$. On the other hand, if $H_{\mathcal{O}}(E[I]) \cap H_{\mathcal{O}}(\sqrt{\alpha}) = H_{\mathcal{O}}$ one can certainly find $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/H_{\mathcal{O}})$ such that $\chi_\alpha(\sigma) = -1$ and $\rho_{E,I}(\sigma) = 1$, which shows by (15) that $\rho_{E^{(\alpha)},I}$ has maximal image. ◻

We want now to derive some consequences of Proposition 5.1 when $\mathrm{Pic}(\mathcal{O}) = 1$, $\alpha \in \mathbb{Q}^\times$ and the elliptic curve $E_{/K}$ is the base change to the imaginary quadratic field $K = H_{\mathcal{O}}$ of an elliptic curve defined over $\mathbb{Q}$. To do this, we need a formula originally due to Deuring that relates the conductor of a CM elliptic curve defined over $\mathbb{Q}$ to the conductor of the unique Hecke character $\varphi \colon \mathbb{A}_K^\times \longrightarrow \mathbb{C}^\times$ associated to its base change over K by Theorem 4.1.

Proposition 5.2 (Deuring). *Let $\mathcal{O} \subseteq K$ be an order inside an imaginary quadratic field K. Let E be an elliptic curve defined over $\mathbb{Q}(j(E))$ with complex multiplication by $\mathcal{O}$. Denote by $\varphi \colon \mathbb{A}_{H_{\mathcal{O}}}^\times \longrightarrow \mathbb{C}^\times$ the unique Hecke character associated by Theorem 4.1 to the base change of E over $K(j(E)) = H_{\mathcal{O}}$. Then, letting $j = j(E)$, one can write the conductor $\mathfrak{f}_E \subseteq \mathcal{O}_{\mathbb{Q}(j)}$ of E as*

$$\mathfrak{f}_E = \mathrm{N}_{K(j)/\mathbb{Q}(j)}(\mathfrak{f}_\varphi) \cdot \delta_{K(j)/\mathbb{Q}(j)}$$

where $\mathrm{N}_{K(j)/\mathbb{Q}(j)}(\mathfrak{f}_\varphi) \subseteq \mathcal{O}_{\mathbb{Q}(j)}$ denotes the relative norm of the conductor $\mathfrak{f}_\varphi \subseteq \mathcal{O}_{K(j)}$ of the Hecke character φ and $\delta_{K(j)/\mathbb{Q}(j)} \subseteq \mathcal{O}_{\mathbb{Q}(j)}$ denotes the relative discriminant ideal associated to the quadratic extension $\mathbb{Q}(j) \subseteq K(j)$.

Proof. A modern proof of this formula can be obtained using [21, Theorem 3] and [26, Theorem 12]. This is detailed in [24, Appendix A]. ◻

We go back to study the consequences of Proposition 5.1. Let $E_{/K}$ be the base change to an imaginary quadratic field $K = H_{\mathcal{O}}$ of an elliptic curve $E_{/\mathbb{Q}}$ of conductor $\mathfrak{f}_E \subseteq \mathbb{Z}$ and with complex multiplication by an order $\mathcal{O}$ of class number one and discriminant $\Delta_{\mathcal{O}} < -4$. Fix also $\alpha \in \mathbb{Q}^\times$. Under these assumptions we may assume that $\alpha = \Delta$ where $\Delta = \Delta_F \in \mathbb{Z}$ is the fundamental discriminant associated to some quadratic extension $\mathbb{Q} \subseteq F$. Since $E^{(\alpha\beta)} = (E^{(\alpha)})^{(\beta)}$ for any $\alpha, \beta \in \mathbb{Q}^\times$, we reduce the study of the Galois representation $\rho_{E^{(\Delta)},p^n}$ for any prime $p \in \mathbb{Z}_{\geq 1}$ and any $n \in \mathbb{N}$ to the following cases:

$\boxed{\text{T.1}}$ $\Delta = (-1)^{(q-1)/2}\, q$ for some prime $q \in \mathbb{Z}_{\geq 3}$ with $q \nmid p\, \mathfrak{f}_E$. In this case $K(\sqrt{\Delta}) \cap K(E[p^n]) = K$. Indeed any prime $\mathfrak{q} \subseteq \mathcal{O}_K$ such that $\mathfrak{q} \mid q\mathcal{O}_K$ does not ramify in $K \subseteq K(E[p^n])$, as follows from Proposition 3.2 because $q \nmid p\, \mathfrak{f}_E$. On the other hand, any prime $\mathfrak{q} \mid q\mathcal{O}_K$ ramifies in $K \subseteq K(\sqrt{\Delta})$ since Proposition 5.2 shows that $q \nmid \Delta_K$, where $\Delta_K \in \mathbb{Z}_{<0}$ denotes the absolute discriminant of the imaginary quadratic field K. Thus Proposition 5.1 implies that $\rho_{E^{(\Delta)},p^n}$ will have maximal image independently from the behaviour of ρ_{E,p^n};

$\boxed{\text{T.2}}$ $p \geq 3$ and $\Delta = (-1)^{(p-1)/2}\, p$. In this case class field theory shows that

$$\mathbb{Q}(\sqrt{\Delta}) \subseteq \mathbb{Q}(\mu_p) \subseteq H_{p^n,\mathcal{O}}$$

where for every $m \in \mathbb{N}$ we let $\mu_m \subseteq \overline{\mathbb{Q}}$ denote the group of m-th roots of unity. Hence Proposition 5.1 implies that $\rho_{E^{(\Delta)},p^n}$ has maximal image if and only if ρ_{E,p^n} does;

$\boxed{\text{T.3}}$ $\Delta \in \{-4, -8, 8\}$ and $2 \nmid p\, \mathfrak{f}_E$. In this case $K(\sqrt{\Delta}) \cap K(E[p^n]) = K$, as in $\boxed{\text{T.1}}$, hence Proposition 5.1 shows that $\rho_{E^{(\Delta)},p^n}$ will have maximal image independently from the behaviour of ρ_{E,p^n};

$\boxed{\text{T.4}}$ $\Delta \in \{-4, -8, 8\}$ and $p = 2$. In this case $\mathbb{Q}(\sqrt{\Delta}) \subseteq \mathbb{Q}(\mu_{|\Delta|}) \subseteq H_{|\Delta|,\mathcal{O}}$ by class field theory. Hence Proposition 5.1 implies that for every $n \in \mathbb{N}$ such that $2^n \geq |\Delta|$ the representation $\rho_{E^{(\Delta)},2^n}$ has maximal image if and only if $\rho_{E,2^n}$ does, similarly to what we proved in $\boxed{\text{T.2}}$.

Remark 5.3. The previous discussion shows in particular that, under suitable hypotheses on Δ, if the Galois representation ρ_{E,p^n} is surjective then $\rho_{E^{(\Delta)},p^n}$ is surjective. This might not be the case if these assumptions on Δ are not satisfied, as it follows from Theorem 5.4.

We are now ready to study the entanglement of division fields of CM elliptic curves E defined over $\mathbb{Q}$ such that $j(E) \notin \{0, 1728\}$.

First of all, assume that E has complex multiplication by an order $\mathcal{O}$ with $\gcd(\Delta_{\mathcal{O}}, 6) = 1$. Here $\Delta_{\mathcal{O}} := \mathfrak{f}_{\mathcal{O}}^2 \Delta_K$ denotes the discriminant of $\mathcal{O}$, where $\Delta_K \in \mathbb{Z}$ denotes the absolute discriminant of K and $\mathfrak{f}_{\mathcal{O}} := [\mathcal{O}_K \colon \mathcal{O}]$ denotes the conductor of $\mathcal{O}$. Since $\operatorname{Pic}(\mathcal{O}) = \{1\}$ we have that $\mathcal{O} = \mathcal{O}_K$ and $\Delta_{\mathcal{O}} = \Delta_K = -p$ where $p \in \mathbb{N}$ is a prime number such that $p \geq 7$ and $p \equiv 3 \bmod 4$ (see [11, Theorem 7.30]). Moreover $E = E_0^{(\Delta)}$ for some fundamental discriminant $\Delta \in \mathbb{Z}$, where E_0 is one of the two elliptic curves with $j(E_0) = j(E)$ appearing in Table 1, which lists the CM elliptic curves defined over $\mathbb{Q}$ whose conductor $|\mathfrak{f}_E| \in \mathbb{N}$ is minimal among their twists.

