ISOGENY GRAPHS OF ORDINARY ABELIAN VARIETIES

ERNEST HUNTER BROOKS, DIMITAR JETCHEV AND BENJAMIN WESOLOWSKI

Abstract. Fix a prime number ℓ. Graphs of isogenies of degree a power of ℓ are well-understood for elliptic curves, but not for higher-dimensional abelian varieties. We study the case of absolutely simple ordinary abelian varieties over a finite field. We analyse graphs of so-called $\mathfrak{l}$-isogenies, resolving that they are (almost) volcanoes in any dimension. Specializing to the case of principally polarizable abelian surfaces, we then exploit this structure to describe graphs of a particular class of isogenies known as (ℓ, ℓ)-isogenies: those whose kernels are maximal isotropic subgroups of the ℓ-torsion for the Weil pairing. We use these two results to write an algorithm giving a path of computable isogenies from an arbitrary absolutely simple ordinary abelian surface towards one with maximal endomorphism ring, which has immediate consequences for the CM-method in genus 2, for computing explicit isogenies, and for the random self-reducibility of the discrete logarithm problem in genus 2 cryptography.

1. Introduction

1.1. **Background.** Graphs of isogenies of principally polarized abelian varieties of dimension g have been an extensive object of study in both number theory and mathematical cryptology. When $g = 1$, Kohel [Koh96] gave a description of the structure of such graphs and used it to compute the endomorphism ring of an elliptic curve over a finite field. This description has subsequently been utilized in a variety of cryptographic applications such as point counting on elliptic curves [FM02], random self-reducibility of the elliptic curve discrete logarithm problem in isogeny classes [JMV05, JMV09], generating elliptic curves with a prescribed number of points via the CM method based on the Chinese Remainder Theorem [Sut12], as well as computing modular polynomials [BLS12].

When $g > 1$, the problem of describing the structure of these graphs becomes harder. The literature has seen a number of attempts to generalize Kohel's thesis, yet the structure of these isogeny graphs has not been studied systematically. For $g = 2$, Bröker, Gruenewald and Lauter [BGL11] proved that graphs of (ℓ, ℓ)-isogenies of abelian surfaces are not volcanoes. In [LR12a], Lauter and Robert observed that from a random abelian surface, it might not always be possible to reach an isogenous one with maximal endomorphism ring (locally at ℓ) using only (ℓ, ℓ)-isogenies. Following the footsteps of Kohel, Bisson [Bis15, Ch.5] sketched the relation between isogeny graphs and the lattice of orders in the endomorphism algebra for abelian varieties of higher dimension. This provides a first approximation of the global structure of the graphs, but allows no fine-grained analysis.

It was also unclear whether the notion of (ℓ, ℓ)-isogenies is the right one to generalize the structure of isogeny graphs. Ionica and Thomé [IT14] observed that

Date: September 30, 2016.

Key words and phrases. Isogeny graphs, (ℓ, ℓ)-isogenies, principally polarised abelian varieties, Jacobians of hyperelliptic curves, lattices in symplectic spaces, orders in CM-fields.

the subgraph of (ℓ,ℓ)-isogenies restricted to surfaces with maximal real order in K_0 (globally) could be studied through what they called $\mathfrak{l}$-isogenies, where $\mathfrak{l}$ is a prime ideal in K_0 above ℓ. They suggest that the $\mathfrak{l}$-isogeny graphs should be volcanoes, under certain assumptions[1]. When $\mathfrak{l}$ is principal, of prime norm, generated by a real, totally positive endomorphism β, then $\mathfrak{l}$-isogenies coincide with the cyclic β-isogenies from [DJR16] — an important notion, since these are the cyclic isogenies preserving principal polarizability.

Our main contributions include a full description of graphs of $\mathfrak{l}$-isogenies for any $g \geq 1$. This proves the claims of [IT14] and extends them to a much more general setting. For $g = 2$, we exploit this $\mathfrak{l}$-structure to provide a complete description of graphs of (ℓ,ℓ)-isogenies preserving the maximal real multiplication locally at ℓ. We also explore the structure of (ℓ,ℓ)-isogenies when the real multiplication is not necessarily locally maximal. As an application of these results, we build an algorithm that, given as input a principally polarized abelian surface, finds a path of computable isogenies leading to a surface with maximal endomorphism ring. This was a missing — yet crutial — building block for the CRT-based CM-method in dimension 2, for computing explicit isogenies between two given surfaces, and for the random self-reducibility of the discrete logarithm problem in genus 2 cryptography. Applications are discussed more thoroughly in Section 1.5.

This structure of $\mathfrak{l}$-isogenies, when one assumes that $\mathfrak{l}$ is of prime norm and trivial in the narrow class group of K_0, implies in particular that graphs of cyclic β-isogenies are volcanoes. In parallel to the present work, Chloe Martindale has recently announced a similar result on cyclic β-isogenies. It will be found in her forthcoming Ph.D. thesis, as part of a larger project aimed at computing Hilbert class polynomials and modular polynomials in genus 2. Her results, which are proven in a complex-analytic setting different from our ℓ-adic methods, yield the same description of the graph in this particular case.

1.2. **Setting.**

For a given ordinary, absolutely simple abelian variety $\mathscr{A}$ over a finite field $k = \mathbb{F}_q$, the associated endomorphism algebra $\mathrm{End}(\mathscr{A}) \otimes_{\mathbb{Z}} \mathbb{Q}$ is isomorphic to a CM-field K, i.e., a totally imaginary quadratic extension of a totally real number field K_0. Moreover, the dimension g of $\mathscr{A}$ equals the degree $[K_0 : \mathbb{Q}]$. The endomorphism ring $\mathrm{End}(\mathscr{A})$ identifies with an order $\mathcal{O}$ in K. The Frobenius endomorphism π of $\mathscr{A}$ generates the endomorphism algebra $K = \mathbb{Q}(\pi)$, and its characteristic polynomial determines its k-isogeny class, by Tate's isogeny theorem [Tat66]. In particular, since $\mathrm{End}_k(\mathscr{A}) = \mathrm{End}_{\overline{k}}(\mathscr{A})$ (see [Wat69, Thm.7.2.]), all isogenous varieties (over $\overline{k}$) share the same CM-field K, and their endomorphism rings all correspond to orders in K. Thus, the structure of isogeny graphs is related to the structure of the lattice of orders of the field K.

The choice of an isomorphism $\mathrm{End}(\mathscr{A}) \otimes_{\mathbb{Z}} \mathbb{Q} \cong K$ naturally induces an embedding $\imath_{\mathscr{B}} : \mathrm{End}(\mathscr{B}) \to K$ for any variety $\mathscr{B}$ that is isogenous to $\mathscr{A}$, and it does not depend on the choice of an isogeny. We can then unambiguously denote by $\mathcal{O}(\mathscr{B})$ the order in K corresponding to the endomorphism ring of any $\mathscr{B}$. Define the suborder $\mathcal{O}_0(\mathscr{A}) = \mathcal{O}(\mathscr{A}) \cap K_0$; the variety $\mathscr{A}$ is said to have *real multiplication* (RM) by

[1] The proof of [IT14, Prop.15] gives a count of the number of points at each level of the graph, but does not allow a conclusive statement on the edge structure, and thus does not appear to prove that the graph is a volcano.

$\mathcal{O}_0(\mathscr{A})$. Recall the conductor $\mathfrak{f}$ of an order $\mathcal{O}$ in a number field L is defined as

$$\mathfrak{f} = \{x \in L \mid x\mathcal{O}_L \subseteq \mathcal{O}\}.$$

Equivalently, it is the largest subset of L which is an ideal in both $\mathcal{O}_L$ and $\mathcal{O}$.

Fix once and for all a prime number ℓ different from the characteristic of the finite field k, and write $\mathfrak{o}(\mathscr{A}) = \mathcal{O}(\mathscr{A}) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$, the *local order* of $\mathscr{A}$. It is an order in the algebra $K_\ell = K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$. Also, $\mathfrak{o}_K = \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ is the maximal order in K_ℓ. Finally, write $\mathfrak{o}_0(\mathscr{A})$ for the *local real order* $\mathcal{O}_0(\mathscr{A}) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$, which is an order in the algebra $K_{0,\ell} = K_0 \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$, and let $\mathfrak{o}_0 = \mathcal{O}_{K_0} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$.

1.3. **Main results.** When $\mathscr{A}$ is an elliptic curve, the lattice of orders is simple: K being a quadratic number field (i.e. $K_0 = \mathbb{Q}$), all the orders in K are of the form $\mathcal{O}_c = \mathbb{Z} + c\mathcal{O}_K$, with $c \in \mathbb{Z}$ generating the conductor of $\mathcal{O}_c$. Locally at a prime number ℓ, the lattice of orders in K_ℓ is simply the chain $\mathfrak{o}_K \supset \mathbb{Z}_\ell + \ell\mathfrak{o}_K \supset \mathbb{Z}_\ell + \ell^2\mathfrak{o}_K \supset \ldots$. The (local) structure of the lattice of orders of a CM-field K is in general not as simple as the linear structure arising in the case of an imaginary quadratic field. This constitutes the main difficulty in generalizing the structural results to $g > 1$. For the rest of the paper, we let $g > 1$, and fix an isogeny class whose endomorphism algebra is the CM-field K.