Let us study the division fields of E_0, as a first step towards the analysis of the division fields of E. Theorem 1.1 provides a decomposition

$$\operatorname{Gal}(K((E_0)_{\text{tors}})/K) \cong \prod_q \operatorname{Gal}(K(E_0[q^\infty])/K) \tag{16}$$

where the product runs over all the rational primes $q \in \mathbb{N}$. Indeed in this case the set S_{E_0} appearing in Theorem 1.1 consists of the single prime p because $|\mathfrak{f}_{E_0}| = p^2$ as follows from an inspection of Table 1. The isomorphism (16) shows that the family of division fields $\{K(E_0[q^\infty])\}_q$ is linearly disjoint over K, where $q \in \mathbb{N}$ runs over all the rational primes. Proposition 3.3 implies also that $\operatorname{Gal}(K(E_0[q^m])/K) \cong (\mathcal{O}/q^m\mathcal{O})^\times$ for every prime $q \neq p$ and every $m \in \mathbb{N}$. On the other hand we have that $\operatorname{Gal}(K(E_0[p^m])/K) \cong (\mathcal{O}/p^m\mathcal{O})^\times/\{\pm 1\}$ for every $m \in \mathbb{N}$. Indeed, it follows from

Δ_K	$\mathfrak{f}_{\mathcal{O}}$	$j(E)$	$\lvert\mathfrak{f}_E\rvert$	Equations
-3	1	0	3^3	$y^2 + y = x^3 - 7$ $y^2 + y = x^3$
	2	$2^4\,3^3\,5^3$	$2^2 3^2$	$y^2 = x^3 - 15x + 22$ $y^2 = x^3 - 135x - 594$
	3	$-2^{15}\,3\,5^3$	3^3	$y^2 + y = x^3 - 30x + 63$ $y^2 + y = x^3 - 270x - 1708$
-4	1	$2^6\,3^3$	2^5	$y^2 = x^3 - x$ $y^2 = x^3 + 4x$
	2	$2^3\,3^3\,11^3$	2^5	$y^2 = x^3 - 11x - 14$ $y^2 = x^3 - 11x + 14$
-7	1	$-3^3\,5^3$	7^2	$y^2 + xy = x^3 - x^2 - 2x - 1$ $y^2 + xy = x^3 - x^2 - 107x + 552$
	2	$3^3\,5^3\,17^3$	7^2	$y^2 + xy = x^3 - x^2 - 37x - 78$ $y^2 + xy = x^3 - x^2 - 1822x + 30393$
-8	1	$2^6\,5^3$	2^8	$y^2 = x^3 - x^2 - 3x - 1$ $y^2 = x^3 + x^2 - 3x + 1$ $y^2 = x^3 - x^2 - 13x + 21$ $y^2 = x^3 + x^2 - 13x - 21$
-11	1	-2^{15}	11^2	$y^2 + y = x^3 - x^2 - 7x + 10$ $y^2 + y = x^3 - x^2 - 887x - 10143$
-19	1	$-2^{15}\,3^3$	19^2	$y^2 + y = x^3 - 38x + 90$ $y^2 + y = x^3 - 13718x - 619025$
-43	1	$-2^{18}\,3^3\,5^3$	43^2	$y^2 + y = x^3 - 860x + 9707$ $y^2 + y = x^3 - 1590140x - 771794326$
-67	1	$-2^{15}\,3^3\,5^3\,11^3$	67^2	$y^2 + y = x^3 - 7370x + 243528$ $y^2 + y = x^3 - 33083930x - 73244287055$
-163	1	$-2^{18}\,3^3\,5^3\,23^3\,29^3$	163^2	$y^2 + y = x^3 - 2174420x + 1234136692$ $y^2 + y = x^3 - 57772164980x - 5344733777551611$

Table 1. Minimal Weierstrass equations of CM elliptic curves defined over $\mathbb{Q}$ having the smallest conductor $\lvert\mathfrak{f}_E\rvert$ amongst all their twists, where $\lvert\mathfrak{f}_E\rvert \in \mathbb{N}$ denotes the unique positive generator of the conductor ideal $\mathfrak{f}_E \subseteq \mathbb{Z}$.

Proposition 5.2 that $\mathfrak{f}_{\varphi_0} = \mathfrak{p}$, where $\mathfrak{p} \subseteq \mathcal{O}$ is the unique prime lying above p and $\varphi_0 \colon \mathbb{A}_K^\times \to \mathbb{C}^\times$ is the unique Hecke character associated to E_0 by Theorem 4.1. Hence Theorem 4.3 shows that $K(E_0[p^m]) = H_{p^m,\mathcal{O}}$ for every $m \in \mathbb{N}$, where $H_{p^m,\mathcal{O}}$ is the ray class field of K modulo p^m because $\mathcal{O} = \mathcal{O}_K$. Hence we can conclude that $\mathrm{Gal}(K(E_0[p^m])/K) \cong (\mathcal{O}/p^m\mathcal{O})^\times/\{\pm 1\}$ using Theorem A.6.

Let us now go back to the division fields of $E = E_0^{(\Delta)}$. We can assume that $p \nmid \Delta$ because otherwise $\Delta = -p\,\Delta'$ for some fundamental discriminant $\Delta' \in \mathbb{Z}$, hence $E \cong_K E_0^{(\Delta')}$ since $\sqrt{-p} \in K$. Here the symbol $\cong_K$ means that the two elliptic curves E and $E_0^{(\Delta')}$, which are defined over $\mathbb{Q}$, become isomorphic when base-changed to K. Observe that $\lvert\mathfrak{f}_E\rvert = (p\,\Delta)^2$, which follows from

(15) and [36, § 10, Proposition 1] because $|\mathfrak{f}_{E_0}|$ is coprime with Δ. Now, Theorem 1.1 gives

$$\operatorname{Gal}(K(E_{\text{tors}})/K) \cong \left(\prod_{q \notin S} \operatorname{Gal}(K(E[q^\infty])/K) \right) \times \operatorname{Gal}(K(E[S^\infty])/K)$$

with the product running over the rational primes $q \in \mathbb{N}$ such that $q \notin S$, where in this case the finite set $S = S_E \subseteq \mathbb{N}$ appearing in Theorem 1.1 consists uniquely of the primes dividing $|\mathfrak{f}_E| = (p\,\Delta)^2$. Moreover, $\operatorname{Gal}(K(E[\ell^m])/K) \cong (\mathcal{O}/\ell^m\mathcal{O})^\times$ for every prime $\ell \in \mathbb{N}$ and every $m \in \mathbb{N}$, since T.1 and T.3 show that for every $m \in \mathbb{N}$ the Galois representation ρ_{E,ℓ^m} has maximal image. On the other hand, Proposition 5.1 shows that $K(E[p^m]) = H_{p^m,\mathcal{O}}(\sqrt{\Delta})$ and

$$K(E[p^m]) \cap K(E[\Delta]) = K(\sqrt{\Delta})$$

for every $m \in \mathbb{Z}_{\geq 1}$. Hence the family of division fields $\{K(E[q^\infty])\}_{q \in S}$ is entangled over K, and for every collection of integers $\{a_q\}_{q \in S} \subseteq \mathbb{Z}_{\geq 1}$ we get

$$\operatorname{Gal}(L/K) \cong \frac{\prod_{q \in S} (\mathcal{O}/q^{a_q}\mathcal{O})^\times}{\{\pm 1\}}$$

where L is the compositum of all the division fields $K(E[q^{a_q}])$ for $q \in S$.

Let us now consider orders $\mathcal{O}$ such that $\gcd(\Delta_{\mathcal{O}}, 6) \neq 1$. The analysis of the division fields of an elliptic curve $E_{/\mathbb{Q}}$ having complex multiplication by $\mathcal{O}$ proceeds similarly to what happened before, with the only exception of the order $\mathcal{O} = \mathbb{Z}[\sqrt{-3}]$. Indeed if

$$\mathcal{O} \in \{\mathbb{Z}[3\zeta_3], \mathbb{Z}[2i], \mathbb{Z}[\sqrt{-2}], \mathbb{Z}[\sqrt{-7}]\}$$

where $\zeta_3 := (-1 + \sqrt{-3})/2$ and $i := \sqrt{-1}$, then all the elliptic curves E_0 appearing in Table 1 with complex multiplication by $\mathcal{O}$ share the property that $|\mathfrak{f}_{E_0}|$ is a power of the unique rational prime $p \in \mathbb{N}$ which ramifies in the quadratic extension $\mathbb{Q} \subseteq K$. Hence Theorem 1.1 provides a decomposition

$$\operatorname{Gal}(K((E_0)_{\text{tors}})/K) \cong \prod_q \operatorname{Gal}(K(E_0[q^\infty])/K)$$

where the product runs over all rational primes $q \in \mathbb{N}$, because in this case the finite set $S_{E_0} \subseteq \mathbb{N}$ appearing in Theorem 1.1 consists of the single prime p. This shows that the division fields of E_0 are linearly disjoint over K. Moreover, Proposition 3.3 implies that $\operatorname{Gal}(K(E_0[q^m])/K) \cong (\mathcal{O}/q^m\mathcal{O})^\times$ for every rational prime $q \neq p$ and every $m \in \mathbb{N}$. On the other hand, Proposition 5.2 shows that $\mathfrak{f}_{\varphi_0} = \mathfrak{p}^k$ is a power of the unique prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ lying over p, with $k \leq 2$ if $\mathcal{O} \notin \{\mathbb{Z}[2i], \mathbb{Z}[\sqrt{-2}]\}$ and $k \leq 6$ otherwise. Hence Theorem 4.3 and Theorem A.6 give $\operatorname{Gal}(K(E_0[p^m])/K) \cong (\mathcal{O}/p^m)^\times/\{\pm 1\}$ for every $m \in \mathbb{N}$ such that $m \geq 1$ if $\mathcal{O} \notin \{\mathbb{Z}[2i], \mathbb{Z}[\sqrt{-2}]\}$ and $m \geq 3$ otherwise.