1.3.1. *Isogeny graphs preserving the real multiplication.* In the case of quadratic number fields, the inclusion of orders corresponds to the divisibility relation of conductors. Neither the one-to-one correspondence between orders and conductors, nor the relationship between inclusion and divisibility holds in higher degree. We can, however, prove that such a correspondence between orders and conductors, and inclusion and divisibility still holds if we restrict to orders with maximal real multiplication, i.e., $\mathcal{O}_{K_0} \subset \mathcal{O}$. More than that, it even holds locally, i.e., for the orders of K_ℓ containing $\mathfrak{o}_0$. More precisely, we show in Section 2, Theorem 4, that any order in K (respectively K_ℓ) with maximal real multiplication is of the form $\mathcal{O}_{K_0} + \mathfrak{f}\mathcal{O}_K$ (respectively $\mathfrak{o}_0 + \mathfrak{f}\mathfrak{o}_K$) for some ideal $\mathfrak{f}$ in $\mathcal{O}_{K_0}$. Our first results use this classification to provide a complete description of graphs of isogenies preserving the maximal real multiplication locally at ℓ. The main building block for isogenies preserving the real multiplication is the notion of $\mathfrak{l}$-isogeny.

Definition 1.1 ($\mathfrak{l}$-isogeny). *Let $\mathfrak{l}$ be a prime above ℓ in K_0, and $\mathscr{A}$ a variety in the fixed isogeny class. Suppose $\mathfrak{l}$ is coprime to the conductor of $\mathcal{O}_0(\mathscr{A})$. An $\mathfrak{l}$-isogeny from $\mathscr{A}$ is an isogeny whose kernel is a proper, $\mathcal{O}_0(\mathscr{A})$-stable subgroup of*[2] $\mathscr{A}[\mathfrak{l}]$.

Remark 1.2. The degree of an $\mathfrak{l}$-isogeny is $N\mathfrak{l}$.

We will therefore study the structure of the graph $\mathscr{W}_\mathfrak{l}$ whose vertices are the isomorphism classes of abelian varieties $\mathscr{A}$ in the fixed isogeny class, which have maximal real multiplication locally at ℓ (i.e., $\mathfrak{o}_0 \subset \mathfrak{o}(\mathscr{A})$), and there is an edge of multiplicity m from such a vertex with representative $\mathscr{A}$ to a vertex $\mathscr{B}$ if there are m distinct subgroups $\kappa \subset \mathscr{A}$ that are kernels of $\mathfrak{l}$-isogenies such that $\mathscr{A}/\kappa \cong \mathscr{B}$ (of course, the multiplicity m does not depend on the choice of the representative $\mathscr{A}$).

Remark 1.3. When $\mathfrak{l}$ is trivial in the narrow class group of K_0, then $\mathfrak{l}$-isogenies preserve principal polarizability. The graph $\mathscr{W}_\mathfrak{l}$ does not account for polarizations, but it is actually easy to add polarizations back to graphs of unpolarized varieties, as will be discussed in Section 5.

[2] By abuse of notation, we write $\mathscr{A}[\mathfrak{l}]$ in place of $\mathscr{A}[\mathfrak{l} \cap \mathcal{O}(\mathscr{A})]$.

Each vertex $\mathscr{A}$ of this graph $\mathscr{W}_{\mathfrak{l}}$ has a level, given by the valuation $v_{\mathfrak{l}}(\mathscr{A})$ at $\mathfrak{l}$ of the conductor of $\mathcal{O}(\mathscr{A})$. Our first result, Theorem 1, completely describes the structure of the connected components of $\mathscr{W}_{\mathfrak{l}}$, which turns out to be closely related to the volcanoes observed for cyclic isogenies of elliptic curves. It is proven in Subsection 4.2.

Theorem 1. *Let $\mathscr{V}$ be any connected component of the leveled $\mathfrak{l}$-isogeny graph $(\mathscr{W}_{\mathfrak{l}}, v_{\mathfrak{l}})$. For each $i \geq 0$, let $\mathscr{V}_i$ be the subgraph of $\mathscr{V}$ at level i. We have:*

(i) For each $i \geq 0$, the varieties in $\mathscr{V}_i$ share a common endomorphism ring $\mathcal{O}_i$. The order $\mathcal{O}_0$ can be any order with locally maximal real multiplication at ℓ, whose conductor is not divisible by $\mathfrak{l}$;

(ii) The level $\mathscr{V}_0$ is isomorphic to the Cayley graph of the subgroup of $\operatorname{Pic}(\mathcal{O}_0)$ with generators the prime ideals above $\mathfrak{l}$; fixing $\mathscr{A} \in \mathscr{V}_0$, an isomorphism is given by sending any ideal class $[\mathfrak{a}]$ to the isomorphism class of $\mathscr{A}/\mathscr{A}[\mathfrak{a}]$;

(iii) For any $\mathscr{A} \in \mathscr{V}_0$, there are $\left(N(\mathfrak{l}) - \left(\frac{K}{\mathfrak{l}}\right)\right)/[\mathcal{O}_0^\times : \mathcal{O}_1^\times]$ edges of multiplicity $[\mathcal{O}_0^\times : \mathcal{O}_1^\times]$ from $\mathscr{A}$ to distinct vertices of $\mathscr{V}_1$ (where $\left(\frac{K}{\mathfrak{l}}\right)$ is -1, 0 or 1 if $\mathfrak{l}$ is inert, ramified, or split in K);

(iv) For each $i > 0$, and any $\mathscr{A} \in \mathscr{V}_i$, there is one simple edge from $\mathscr{A}$ to a vertex of $\mathscr{V}_{i-1}$, and $N(\mathfrak{l})/[\mathcal{O}_i^\times : \mathcal{O}_{i+1}^\times]$ edges of multiplicity $[\mathcal{O}_i^\times : \mathcal{O}_{i+1}^\times]$ to distinct vertices of $\mathscr{V}_{i+1}$, and there is no other edge from $\mathscr{A}$;

(v) For each path $\mathscr{A} \to \mathscr{B} \to \mathscr{C}$ where the first edge is descending, and the second ascending, we have $\mathscr{C} \cong \mathscr{A}/\mathscr{A}[\mathfrak{l}]$;

(vi) For each ascending edge $\mathscr{B} \to \mathscr{C}$, there is a descending edge $\mathscr{C} \to \mathscr{B}/\mathscr{B}[\mathfrak{l}]$.

In particular, the graph $\mathscr{V}$ is an $N(\mathfrak{l})$-volcano if and only if $\mathcal{O}_0^\times \subset K_0$ and $\mathfrak{l}$ is principal in $\mathcal{O}_0 \cap K_0$.

Also, if $\mathscr{V}$ contains a variety defined over the finite field k, the subgraph containing only the varieties defined over k consists of the subgraph of the first v levels, where v is the valuation at $\mathfrak{l}$ of the conductor of $\mathcal{O}_{K_0}[\pi] = \mathcal{O}_{K_0}[\pi, \pi^\dagger]$.

1.3.2. *Graphs of (ℓ, ℓ)-isogenies.* The following results focus on the case $g = 2$. In contrast to the case of elliptic curves, where a principal polarization always exists, the property of being principally polarizable is not even invariant under cyclic isogeny in genus 2. In addition, basic algorithms for computing isogenies of elliptic curves from a given kernel (such as Vélu's formulae [Vél71]) are difficult to generalize and the only known methods [Rob10b, CR15, LR12b, DJR16] assume certain hypotheses and thus do not apply for general isogenies of cyclic kernels. On the other hand, (ℓ, ℓ)-isogenies always preserve principal polarizability, and are computable with the most efficient of these algorithms [CR15]. These (ℓ, ℓ)-isogenies are therefore an important notion, and we are interested in understanding the structure of the underlying graphs.

Definition 1.4 ((ℓ, ℓ)-isogeny)**.** *Let $(\mathscr{A}, \xi_{\mathscr{A}})$ be a principally polarized abelian surface. We call an isogeny $\varphi\colon \mathscr{A} \to \mathscr{B}$ an (ℓ, ℓ)-isogeny (with respect to $\xi_{\mathscr{A}}$) if* $\ker(\varphi)$ *is a maximal isotropic subgroup of $\mathscr{A}[\ell]$ with respect to the Weil pairing on $\mathscr{A}[\ell]$ induced by the polarization isomorphism corresponding to $\xi_{\mathscr{A}}$.*

One knows that if $\varphi\colon \mathscr{A} \to \mathscr{B}$ is an (ℓ, ℓ)-isogeny, then there is a unique principal polarization $\xi_{\mathscr{B}}$ on $\mathscr{B}$ such that $\varphi^*\xi_{\mathscr{B}} = \xi_{\mathscr{A}}^\ell$ (this is a consequence of Grothendieck descent [Mum66, pp.290–291]; see also [Rob10a, Prop. 2.4.7]). This allows us to view an isogeny of *a priori* non-polarized abelian varieties φ as an isogeny of polarized abelian varieties $\varphi\colon (\mathscr{A}, \mathcal{L}^\ell) \to (\mathscr{B}, \mathcal{M})$.

First, we restrict our attention to abelian surfaces with maximal real multiplication at ℓ. The description of $\mathfrak{l}$-isogeny graphs provided by Theorem 1 leads to a complete understanding of graphs of (ℓ,ℓ)-isogenies preserving the maximal real order locally at ℓ, via the next theorem. More precisely, we study the structure of the graph $\mathscr{G}_{\ell,\ell}$ whose vertices are the isomorphism classes of principally polarizable surfaces $\mathscr{A}$ in the fixed isogeny class, which have maximal real multiplication locally at ℓ (i.e., $\mathfrak{o}_0 \subset \mathfrak{o}(\mathscr{A})$), with an edge of multiplicity m from such a vertex $\mathscr{A}$ to a vertex $\mathscr{B}$ if there are m distinct subgroups $\kappa \subset \mathscr{A}$ that are kernels of (ℓ,ℓ)-isogenies such that $\mathscr{A}/\kappa \cong \mathscr{B}$. This definition will be justified by the fact that the kernels of (ℓ,ℓ)-isogenies preserving the maximal real multiplication locally at ℓ do not depend on the choice of a principal polarization on the source (see Remark 7.10). The following theorem is proven in Subsection 7.2, where its consequences are discussed in details.