Let now $E_{/\mathbb{Q}}$ be any elliptic curve with complex multiplication by $\mathcal{O}$. Since $j(E) = j(E_0) \notin \{0, 1728\}$ we know that $E = E_0^{(\Delta)}$ for some fundamental discriminant $\Delta \in \mathbb{Z}$. If $\mathcal{O} = \mathbb{Z}[3\zeta_3]$ or $\mathcal{O} = \mathbb{Z}[\sqrt{-7}]$ we can assume that $p \nmid \Delta$ because $\sqrt{-p} \in K$. Hence Theorem 1.1 shows that

$$\operatorname{Gal}(K(E_{\text{tors}})/K) \cong \left(\prod_{q \notin S} \operatorname{Gal}(K(E[q^\infty])/K) \right) \times \operatorname{Gal}(K(E[S^\infty])/K)$$

with the product running over the rational primes $q \in \mathbb{N}$ such that $q \notin S$, where in this case the finite set $S = S_E \subseteq \mathbb{N}$ appearing in Theorem 1.1 consists uniquely of the primes dividing $|\mathfrak{f}_E| = (p\,\Delta)^2$. Exactly as before T.1 and T.3 show that $\operatorname{Gal}(K(E[\ell^m])/K) \cong (\mathcal{O}/\ell^m\mathcal{O})^\times$ for every prime $\ell \in \mathbb{N}$ and every $m \in \mathbb{N}$. Moreover, Proposition 5.1 shows that $K(E[p^m]) = H_{p^m,\mathcal{O}}(\sqrt{\Delta})$

and $K(E[p^m]) \cap K(E[\Delta]) = K(\sqrt{\Delta})$ for every $m \in \mathbb{Z}_{\geq 1}$. Hence the family of division fields $\{K(E[q^\infty])\}_{q \in S}$ is entangled over K, and for every collection of integers $\{a_q\}_{q \in S} \subseteq \mathbb{Z}_{\geq 1}$ we get

$$\mathrm{Gal}(L/K) \cong \frac{\prod_{q \in S} (\mathcal{O}/q^{a_q}\mathcal{O})^\times}{\{\pm 1\}}$$

where L is the compositum of all the division fields $K(E[q^{a_q}])$ for $q \in S$.

Studying the entanglement in the family of division fields of E becomes slightly more complicated if $\mathcal{O} \in \{\mathbb{Z}[2i], \mathbb{Z}[\sqrt{-2}]\}$. First of all, note that there exists a unique $\Delta_2 \in \{1, -4, -8, 8\}$ such that $\Delta = \Delta_2 \, \Delta'$ where $\Delta' \in \mathbb{Z}$ is an odd fundamental discriminant. We can now write $E = E_1^{(\Delta')}$ where $E_1 := E_0^{(\Delta_2)}$. One can check that if $\mathcal{O} = \mathbb{Z}[\sqrt{-2}]$ then E_1 is isomorphic to one of the four elliptic curves with complex multiplication by $\mathbb{Z}[\sqrt{-2}]$ appearing in Table 1. On the other hand, if $\mathcal{O} = \mathbb{Z}[2i]$ then E_1 can be either one of the two elliptic curves

$$y^2 = x^3 - 44x - 112$$
$$y^2 = x^3 - 44x + 112$$

or one of the two elliptic curves with complex multiplication by $\mathbb{Z}[2i]$ appearing in Table 1. In each case it is not difficult to see that $|\mathfrak{f}_{E_1}| \in \mathbb{N}$ is a power of 2, which shows that the division fields of E_1 behave similarly to the division fields of E_0. More precisely, Theorem 1.1 gives

$$\mathrm{Gal}(K((E_1)_{\mathrm{tors}})/K) \cong \prod_q \mathrm{Gal}(K(E_1[q^\infty])/K)$$

where the product runs over all the rational primes $q \in \mathbb{N}$. This shows that the division fields of E_1 are linearly disjoint over K. Moreover, Proposition 3.3 shows that $\mathrm{Gal}(K(E_1[q^m])/K) \cong (\mathcal{O}/q^m\mathcal{O})^\times$ for every rational prime $q \geq 3$ and every $m \in \mathbb{N}$, and a combination of Proposition 5.2 and Theorem 4.3 gives $\mathrm{Gal}(K(E_1[2^m])/K) \cong (\mathcal{O}/2^m\mathcal{O})^\times/\{\pm 1\}$ for every $m \in \mathbb{N}$ such that $m \geq 3$. This concludes the analysis of the division fields of $E = E_1$ if $\Delta' = 1$. On the other hand, if $\Delta' \neq 1$ then $|\mathfrak{f}_E| = |\mathfrak{f}_{E_1}| \, (\Delta')^2$ where $|\mathfrak{f}_{E_1}|$ is a power of 2. Hence Theorem 1.1 shows that

$$\mathrm{Gal}(K(E_{\mathrm{tors}})/K) \cong \left(\prod_{q \notin S} \mathrm{Gal}(K(E[q^\infty])/K) \right) \times \mathrm{Gal}(K(E[S^\infty])/K)$$

with the product running over the rational primes $q \in \mathbb{N}$ such that $q \notin S$ where $S = S_E$ denotes the finite set appearing in Theorem 1.1, which in this case consists of the primes dividing $2 \cdot \Delta'$. Similarly to what happened before, T.1 and T.4 show that $\mathrm{Gal}(K(E[\ell^m])/K) \cong (\mathcal{O}/\ell^m\mathcal{O})^\times$ for every prime $\ell \in \mathbb{N}$ and every $m \in \mathbb{N}$. Moreover, Proposition 5.1 gives $K(E[2^m]) = H_{2^m,\mathcal{O}}(\sqrt{\Delta'})$ and $K(E[2^m]) \cap K(E[\Delta']) = K(\sqrt{\Delta'})$ for every $m \geq 3$. Hence the family of division fields $\{K(E[q^\infty])\}_{q \in S}$ is entangled over K, and for all $\{a_q\}_{q \in S} \subseteq \mathbb{Z}_{\geq 1}$ with $a_2 \geq 3$ we get

$$\mathrm{Gal}(L/K) \cong \frac{\prod_{q \in S} (\mathcal{O}/q^{a_q}\mathcal{O})^\times}{\{\pm 1\}}$$

where L is the compositum of all the division fields $K(E[q^{a_q}])$ for $q \in S$.

We are left with the analysis of the entanglement between the division fields of an elliptic curve E defined over $\mathbb{Q}$ which has complex multiplication by $\mathcal{O} = \mathbb{Z}[\sqrt{-3}]$. As usual $E = E_0^{(\Delta)}$ for some fundamental discriminant $\Delta \in \mathbb{Z}$, where E_0 is one of the two elliptic curves with complex multiplication by $\mathbb{Z}[\sqrt{-3}]$ appearing in Table 1. In contrast to what we have seen before, here $|\mathfrak{f}_{E_0}| = 2^2 \, 3^2$ is not a prime power. This forces us to study separately the division fields $K(E_0[2^\infty])$ and $K(E_0[3^\infty])$. First of all, one can compute that for any of the two possibilities for E_0, given by the Weierstrass equations $y^2 = x^3 - 15x + 22$ and $y^2 = x^3 - 135x - 594$, the representation $\rho_{E_0,3}$ is not surjective, *i.e.* $K(E_0[3]) = H_{3,\mathcal{O}} = K(\sqrt[3]{2})$. This clearly shows that $\rho_{E_0,3^n}$ is not surjective for every $n \in \mathbb{Z}_{\geq 1}$. Moreover, $\rho_{E_0,2^n}$ is surjective for every $n \in \mathbb{Z}_{\geq 1}$. Indeed Theorem A.6 and Theorem A.7 imply that