Theorem 2. *Suppose that $\mathscr{A}$ has maximal real multiplication locally at ℓ. Let ξ be any principal polarization on $\mathscr{A}$. There is a total of $\ell^3+\ell^2+\ell+1$ kernels of (ℓ,ℓ)-isogenies from $\mathscr{A}$ with respect to ξ. Among these, the kernels whose target also has maximal local real order do not depend on ξ, and are:*

(i) the ℓ^2+1 kernels of $\ell\mathcal{O}_{K_0}$-isogenies if ℓ is inert in K_0,

(ii) the $\ell^2+2\ell+1$ kernels of compositions of an $\mathfrak{l}_1$-isogeny with an $\mathfrak{l}_2$-isogeny if ℓ splits as $\mathfrak{l}_1\mathfrak{l}_2$ in K_0,

(iii) the $\ell^2+\ell+1$ kernels of compositions of two $\mathfrak{l}$-isogenies if ℓ ramifies as $\mathfrak{l}^2$ in K_0.

The other (ℓ,ℓ)-isogenies have targets with real multiplication by $\mathfrak{o}_1 = \mathbb{Z}_\ell + \ell\mathfrak{o}_0$.

Second, we look at (ℓ,ℓ)-isogenies when the real multiplication is not maximal at ℓ. Note that since $g = 2$, even though the lattice of orders in K is much more intricate than in the quadratic case, there still is some linearity when looking at the suborders $\mathcal{O}_0(\mathscr{A}) = \mathcal{O}(\mathscr{A}) \cap K_0$, since K_0 is a quadratic number field. For any variety $\mathscr{A}$ in the fixed isogeny class, there is an integer f, the conductor of $\mathcal{O}_0(\mathscr{A})$, such that $\mathcal{O}_0(\mathscr{A}) = \mathbb{Z} + f\mathcal{O}_{K_0}$. The local order $\mathfrak{o}_0(\mathscr{A})$ is exactly the order $\mathfrak{o}_n = \mathbb{Z}_\ell + \ell^n\mathfrak{o}_0$ in $K_{0,\ell}$, where $n = v_\ell(f)$ is the valuation of f at the prime ℓ.

The next result describes how (ℓ,ℓ)-isogenies can navigate between these “levels” of real multiplication. Let $\varphi\colon \mathscr{A} \to \mathscr{B}$ be an (ℓ,ℓ)-isogeny with respect to a polarization ξ on $\mathscr{A}$. If $\mathfrak{o}_0(\mathscr{A}) \subset \mathfrak{o}_0(\mathscr{B})$, we refer to φ as an *RM-ascending* isogeny; if $\mathfrak{o}_0(\mathscr{B}) \subset \mathfrak{o}_0(\mathscr{A})$, we call φ *RM-descending*; otherwise, if $\mathfrak{o}_0(\mathscr{A}) = \mathfrak{o}_0(\mathscr{B})$, φ is called *RM-horizontal.* Note that we start by considering (ℓ,ℓ)-isogenies defined over the algebraic closure of the finite field k; in virtue of Remark 3.3, it is then easy to deduce the results on isogenies defined over k. The following assumes $n > 0$ since the case $n = 0$ is taken care of by Theorem 2.

Theorem 3. *Suppose $\mathfrak{o}_0(\mathscr{A}) = \mathfrak{o}_n$ with $n > 0$. For any principal polarization ξ on $\mathscr{A}$, the kernels of (ℓ,ℓ)-isogenies from $(\mathscr{A},\xi)$ are:*

(i) A unique RM-ascending one, whose target has local order $\mathfrak{o}_{n-1}\cdot\mathfrak{o}(\mathscr{A})$ (in particular, its local real order is $\mathfrak{o}_{n-1}$, and the kernel is defined over the same field as $\mathscr{A}$),

(ii) $\ell^2+\ell$ RM-horizontal ones, and

(iii) ℓ^3 RM-descending isogenies, whose targets have local real order $\mathfrak{o}_{n+1}$.

The proof of this theorem is the matter of Section 6.

1.4. **Lattices in ℓ-adic symplectic spaces.** The theorems stated above are proven using a different approach from the currently available analyses of the structure of ℓ-power isogeny graphs. Rather than working with complex tori, we attach to an ℓ-isogeny of abelian varieties a pair of lattices in an ℓ-adic symplectic space, whose relative position is determined by the kernel of the isogeny, following the proof of Tate's isogeny theorem [Tat66].

Inspired by [CV04, §6], where the theory of Hecke operators on GL_2 is used to understand the CM elliptic curves isogenous to a fixed curve, we analyze the possible local endomorphism rings (in $K_\ell = K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$) for an analogous notion of "neighboring" lattices. This method gives a precise count of the horizontal isogenies as well as the vertical isogenies that increase or decrease the local endomorphism ring at ℓ.

1.5. **"Going up" and applications.** One of the applications of the above structural results is an algorithm that, given as input a principally polarized abelian surface, finds a path of computable isogenies leading to a surface with maximal endomorphism ring, when it is possible (and we can charaterize when it is possible). This algorithm is built and analysed in Section 8.

Such an algorithm has various applications. One of them is in generating (hyperelliptic) curves of genus 2 over finite fields with suitable security parameters via the CM method. The method is based on first computing invariants for the curve (Igusa invariants) and then using a method of Mestre [Mes91] (see also [CQ05]) to reconstruct the equation of the curve. The computation of the invariants is expensive and there are three different ways to compute their minimal polynomials (the Igusa class polynomials): 1) complex analytic techniques [vW99, Wen03, Str10]; 2) p-adic lifting techniques [CKL08, CL09, GHK$^+$06]; 3) a technique based on the Chinese Remainder Theorem [EL10, FL08, BGL11] (the *CRT method*).

Even if 3) is currently the least efficient method, it is also the least understood and deserves more attention: its analog for elliptic curves holds the records for time and space complexity and for the size of the computed examples [ES10, Sut11].

The CRT method of [BGL11] requires one to find an ordinary abelian surface $\mathscr{A}/\mathbb{F}_q$ whose endomorphism ring is the maximal order $\mathcal{O}_K$ of the quartic CM field K isomorphic to the endomorphism algebra $\mathrm{End}(\mathscr{A}) \otimes_{\mathbb{Z}} \mathbb{Q}$. This is obtained by trying random hyperelliptic curves $\mathscr{C}$ in the isogeny class and using the maximal endomorphism test of [FL08], thus making the algorithm quite inefficient.

In [LR12a], the authors propose a different method based on (ℓ, ℓ)-isogenies that does not require the endomorphism ring to be maximal (generalizing the method of Sutherland [Sut11] for elliptic curves). Starting from an arbitrary abelian surface in the isogeny class, the method is based on a probabilistic algorithm for "going up" to an abelian surface with maximal endomorphism ring. Although the authors cannot prove that the going-up algorithm succeeds with any fixed probability, the improvement is practical and heuristically, it reduces the running time of the CRT method in genus 2 from $\mathcal{O}(q^3)$ to $\mathcal{O}(q^{3/2})$. Our algorithm for going up takes inspiration from [LR12a], but exploits our new structural results on isogeny graphs.

A second application is in the computation of an explicit isogeny between any two given principally polarized abelian surfaces in the same isogeny class. An algorithm is given in [JW15] to find an isogeny between two such surfaces with maximal endomorphism ring. This can be extended to other pairs of isogenous principally polarized abelian surfaces, by first computing paths of isogenies to reach the maximal endomorphism ring, then applying the method of [JW15].

Similarly, this "going up" algorithm can also extend results about the random self-reducibility of the discrete logarithm problem in genus 2 cryptography. The results of [JW15] imply that if the discrete logarithm problem is efficiently solvable on a non-negligible proportion of the Jacobians with maximal endomorphism ring within an isogeny class, then it is efficiently solvable for all isogenous Jacobians with maximal endomorphism ring. For this to hold on any other Jacobian in the isogeny class, it only remains to compute a path of isogenies reaching the level of the maximal endomorphism ring.

Finally, we note that the "going-up" algorithm can also be applied in the computation of endomorphism rings of abelian surfaces over finite fields, thus extending the work of Bisson [Bis15]. This will be the subject of a forthcoming paper.

2. Orders

2.1. **Global and local orders.** An order in a number field is a full rank $\mathbb{Z}$-lattice which is also a subring. If ℓ is a prime, and L is a finite extension of $\mathbb{Q}_\ell$ or a finite product of finite extensions of $\mathbb{Q}_\ell$, an order in L is a full rank $\mathbb{Z}_\ell$-lattice which is also a subring. If K is a number field, write $K_\ell = K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$. In this section, if $\mathcal{O}$ an order in K, write $\mathcal{O}_\ell = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$; then $\mathcal{O}_\ell$ is an order in K_ℓ.