$$\left|\left(\frac{\mathcal{O}}{2^n\mathcal{O}}\right)^\times\right| = \frac{[H_{2^n 3,\mathcal{O}} \colon K]}{[H_{3,\mathcal{O}} \colon K]} = \frac{[H_{2^n 3,\mathcal{O}} \colon K]}{[K(E_0[3]) \colon K]} \leq \frac{[K(E_0[2^n 3]) \colon K]}{[K(E_0[3]) \colon K]} \leq [K(E_0[2^n]) \colon K]$$

hence Lemma 3.1 shows that every inequality is actually an equality, and $\rho_{E_0,2^n}$ is surjective. This gives that $K(E_0[2^n]) \cap K(E_0[3^m]) = K$ for every $n, m \in \mathbb{Z}_{\geq 1}$. These considerations together with Theorem 1.1 and Proposition 3.3 give a decomposition

$$\operatorname{Gal}(K((E_0)_{\mathrm{tors}})/K) \cong \prod_q \operatorname{Gal}(K(E_0[q^\infty])/K)$$

where the product runs over all rational primes $q \in \mathbb{N}$. Moreover, for every $m \in \mathbb{N}$ we get

$$\operatorname{Gal}(K(E_0[q^m])/K) \cong \begin{cases} (\mathcal{O}/q^m\mathcal{O})^\times, \text{ if } q \neq 3 \\ (\mathcal{O}/3^m\mathcal{O})^\times/\{\pm 1\}, \text{ if } q = 3 \end{cases}$$

and the family of division fields $\{K(E[q^\infty])\}_q$ is linearly disjoint over K.

Let us go back to the division fields of $E = E_0^{(\Delta)}$, where we can assume that $3 \nmid \Delta$ because $\sqrt{-3} \in K$. Write now $\Delta = \Delta_2 \Delta'$ as above, where $\Delta_2 \in \{1, -4, -8, 8\}$ and $\Delta' \in \mathbb{Z}$ an odd fundamental discriminant, and let $E_1 := E_0^{(\Delta_2)}$. Then T.4 shows that $\rho_{E_1,2^n}$ is surjective for every $n \geq 3$. Moreover, $\rho_{E_1,3^n}$ is surjective for every $n \geq 1$, which follows from Proposition 5.1 after observing that $K(E_0[3]) \cap K(\sqrt{\Delta_2}) = K$ because $[K(E_0[3]) \colon K] = 3$. These considerations, together with Theorem 1.1, show that

$$\operatorname{Gal}(K((E_1)_{\mathrm{tors}})/K) \cong \left(\prod_{q \notin S} \operatorname{Gal}(K(E_1[q^\infty])/K)\right) \times \operatorname{Gal}(K(E_1[S^\infty])/K)$$

with the product running over the rational primes $q \in \mathbb{N}$ such that $q \notin S$ where $S = \{2, 3\}$ and $K(E_1[S^\infty])$ denotes the compositum of the division fields $K(E_1[2^\infty])$ and $K(E_1[3^\infty])$. Moreover, T.1, T.2 and the previous considerations show that $\operatorname{Gal}(K(E_1[\ell^m])/K) \cong (\mathcal{O}/\ell^m\mathcal{O})^\times$ for every prime $\ell \in \mathbb{N}$ and every $m \in \mathbb{N}$. Now, Proposition 5.1 shows that $K(E_1[3^m]) \cap K(E_1[\Delta_2]) = K(\sqrt{\Delta_2})$ and $K(E_1[3^m]) = H_{3^m,\mathcal{O}}(\sqrt{\Delta_2})$ for every $m \in \mathbb{Z}_{\geq 1}$. Hence $K(E_1[2^\infty])$ and $K(E_1[3^\infty])$ are entangled over K, and for every pair of integers $a, b \in \mathbb{Z}_{\geq 1}$ we have that

$$\operatorname{Gal}(L/K) \cong \frac{(\mathcal{O}/2^a\mathcal{O})^\times \times (\mathcal{O}/3^b\mathcal{O})^\times}{\{\pm 1\}}$$

where L denotes the compositum of $K(E_1[2^a])$ and $K(E_1[3^b])$.

To conclude our analysis of the division fields of $E = E_0^{(\Delta)}$ we can observe that $E = E_1^{(\Delta')}$ and that $\gcd(\Delta', \mathfrak{f}_{E_1}) = \gcd(\Delta', 6) = 1$. Hence Theorem 1.1 gives the decomposition

$$\operatorname{Gal}(K(E_{\mathrm{tors}})/K) \cong \left(\prod_{q \notin S} \operatorname{Gal}(K(E[q^\infty])/K)\right) \times \operatorname{Gal}(K(E[S^\infty])/K)$$

with the product running over the rational primes $q \in \mathbb{N}$ such that $q \notin S$ where $S \subseteq \mathbb{N}$ denotes the finite set of primes dividing $6\Delta'$. Now, T.1 and T.2 show that $\operatorname{Gal}(K(E[\ell^m])/K) \cong (\mathcal{O}/\ell^m)^\times$ for all rational primes $\ell \in \mathbb{Z}$ and all $m \in \mathbb{N}$. Moreover, Proposition 5.1 shows that $K(E[3^m]) \cap K(E[\Delta]) = K(\sqrt{\Delta})$ and $K(E[3^m]) = H_{3^m,\mathcal{O}}(\sqrt{\Delta})$ for every $m \in \mathbb{Z}_{\geq 1}$. Hence the family $\{K(E[q^\infty])\}_{q \in S}$ is entangled over K, and for every collection of integers $\{a_q\}_{q \in S} \subseteq \mathbb{Z}_{\geq 1}$ we get

$$\operatorname{Gal}(L/K) \cong \frac{\prod_{q \in S} (\mathcal{O}/q^{a_q}\mathcal{O})^\times}{\{\pm 1\}}$$

where L is the compositum of all the division fields $K(E[q^{a_q}])$ for $q \in S$.

The following theorem summarises the previous discussion. Recall that, for every rational prime $q \in \mathbb{N}$, we denote by $K(E[q^\infty])$ the compositum of all the division fields $\{K(E[q^n])\}_{n\in\mathbb{N}}$ associated to an elliptic curve E, and for every finite set of primes $S \subseteq \mathbb{N}$ we denote by $K(E[S^\infty])$ the compositum of all the fields $\{K(E[q^\infty])\}_{q\in S}$.

Theorem 5.4. *Let $\mathcal{O}$ be an order inside an imaginary quadratic field K such that* $\mathrm{Pic}(\mathcal{O}) = 1$ *and $\Delta_\mathcal{O} < -4$. We introduce the following notation:*

$$n := \begin{cases} 4, & \text{if } \mathcal{O} \in \{\mathbb{Z}[2i], \mathbb{Z}[\sqrt{-2}]\} \\ 2, & \text{otherwise} \end{cases} \qquad \text{and} \qquad \begin{array}{l} p \in \mathbb{N} \text{ the unique prime ramifying in } \mathbb{Q} \subseteq K, \\ \mathfrak{p} \subseteq \mathcal{O}_K \text{ the unique prime lying above } p. \end{array}$$

Label all the elliptic curves defined over $\mathbb{Q}$ which have complex multiplication by $\mathcal{O}$ as $\{A_r\}_{r\in\mathbb{Z}_{\geq 1}}$ in such a way that $|\mathfrak{f}_{A_r}| \leq |\mathfrak{f}_{A_{r+1}}|$ for every $r \in \mathbb{Z}_{\geq 1}$. Then $|\mathfrak{f}_{A_n}| < |\mathfrak{f}_{A_{n+1}}|$ and the properties of the division fields associated to the elliptic curve A_r depend on r as follows:

$\boxed{r \leq n}$ **Disjointness:** *the family $\{K(A_r[q^\infty])\}_q$, where $q \in \mathbb{N}$ runs over all the rational primes, is linearly disjoint over K;*

Maximality: $\mathrm{Gal}(K(A_r[q^m])/K) \cong (\mathcal{O}/q^m\mathcal{O})^\times$ *for every prime $q \neq p$ and every $m \in \mathbb{N}$;*

Minimality: $\mathrm{Gal}(K(A_r[p^m])/K) \cong (\mathcal{O}/p^m\mathcal{O})^\times/\{\pm 1\}$ *for every $m \geq n-1$;*

$\boxed{r > n}$ **Twist:** *there exists a unique $r_0 \leq n$ and a unique fundamental discriminant $\Delta \in \mathbb{Z}$ coprime with p such that $A_r = A_{r_0}^{(\Delta)}$;*

Disjointess: *there is a decomposition*

$$\mathrm{Gal}(K((A_r)_{tors})/K) \cong \left(\prod_{q \notin S} \mathrm{Gal}(K(A_r[q^\infty])/K) \right) \times \mathrm{Gal}(K(A_r[S^\infty])/K)$$

where $S \subseteq \mathbb{N}$ denotes the finite set of primes dividing $p \cdot \Delta$ and the product runs over the rational primes $q \in \mathbb{N}$ such that $q \notin S$. This shows that the family

$$\{\, K(A_r[S^\infty]) \,\} \cup \{\, K(A_r[q^\infty]) \,\}_{q \notin S}$$

is linearly disjoint over K;

Entanglement: *for every $m \in \mathbb{N}$ such that $m \geq n-1$ we have that*

$$K(A_r[p^m]) = H_{p^m,\mathcal{O}}(\sqrt{\Delta}) \qquad \text{and} \qquad K(A_r[p^m]) \cap K(A_r[\Delta]) = K(\sqrt{\Delta})$$

which shows that the family $\{K(A_r[q^\infty])\}_{q\in S}$ is entangled over K;

Maximality: $\mathrm{Gal}(K(A_r[q^m])/K) \cong (\mathcal{O}/q^m\mathcal{O})^\times$ *for every prime $q \in \mathbb{N}$ and every $m \in \mathbb{N}$;*

Minimality: *for every collection of integers $\{a_q\}_{q\in S} \subseteq \mathbb{Z}_{\geq 1}$ with $a_p \geq n-1$ we get*

$$\mathrm{Gal}(L/K) \cong \frac{\prod_{q\in S} (\mathcal{O}/q^{a_q}\mathcal{O})^\times}{\{\pm 1\}}$$

where L is the compositum of all the division fields $K(A_r[q^{a_q}])$ for $q \in S$.

Remark 5.5. We exclude the two orders $\mathbb{Z}[i]$ and $\mathbb{Z}[\zeta_3]$ in the statement of Theorem 5.4 because elliptic curves having complex multiplication by these orders admit quartic (respectively sextic) twists (as explained in [30, Chapter X, Proposition 5.4]). To study these we would need a generalisation of Proposition 5.1, which will be subject of future investigations.

Appendix A. Ray class fields for orders

The aim of this appendix is to study certain abelian extensions $H_{I,\mathcal{O}}$ of a number field F associated to ideals $I \subseteq \mathcal{O}$ contained in a general *order* $\mathcal{O} \subseteq F$. We call the extension $H_{I,\mathcal{O}}$ the *ray class field modulo I for the order $\mathcal{O}$*. This definition generalises the one given by Söhngen in [33] and Stevenhagen in [34, § 4], who restrict their attention to imaginary quadratic fields F

and ideals $I = N \cdot \mathcal{O}$ for some $N \in \mathbb{N}$. The material present in this appendix is probably well known to the experts, but the authors have included it here since they have been unable to find a suitable reference.

A.1. **The general theory.** In this section we define the ray class fields $H_{I,\mathcal{O}}$ and we study their Galois groups. The notation used for lattices and idèles is the one established in Section 4.

Definition A.1. Let F be a number field, let $\mathcal{O} \subseteq \mathcal{O}_F$ be an order and let $I \subseteq \mathcal{O}$ be a non-zero ideal. Then we define the *ray class field of F modulo I relative to the order $\mathcal{O}$* as

$$H_{I,\mathcal{O}} := (F^{\mathrm{ab}})^{[U_{I,\mathcal{O}},F]} \subseteq F^{\mathrm{ab}} \tag{17}$$

where $[\cdot, F] \colon \mathbb{A}_F^\times \to \mathrm{Gal}(F^{\mathrm{ab}}/F)$ is the *global Artin map* and $U_{I,\mathcal{O}} \subseteq \mathbb{A}_F^\times$ is the subgroup

$$U_{I,\mathcal{O}} := \left\{ s \in \mathbb{A}_F^\times \;\middle|\; s_p \in \left(\mathcal{O}_p^\times \cap (1 + I \cdot \mathcal{O}_p)\right) \text{ for all rational primes } p \in \mathbb{N} \right\} \tag{18}$$

defined using the decomposition (11), where

$$\mathcal{O}_p := \varprojlim_{n \in \mathbb{N}} \frac{\mathcal{O}}{p^n \mathcal{O}} \cong \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p \tag{19}$$

denotes the completion of $\mathcal{O}$ with respect to the ideal $p\,\mathcal{O}$.

When $I = N \cdot \mathcal{O}$ for some $N \in \mathbb{Z}_{\geq 1}$ we denote $U_{I,\mathcal{O}}$ by $U_{N,\mathcal{O}}$, and we write $U_{\mathcal{O}} := U_{1,\mathcal{O}}$. Analogously, we will write $H_{N,\mathcal{O}}$ in place of $H_{N \cdot \mathcal{O},\mathcal{O}}$, and we will denote by $H_{\mathcal{O}} := H_{1,\mathcal{O}}$ the *ring class field* of $\mathcal{O}$.

Remark A.2. When $\mathcal{O} = \mathcal{O}_F$ is the ring of integers, the ray class fields $H_{I,\mathcal{O}_F}$ coincide with the usual ray class fields of F modulo I (see [23, Chapter VI, Definition 6.2]). Moreover, when $F = K$ is an imaginary quadratic field, the ray class fields $H_{N,\mathcal{O}}$ have been defined by Söhngen in [33]. This work has been reformulated using an adelic language by Stevenhagen in [34, § 4]. Finally, the ring class fields $H_{\mathcal{O}}$ have been studied for general number fields F by Lv and Deng in [20] and by Yi and Lv in [38].

Remark A.3. It is clear from the definition that for every pair of ideals $I \subseteq J \subseteq \mathcal{O}$ we have that $U_{I,\mathcal{O}} \subseteq U_{J,\mathcal{O}}$, which implies that $H_{I,\mathcal{O}} \supseteq H_{J,\mathcal{O}}$. In particular, $H_{\mathcal{O}} \subseteq H_{I,\mathcal{O}}$ for every ideal $I \subseteq \mathcal{O}$. Similarly, for every pair of orders $\mathcal{O}_1 \subseteq \mathcal{O}_2 \subseteq F$ and every ideal $I \subseteq \mathcal{O}_1$ we have that $U_{I,\mathcal{O}_1} \subseteq U_{I \cdot \mathcal{O}_2,\mathcal{O}_2}$, which gives the containment $H_{I,\mathcal{O}_1} \supseteq H_{I \cdot \mathcal{O}_2,\mathcal{O}_2}$ generalising the *Anordnungssatz* explained in [34, Page 169]. In particular for every order $\mathcal{O} \subseteq F$ and every ideal $I \subseteq \mathcal{O}$ we get the following inclusions

$$\begin{array}{ccccccc}
 & & H_{I \cdot \mathcal{O}_F,\mathcal{O}_F} & \subseteq & H_{I,\mathcal{O}} & \subseteq & H_{I \cdot \mathfrak{f}_{\mathcal{O}} \cdot \mathcal{O}_F,\mathcal{O}_F} \\
 & & \cup\!\mathrm{I} & & \cup\!\mathrm{I} & & \cup\!\mathrm{I} \\
F & \subseteq & H_{\mathcal{O}_F} & \subseteq & H_{\mathcal{O}} & \subseteq & H_{\mathfrak{f}_{\mathcal{O}},\mathcal{O}_F}
\end{array}$$

where $\mathfrak{f}_{\mathcal{O}} := (\mathcal{O} \colon \mathcal{O}_F) = \{\alpha \in F \mid \alpha \mathcal{O}_F \subseteq \mathcal{O}\} \subseteq \mathcal{O}$ is the *conductor* of $\mathcal{O}$, which is the biggest ideal of $\mathcal{O}_F$ contained in $\mathcal{O}$. This shows, applying [23, Chapter VI, Corollary 6.6], that the extension $F \subseteq H_{I,\mathcal{O}}$ is unramified outside the set of primes dividing $I \cdot \mathfrak{f}_{\mathcal{O}} \cdot \mathcal{O}_F$.

We describe now the Galois groups of the abelian extensions $F \subseteq H_{I,\mathcal{O}}$.

Lemma A.4. *Let F be a number field, $\mathcal{O} \subseteq \mathcal{O}_F$ be an order and $I \subseteq \mathcal{O}$ be a non-zero ideal. Then $F^\times \cdot U_{I,\mathcal{O}} \subseteq \mathbb{A}_F^\times$ is a closed subgroup of finite index, and there is an isomorphism*

$$\mathrm{Gal}(H_{I,\mathcal{O}}/F) \cong \frac{\mathbb{A}_F^\times}{F^\times \cdot U_{I,\mathcal{O}}}$$

induced by the global Artin map $[\cdot, F] \colon \mathbb{A}_F^\times \twoheadrightarrow \mathrm{Gal}(F^{ab}/F)$.

Proof. The fact that $F^\times \cdot U_{I,O}$ is closed of finite index follows from [23, Chapter VI, Proposition 1.8], because $U_{I\cdot\mathfrak{f}_O\cdot O_F, O_F} \subseteq U_{I,O}$. Then we can conclude using the global reciprocity law [23, Chapter VI, Theorem 6.1]. □

The previous description can be made more explicit by dividing the extension $F \subseteq H_{I,O}$ in the two sub-extensions $F \subseteq H_O$ and $H_O \subseteq H_{I,O}$.