Lemma 2.1. *Given a number field K and a sequence $R(\ell)$ of orders in K_ℓ, such that $R(\ell)$ is the maximal order in K_ℓ for almost all ℓ, there exists a unique order $\mathcal{O}$ in K such that $\mathcal{O}_\ell = R(\ell)$ for all ℓ. This order $\mathcal{O}$ is the intersection $\bigcap_\ell (R(\ell) \cap K)$.*

Proof. This is well-known, but we include a proof for completeness. Let $n = [K : \mathbb{Q}]$ and pick a $\mathbb{Z}$-basis for the maximal order $\mathcal{O}_K$ of K. With this choice, a lattice Λ in $\mathcal{O}_K$ may be described by a matrix in $M_n(\mathbb{Z}) \cap \mathrm{GL}_n(\mathbb{Q})$ whose column vectors are a basis; this matrix is well-defined up to the left action of $\mathrm{GL}_n(\mathbb{Z})$. Similarly, a local lattice Λ_ℓ in K_ℓ may be described by a matrix in $M_n(\mathbb{Z}_\ell) \cap \mathrm{GL}_n(\mathbb{Q}_\ell)$, well-defined up to the left-action of $\mathrm{GL}_n(\mathbb{Z}_\ell)$. It thus suffices to prove that, given matrices $M_\ell \in M_n(\mathbb{Z}_\ell) \cap \mathrm{GL}_n(\mathbb{Q}_\ell)$, almost all of which are in $\mathrm{GL}_n(\mathbb{Z}_\ell)$, there exists an $N \in M_n(\mathbb{Z}) \cap \mathrm{GL}_n(\mathbb{Q})$ such that $NM_\ell^{-1} \in \mathrm{GL}_n(\mathbb{Z}_\ell)$. This follows from

$$\mathrm{GL}_n(\mathbb{A}_{\mathrm{fin}}) = \mathrm{GL}_n(\mathbb{Q}) \cdot \prod_\ell \mathrm{GL}_n(\mathbb{Z}_\ell),$$

a consequence of strong approximation for SL_n and the surjectivity of the determinant map $\mathrm{GL}_n(\mathbb{Z}_\ell) \to \mathbb{Z}_\ell^\times$ (see the argument in [Gel75, p. 52], which generalizes in an obvious way when $n > 2$). Finally, the identity $\mathcal{O} = \bigcap_\ell (\mathcal{O}_\ell \cap K)$ follows from the fact that $\tilde{\mathcal{O}} = \bigcap_\ell (\mathcal{O}_\ell \cap K)$ is an order in K such that $\tilde{\mathcal{O}}_\ell = \mathcal{O}_\ell$ for all ℓ. □

2.2. **Orders with maximal real multiplication.** Suppose that K_0 is a number field or finite product of extensions of $\mathbb{Q}_p$, and let K a quadratic extension of K_0 (i.e., an algebra of the form $K_0[x]/f(x)$, where f is a separable quadratic polynomial). The non-trivial element of $\mathrm{Aut}(K/K_0)$ will be denoted †. In the case that K is a CM-field and K_0 its maximally real subfield, Goren and Lauter [GL09] proved that if K_0 has a trivial class group, the orders with maximal real multiplication, i.e., the orders containing $\mathcal{O}_{K_0}$, are characterized by their conductor — under the assumption that ideals of $\mathcal{O}_K$ fixed by $\mathrm{Gal}(K/K_0)$ are ideals of $\mathcal{O}_{K_0}$ augmented to $\mathcal{O}_K$, which is rather restrictive, since it implies that no finite prime of K_0 ramifies in K. In that case, these orders are exactly the orders $\mathcal{O}_{K_0} + \mathfrak{f}_0\mathcal{O}_K$, for any ideal $\mathfrak{f}_0$ in $\mathcal{O}_{K_0}$. We generalize this result to an arbitrary quadratic extension; abusing language, we will continue to say an order of K has "maximal real multiplication" if it contains $\mathcal{O}_{K_0}$.

Theorem 4. *The map $\mathfrak{f}_0 \mapsto \mathcal{O}_{K_0} + \mathfrak{f}_0\mathcal{O}_K$ is a bijection between the set of ideals in $\mathcal{O}_{K_0}$ and the set of orders in K containing $\mathcal{O}_{K_0}$. More precisely,*

(i) for any ideal $\mathfrak{f}_0$ in $\mathcal{O}_{K_0}$, the conductor of $\mathcal{O}_{K_0} + \mathfrak{f}_0\mathcal{O}_K$ is $\mathfrak{f}_0\mathcal{O}_K$, and

(ii) for any order $\mathcal{O}$ in K with maximal real multiplication and conductor $\mathfrak{f}$, one has $\mathcal{O} = \mathcal{O}_{K_0} + (\mathfrak{f} \cap \mathcal{O}_{K_0})\mathcal{O}_K$.