Proposition A.5. *Let O be an order inside a number field F. Then*

$$\mathrm{Gal}(H_O/F) \cong \mathrm{Pic}(O)$$

where $\mathrm{Pic}(O)$ denotes the class group of the order O.

Proof. Combine [38, Theorem and Definition 2.11] and [38, Theorem 4.2]. □

Theorem A.6. *Let F be a number field, $O \subseteq O_F$ be an order and $I \subseteq O$ be a non-zero ideal. Then*

$$\mathrm{Gal}(H_{I,O}/H_O) \cong \frac{(O/I)^\times}{\pi_I^\times(O^\times)}$$

where $\pi_I^\times \colon O^\times \longrightarrow (O/I)^\times$ is the map induced by the projection $\pi_I \colon O \twoheadrightarrow O/I$.

Proof. First of all, we see that

$$\begin{aligned}\mathrm{Gal}(H_{I,O}/H_O) &= \ker\left(\mathrm{Gal}(H_{I,O}/F) \twoheadrightarrow \mathrm{Gal}(H_O/F)\right) \overset{(a)}{\cong} \ker\left(\frac{\mathbb{A}_F^\times}{F^\times \cdot U_{I,O}} \twoheadrightarrow \frac{\mathbb{A}_F^\times}{F^\times \cdot U_O}\right) \cong \\ &\cong \frac{F^\times \cdot U_O}{F^\times \cdot U_{I,O}} \cong \frac{F^\times \cdot U_O/F^\times}{F^\times \cdot U_{I,O}/F^\times} \overset{(b)}{\cong} \frac{U_O/(F^\times \cap U_O)}{(U_{I,O} \cdot (F^\times \cap U_O))/(F^\times \cap U_O)} \cong \\ &\cong \frac{U_O}{U_{I,O} \cdot (F^\times \cap U_O)} \overset{(c)}{=} \frac{U_O}{U_{I,O} \cdot O^\times}\end{aligned}$$

where (a) comes from Lemma A.4, (b) holds because $U_{I,O} \subseteq U_O$ and (c) follows from the fact that $F^\times \cap U_O = O^\times$.

Now, observe that $F_\infty^\times \subseteq O$, where $F_\infty := F \otimes_{\mathbb{Q}} \mathbb{R} \cong \prod_{w|\infty} F_w \hookrightarrow \mathbb{A}_F^\times$. Moreover, we have

$$\frac{U_O}{F_\infty^\times} \cong \prod_{p\in\mathbb{N}} O_p^\times \cong \prod_{p\in\mathbb{N}} \varprojlim_{n\in\mathbb{N}} \left(\frac{O}{p^n O}\right)^\times \cong \varprojlim_{N\in\mathbb{Z}_{\geq 1}} \left(\frac{O}{NO}\right)^\times \cong \widehat{O}^\times \tag{20}$$

where the products run over the rational primes $p \in \mathbb{N}$, and O_p is the ring defined in (19). In the chain of isomorphisms (20) the ring $\widehat{O}$ is the profinite completion of O, *i.e.*

$$\widehat{O} := \varprojlim_{N\in\mathbb{Z}_{\geq 1}} \frac{O}{NO} \cong \prod_{p\in\mathbb{N}} O_p \cong \prod_{\mathfrak{p}\subseteq O} O_{\mathfrak{p}} \tag{21}$$

where the second product runs over all the non-zero prime ideals $\mathfrak{p} \subseteq O$ and $O_{\mathfrak{p}} := \varprojlim_{n\in\mathbb{N}} O/\mathfrak{p}^n$ is the completion of O at the prime $\mathfrak{p}$. The second isomorphism appearing in (21) can be obtained by applying [12, Corollary 7.6] to $R = \mathbb{Z}_p$ and $A = O_p$. This gives the decomposition

$$O_p \cong \prod_{\mathfrak{p}\supseteq p} O_{\mathfrak{p}}$$

where the product runs over all primes $\mathfrak{p} \subseteq O$ lying above p.

Under the isomorphism (20) the subgroup $U_{I,O}/F_\infty^\times \subseteq U_O/F_\infty^\times \cong \widehat{O}^\times$ is identified with the kernel of the map $\widehat{\pi}_I^\times \colon \widehat{O}^\times \longrightarrow (\widehat{O}/I\widehat{O})^\times$ induced by the projection $\widehat{\pi}_I \colon \widehat{O} \twoheadrightarrow \widehat{O}/I\widehat{O}$. Hence

$$\mathrm{Gal}(H_{I,O}/H_O) \cong \frac{U_O}{U_{I,O} \cdot O^\times} \cong \frac{U_O/F_\infty^\times}{(U_{I,O} \cdot O^\times)/F_\infty^\times} \cong \frac{\widehat{O}^\times}{\ker(\widehat{\pi}_I^\times) \cdot O^\times} \cong \frac{(\widehat{O}/I\widehat{O})^\times}{\widehat{\pi}_I^\times(O^\times)}$$

because $\widehat{\pi}_I^{\times}$ is surjective. This surjectivity is shown by the factorisation

$$\begin{tikzcd} \widehat{\mathcal{O}}^{\times} \arrow[rr, "\widehat{\pi}_I^{\times}"] \arrow[dr, two heads] & & \left(\widehat{\mathcal{O}}/I\widehat{\mathcal{O}}\right)^{\times} \\ & \prod_{\mathfrak{p} \supseteq I} \mathcal{O}_{\mathfrak{p}}^{\times} \arrow[ur, two heads] & \end{tikzcd}$$

where the first map $\widehat{\mathcal{O}}^{\times} \twoheadrightarrow \prod_{\mathfrak{p} \supseteq I} \mathcal{O}_{\mathfrak{p}}^{\times}$ is surjective as follows from (21), and the second map

$$\prod_{\mathfrak{p} \supseteq I} \mathcal{O}_{\mathfrak{p}}^{\times} \twoheadrightarrow \prod_{\mathfrak{p} \supseteq I} \left(\frac{\mathcal{O}_{\mathfrak{p}}}{I\mathcal{O}_{\mathfrak{p}}} \right)^{\times} \cong \left(\frac{\widehat{\mathcal{O}}}{I\widehat{\mathcal{O}}} \right)^{\times}$$

is surjective by [8, Corollary 2.3], which can be applied since the ring $\prod_{\mathfrak{p} \supseteq I} \mathcal{O}_{\mathfrak{p}}$ has finitely many maximal ideals.

To finish our proof we need to show that

$$\frac{(\widehat{\mathcal{O}}/I\widehat{\mathcal{O}})^{\times}}{\widehat{\pi}_I^{\times}(\mathcal{O}^{\times})} \cong \frac{(\mathcal{O}/I)^{\times}}{\pi_I^{\times}(\mathcal{O}^{\times})}.$$

To do this recall that π_I and $\widehat{\pi}_I$ are related by the commutative diagram

$$\begin{tikzcd} \mathcal{O} \arrow[r, two heads, "\pi_I"] \arrow[d, hook] & \mathcal{O}/I \arrow[r, "\gamma"] \arrow[d] & \prod_{\mathfrak{p} \supseteq I} \frac{\mathcal{O}_{(\mathfrak{p})}}{I\mathcal{O}_{(\mathfrak{p})}} \arrow[d, "\beta"] \\ \widehat{\mathcal{O}} \arrow[r, two heads, "\widehat{\pi}_I"] & \widehat{\mathcal{O}}/I\widehat{\mathcal{O}} \arrow[r, "\alpha", "\sim"'] & \prod_{\mathfrak{p} \supseteq I} \frac{\mathcal{O}_{\mathfrak{p}}}{I\mathcal{O}_{\mathfrak{p}}} \end{tikzcd}$$

where α is the isomorphism coming from the decomposition (21), and β and γ are the maps induced by the natural inclusions $\mathcal{O} \subseteq \mathcal{O}_{(\mathfrak{p})} \subseteq \mathcal{O}_{\mathfrak{p}}$. Moreover the products run over all the prime ideals $\mathfrak{p} \subseteq \mathcal{O}$ such that $\mathfrak{p} \supseteq I$, and $\mathcal{O}_{(\mathfrak{p})}$ denotes the localisation of $\mathcal{O}$ at the prime $\mathfrak{p}$.

Hence to conclude it is sufficient to observe that γ is an isomorphism by [23, Chapter I, Proposition 12.3], and β is an isomorphism because $\mathcal{O}$ is a one-dimensional Noetherian domain (see [23, Chapter I, Proposition 12.2]). More explicitly, for any prime $\mathfrak{p} \subseteq \mathcal{O}$ such that $\mathfrak{p} \supseteq I$ we have that $\mathfrak{p} \cdot \mathcal{O}_{(\mathfrak{p})} = \sqrt{I \cdot \mathcal{O}_{(\mathfrak{p})}}$ because $\mathcal{O}_{(\mathfrak{p})}$ is a one-dimensional local ring. Hence [3, Chapter II, § 2.6, Proposition 15] shows that $\mathcal{O}_{(\mathfrak{p})}/I\mathcal{O}_{(\mathfrak{p})}$ is complete with respect to $\mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$. Thus we can conclude that $\mathcal{O}_{(\mathfrak{p})}/I\mathcal{O}_{(\mathfrak{p})}$ is isomorphic to $\mathcal{O}_{\mathfrak{p}}/I\mathcal{O}_{\mathfrak{p}}$ using the exactness of completion, which holds because $\mathcal{O}_{(\mathfrak{p})}$ is Noetherian (see [12, Lemma 7.15]). □

A.2. **Ray class fields for imaginary quadratic orders.** Since the definition of the ray class fields $H_{I,\mathcal{O}}$ is somehow implicit, a natural question would be to provide an explicit set of generators for the extension $F \subseteq H_{I,\mathcal{O}}$. This has been done, using the classical theory of complex multiplication, if $F = K$ is an imaginary quadratic field and $\mathcal{O} = \mathcal{O}_K$ or $I = N \cdot \mathcal{O}$ for some $N \in \mathbb{Z}_{\geq 1}$, as explained for example in [29, Chapter II, Theorem 5.6] and [34, § 4]. More precisely, in these cases one can write

$$H_{I,\mathcal{O}} = H_{\mathcal{O}}(\mathfrak{h}_E(E[I])) = K(j(E), \mathfrak{h}_E(E[I])) \tag{22}$$

where E is any elliptic curve $E_{/\mathbb{C}}$ which has complex multiplication by $\mathcal{O}$, $\mathfrak{h}_E$ is the *Weber function* $\mathfrak{h}_E \colon E \twoheadrightarrow E/\mathrm{Aut}(E) \cong \mathbb{P}^1$ and $E[I] := \{x \in E(\mathbb{C}) \mid [\alpha](x) = 0,\ \forall \alpha \in I\}$ is the set of I-torsion points of E. The aim of this section is to show that (22) holds more generally when $I \subseteq \mathcal{O}$ is any *invertible* ideal, as proved in the following theorem.

Theorem A.7. *Let $\mathcal{O}$ be an order inside an imaginary quadratic field $K \subseteq \mathbb{C}$, and let $I \subseteq \mathcal{O}$ be an invertible ideal. Then we have that*

$$H_{I,\mathcal{O}} = H_{\mathcal{O}}(\mathfrak{h}_E(E[I])) = K(j(E), \mathfrak{h}_E(E[I]))$$

for any elliptic curve $E_{/\mathbb{C}}$ such that $\operatorname{End}(E) \cong \mathcal{O}$*. In particular, if E is an elliptic curve defined over a number field F such that* $\operatorname{End}_F(E) \cong \mathcal{O}$ *then $H_{I,\mathcal{O}} \subseteq F(E[I])$.*

Proof. By the previous discussion, we can assume that $j(E) \notin \{0, 1728\}$, because in this case $\mathcal{O} = \mathcal{O}_K$. Fix a generator P of $E[I]$ as a module over $\mathcal{O}/I$, which exists by Lemma 3.1 because $I \subseteq \mathcal{O}$ is invertible. Then $H_{\mathcal{O}}(\mathfrak{h}_E(E[I])) = H_{\mathcal{O}}(\mathfrak{h}_E(P))$, as one can see by writing every endomorphism of E in the standard form described in [37, § 2.9] and applying [15, Chapter I, Theorem 7].

Let now $\xi \colon \mathbb{C}/\mathfrak{a} \xrightarrow{\sim} E(\mathbb{C})$ be a complex parametrisation, where $\mathfrak{a} \subseteq \mathcal{O}$ is an invertible ideal (see [28, Proposition 4.8]). Fix moreover $z \in (\mathfrak{a} \colon I) \subseteq K \subseteq \mathbb{C}$ such that $\xi(\overline{z}) = P$, where $\overline{z} := \mathfrak{a}z/\mathfrak{a}$ denotes the image of z in the quotient $K/\mathfrak{a} \subseteq \mathbb{C}/\mathfrak{a}$. Then [28, Theorem 5.5] shows that

$$H_{\mathcal{O}}(\mathfrak{h}_E(P)) = (K^{\mathrm{ab}})^{[W_P, K]}$$

where $W_P \subseteq \mathbb{A}_K^\times$ is the subgroup defined by $W_P := \left\{ s \in \mathbb{A}_K^\times \,\middle|\, s \cdot \mathfrak{a} = \mathfrak{a},\ s \cdot \overline{z} = \overline{z} \right\}$. In particular, we recall that for any $s \in \mathbb{A}_K^\times$ such that $s \cdot \mathfrak{a} = \mathfrak{a}$ the notation $s \cdot \overline{z}$ stands for the image of $\overline{z} \in K/\mathfrak{a}$ under the map $K/\mathfrak{a} \xrightarrow{s\cdot} K/\mathfrak{a}$. This map is defined by the commutative diagram

$$\begin{tikzcd}
\frac{K}{\mathfrak{a}} \arrow[r, "s\cdot"] \arrow[d, "\wr"'] & \frac{K}{s \cdot \mathfrak{a}} \arrow[r, phantom, "="] \arrow[d, "\wr"'] & \frac{K}{\mathfrak{a}} \arrow[d, "\wr"'] \\
\bigoplus_{p \in M_{\mathbb{Q}}^0} \frac{K_p}{\mathfrak{a}_p} \arrow[r, "(s_p \cdot)_p"] & \bigoplus_{p \in M_{\mathbb{Q}}^0} \frac{K_p}{s_p \mathfrak{a}_p} \arrow[r, phantom, "="] & \bigoplus_{p \in M_{\mathbb{Q}}^0} \frac{K_p}{\mathfrak{a}_p}
\end{tikzcd}$$

where $\mathfrak{a}_p := \mathfrak{a} \otimes_{\mathbb{Z}} \mathbb{Z}_p = \mathfrak{a}\,\mathcal{O}_p$ for any rational prime $p \in \mathbb{N}$. Since $H_{\mathcal{O}} = K(j(E))$ the theorem will follow from the equality $W_P = U_{I,\mathcal{O}}$, where $U_{I,\mathcal{O}} \subseteq \mathbb{A}_K^\times$ is the subgroup defined in (18).

To prove the inclusion $U_{I,\mathcal{O}} \subseteq W_P$ take any $s \in U_{I,\mathcal{O}}$. Then $s \cdot \mathfrak{a} = \mathfrak{a}$ because $s_p \mathfrak{a}_p = \mathfrak{a}_p$ for every rational prime $p \in \mathbb{N}$, since by definition $s_p \in \mathcal{O}_p^\times$. Moreover, $s \cdot \overline{z} = \overline{z}$ because $z \in (\mathfrak{a} \colon I)$ and $s_p \in 1 + I\mathcal{O}_p$ for every rational prime $p \in \mathbb{N}$, which implies that $(s_p - 1)z \in \mathfrak{a}_p$. This shows that $U_{I,\mathcal{O}} \subseteq W_z$

To prove the opposite inclusion $W_P \subseteq U_{I,\mathcal{O}}$ fix any rational prime $p \in \mathbb{N}$ and take $s \in W_P$, so that $s \cdot \mathfrak{a} = \mathfrak{a}$ and $s \cdot \overline{z} = \overline{z}$. Since $\mathfrak{a} \subseteq \mathcal{O}$ is invertible we have that $\mathfrak{a} \cdot (\mathcal{O} \colon \mathfrak{a}) = \mathcal{O}$ and

$$s \cdot \mathcal{O} = s \cdot (\mathfrak{a} \cdot (\mathcal{O} \colon \mathfrak{a})) = (s \cdot \mathfrak{a}) \cdot (\mathcal{O} \colon \mathfrak{a}) = \mathfrak{a} \cdot (\mathcal{O} \colon \mathfrak{a}) = \mathcal{O}$$

which shows that $s_p \in \mathcal{O}_p^\times$. Let us now prove that $s_p \in 1 + I \cdot \mathcal{O}_p$. Since $I \subseteq \mathcal{O}$ and $\mathfrak{a} \subseteq \mathcal{O}$ are both invertible we have that $I \cdot (\mathcal{O} \colon \mathfrak{a}) \cdot (\mathfrak{a} \colon I) = \mathcal{O}$, so that we can write $1 = \sum_{j=1}^J \alpha_j \beta_j \tau_j$ with $\alpha_j \in I$, $\beta_j \in (\mathcal{O} \colon \mathfrak{a})$ and $\tau_j \in (\mathfrak{a} \colon I)$. Notice that $s \cdot \overline{\tau_j} = \overline{\tau_j}$ for every $j \in \{1, \dots, J\}$ because $s \cdot \overline{z} = \overline{z}$ and $P = \xi(\overline{z})$ generates $E[I]$ as a module over $\mathcal{O}/I$. Hence $s_p - 1 \in I \cdot \mathcal{O}_p$ because we can write

$$s_p - 1 = \sum_{j=1}^J \alpha_j\, \beta_j\, (s_p\, \tau_j - \tau_j)$$

where $s_p\, \tau_j - \tau_j \in \mathfrak{a}_p = \mathfrak{a}\,\mathcal{O}_p$ and $\beta_j(s_p\, \tau_j - \tau_j) \in \mathcal{O}_p$ since $\beta_j \in (\mathcal{O} \colon \mathfrak{a})$ for every $j \in \{1, \dots, J\}$. Thus we have shown that $s_p \in \mathcal{O}_p^\times$ and $s_p \in 1 + I \cdot \mathcal{O}_p$ for every prime $p \in \mathbb{N}$, which gives $W_P \subseteq U_{I,\mathcal{O}}$ as we wanted to prove. □

Acknowledgements

We would like to thank Ian Kiming and Fabien Pazuki, for their precious guidance and constant encouragement during the preparation of this work. We thank Peter Stevenhagen for sharing his numerous ideas on division fields of elliptic curves.

This project has received funding from the European Union Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 801199.

References

[1] N. Arthaud. "On Birch and Swinnerton-Dyer's conjecture for elliptic curves with complex multiplication. I". In: *Compositio Mathematica* 37.2 (1978), pp. 209–232 (cit. on p. 9).

[2] E. Artin and J. Tate. *Class field theory*. W. A. Benjamin, Inc., New York-Amsterdam, 1968 (cit. on p. 12).

[3] N. Bourbaki. *Commutative algebra. Chapters 1–7*. Springer-Verlag, Berlin, 1989 (cit. on p. 26).

[4] A. Bourdon, P. Clark, and J. Stankewicz. "Torsion points on CM elliptic curves over real number fields". In: *Transactions of the American Mathematical Society* 369.12 (2017), pp. 8457–8496 (cit. on p. 10).

[5] A. Bourdon and P. L. Clark. "Torsion points and Galois representations on CM elliptic curves". arXiv:1612.03229. (2019) (cit. on p. 6).

[6] F. Campagna and P. Stevenhagen. "Cyclic reduction of CM elliptic curves". *In preparation* (cit. on p. 2).

[7] F. Campagna and P. Stevenhagen. "Cyclic reduction of Elliptic Curves". arXiv:2001.00028. (2020) (cit. on p. 1).

[8] J. Chen. "Surjections of unit groups and semi-inverses". In: *J. Commut. Algebra* (2020). To appear. (cit. on p. 26).

[9] J. Coates and A. Wiles. "On the conjecture of Birch and Swinnerton-Dyer". In: *Inventiones mathematicæ* 39.3 (1977), pp. 223–251 (cit. on pp. 2, 9, 14).

[10] J. Coates. "Lectures on the Birch-Swinnerton-Dyer conjecture". In: *Notices of the International Congress of Chinese Mathematicians* 1.2 (2013), pp. 29–46 (cit. on p. 9).

[11] D. A. Cox. *Primes of the form x^2+ny^2*. Second. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, 2013 (cit. on pp. 2, 6, 10, 16, 18).

[12] D. Eisenbud. *Commutative algebra*. Vol. 150. Graduate Texts in Mathematics. Springer-Verlag, New York, 1995 (cit. on pp. 25, 26).

[13] D. Husemöller. *Elliptic curves*. Second. Vol. 111. Graduate Texts in Mathematics. Springer-Verlag, New York, 2004 (cit. on p. 12).

[14] N. C. Kuhman. "On the Conjecture of Birch and Swinnerton-Dyer for Elliptic Curves with Complex Multiplication." PhD thesis. Stanford University, 1978 (cit. on pp. 2, 14).

[15] S. Lang. *Elliptic functions*. Second. Vol. 112. Graduate Texts in Mathematics. Springer-Verlag, New York, 1987 (cit. on pp. 7, 8, 11, 13, 27).

[16] D. Lombardo. "Galois representations attached to abelian varieties of CM type". In: *Bulletin de la Société Mathématique de France* 145.3 (2017), pp. 469–501 (cit. on p. 10).

[17] Á. Lozano-Robledo. "Formal groups of elliptic curves with potential good supersingular reduction". In: *Pacific Journal of Mathematics* 261.1 (2013), pp. 145–164 (cit. on p. 9).

[18] Á. Lozano-Robledo. "Ramification in the division fields of elliptic curves with potential supersingular reduction". In: *Research in Number Theory* 2.1 (2016), p. 8 (cit. on p. 9).

[19] Á. Lozano-Robledo. "Uniform boundedness in terms of ramification". In: *Research in Number Theory* 4.1 (2018), p. 6 (cit. on p. 9).

[20] C. Lv and Y. Deng. "On orders in number fields: Picard groups, ring class fields and applications". In: *Science China Mathematics* 58.8 (2015), pp. 1627–1638 (cit. on p. 24).

[21] J. S. Milne. "On the arithmetic of abelian varieties". In: *Inventiones mathematicae* 17.3 (1972), pp. 177–190 (cit. on p. 17).

[22] M. R. Murty. "On Artin's conjecture". In: *Journal of Number Theory* 16.2 (1983), pp. 147–168 (cit. on p. 10).

[23] J. Neukirch. *Algebraic Number Theory*. Vol. 322. Grundlehren der mathematischen Wissenschaften. Springer Berlin Heidelberg, 1999 (cit. on pp. 2, 6, 11, 12, 15, 24–26).

[24] R. Pengo. "Mahler's measure and elliptic curves with potential complex multiplication". arXiv:2005.04159. (2020) (cit. on pp. 2, 17).

[25] J.-P. Serre. "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques". In: *Inventiones mathematicæ* 15.4 (1971), pp. 259–331 (cit. on pp. 1, 2).

[26] J.-P. Serre and J. Tate. "Good reduction of abelian varieties". In: *Annals of Mathematics. Second Series* 88 (1968), pp. 492–517 (cit. on p. 17).

[27] G. Shimura. *Abelian varieties with complex multiplication and modular functions*. Vol. 46. Princeton Mathematical Series. Princeton University Press, Princeton, NJ, 1998 (cit. on p. 5).

[28] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*. Vol. 11. Publications of the Mathematical Society of Japan. Princeton University Press, Princeton, NJ, 1994 (cit. on pp. 2, 12–15, 27).

[29] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*. Vol. 151. New York, NY: Springer-Verlag, 1994, pp. xiii + 525 (cit. on pp. 4, 5, 13, 26).

[30] J. H. Silverman. *The arithmetic of elliptic curves. 2nd ed.* 2nd ed. Vol. 106. New York, NY: Springer, 2009, pp. xx + 513 (cit. on pp. 3–5, 7, 8, 16, 23).

[31] J. H. Silverman. "Errata and Corrections to *The Arithmetic of Elliptic Curves*, 2nd Edition". (2015) (cit. on p. 3).

[32] H. Smith. "Ramification in the Division Fields of Elliptic Curves and an Application to Sporadic Points on Modular Curves". arXiv:1810.04809. (2018) (cit. on p. 9).

[33] H. Söhngen. "Zur komplexen Multiplikation". In: *Mathematische Annalen* 111.1 (1935), pp. 302–328 (cit. on pp. 2, 23, 24).

[34] P. Stevenhagen. "Hilbert's 12th Problem, Complex Multiplication and Shimura Reciprocity". In: *Class Field Theory – Its Centenary and Prospect*. Mathematical Society of Japan, 2001, pp. 161–176 (cit. on pp. 2, 23, 24, 26).

[35] M. Streng. "Divisibility sequences for elliptic curves with complex multiplication." In: *Algebra & Number Theory* 2.2 (2008), pp. 183–208 (cit. on pp. 4, 5).

[36] D. Ulmer. "Conductors of ℓ-adic representations". In: *Proceedings of the American Mathematical Society* 144.6 (2016), pp. 2291–2299 (cit. on p. 20).

[37] L. C. Washington. *Elliptic curves*. Second edition. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2008 (cit. on p. 27).

[38] H. Yi and C. Lv. "On Ring Class Fields of Number Rings". arXiv:1810.04810. (2018) (cit. on pp. 24, 25).

Department of Mathematical Sciences, University of Copenhagen, Universitetsparken 5, 2100 Copenhagen, Denmark

E-mail address: campagna@math.ku.dk

E-mail address: pengo@math.ku.dk