Lemma 2.2. *An order $\mathcal{O}$ in K is stable under $\dagger$ if and only if $\mathcal{O} \cap K_0 = (\mathcal{O} + \mathcal{O}^\dagger) \cap K_0$.*

Proof. The direct implication is obvious. For the other direction, suppose $\mathcal{O}\cap K_0 = (\mathcal{O} + \mathcal{O}^\dagger) \cap K_0$ and let $x \in \mathcal{O}$. Then, $x + x^\dagger \in (\mathcal{O} + \mathcal{O}^\dagger) \cap K_0 = \mathcal{O} \cap K_0 \subset \mathcal{O}$, which proves that $x^\dagger \in \mathcal{O}$. □

Lemma 2.3. *Let $\mathfrak{f}$ and $\mathfrak{g}$ be two ideals in $\mathcal{O}_K$, such that $\mathfrak{g}$ divides $\mathfrak{f}$. Let $\pi : \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{f}$ be the natural projection. The canonical isomorphism between $(\mathcal{O}_{K_0}+\mathfrak{f})/\mathfrak{f}$ and $\mathcal{O}_{K_0}/(\mathcal{O}_{K_0}\cap\mathfrak{f})$ induces a bijection between $\pi(\mathcal{O}_{K_0}) \cap \pi(\mathfrak{g})$ and $(\mathcal{O}_{K_0}\cap\mathfrak{g})/(\mathcal{O}_{K_0}\cap\mathfrak{f})$.*

Proof. Any element in $\pi(\mathcal{O}_{K_0}) \cap \pi(\mathfrak{g})$ can be written as $\pi(x) = \pi(y)$ for some $x \in \mathcal{O}_{K_0}$ and $y \in \mathfrak{g}$. Then, $x - y \in \mathfrak{f} \subset \mathfrak{g}$, so $x = (x - y) + y \in \mathfrak{g}$. So

$$\pi(\mathfrak{g}) \cap \pi(\mathcal{O}_{K_0}) = \pi(\mathfrak{g} \cap \mathcal{O}_{K_0}) \cong (\mathfrak{g} \cap \mathcal{O}_{K_0})/(\mathfrak{f} \cap \mathcal{O}_{K_0}),$$

where the last relation comes from the canonical isomorphism between the rings $(\mathcal{O}_{K_0} + \mathfrak{f})/\mathfrak{f}$ and $\mathcal{O}_{K_0}/(\mathcal{O}_{K_0} \cap \mathfrak{f})$. □

Lemma 2.4. *Let $\mathcal{O}$ be an order in K of conductor $\mathfrak{f}$ with maximal real multiplication. Then, $\mathcal{O}$ is stable under $\dagger$ and $\mathfrak{f}$ comes from an ideal of $\mathcal{O}_{K_0}$, i.e., $\mathfrak{f} = \mathfrak{f}_0\mathcal{O}_K$, where $\mathfrak{f}_0$ is the $\mathcal{O}_{K_0}$-ideal $\mathfrak{f} \cap \mathcal{O}_K$.*

Proof. From Lemma 2.2, it is obvious that any order with maximal real multiplication is stable under $\dagger$. Its conductor $\mathfrak{f}$ is thereby a $\dagger$-stable ideal of $\mathcal{O}_K$. For any prime ideal $\mathfrak{p}_0$ in $\mathcal{O}_{K_0}$, let $\mathfrak{f}_{\mathfrak{p}_0}$ be the part of the factorization of $\mathfrak{f}$ that consists in prime ideals above $\mathfrak{p}_0$. Then, $\mathfrak{f} = \prod_{\mathfrak{p}_0} \mathfrak{f}_{\mathfrak{p}_0}$, and each $\mathfrak{f}_{\mathfrak{p}_0}$ is $\dagger$-stable. It is easy to see that each $\mathfrak{f}_{\mathfrak{p}_0}$ comes from an ideal of $\mathcal{O}_{K_0}$ when $\mathfrak{p}_0$ is inert or splits in $\mathcal{O}_K$. Now suppose it ramifies as $\mathfrak{p}_0\mathcal{O}_K = \mathfrak{p}^2$. Then $\mathfrak{f}_{\mathfrak{p}_0}$ is of the form $\mathfrak{p}^\alpha$. If α is even, $\mathfrak{f}_{\mathfrak{p}_0} = \mathfrak{p}_0^{\alpha/2}\mathcal{O}_K$. We now need to prove that α cannot be odd.

By contradiction, suppose $\alpha = 2\beta + 1$ for some integer β. Let $\pi : \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{f}$ be the canonical projection. The ring $\pi(\mathcal{O})$ contains $\pi(\mathcal{O}_{K_0}) = (\mathcal{O}_{K_0} + \mathfrak{f})/\mathfrak{f}$. Write $\mathfrak{f} = \mathfrak{p}^\alpha\mathfrak{g}$ and let us prove that $\pi(\mathfrak{p}^{\alpha-1}\mathfrak{g}) \subset \pi(\mathcal{O}_{K_0})$. From Lemma 2.3,

$$\left|\pi(\mathcal{O}_{K_0}) \cap \pi(\mathfrak{p}^{\alpha-1}\mathfrak{g})\right| = |\mathfrak{p}_0^\beta\mathfrak{g}_0/\mathfrak{p}_0^{\beta+1}\mathfrak{g}_0| = N(\mathfrak{p}_0) = N(\mathfrak{p}) = |\pi(\mathfrak{p}^{\alpha-1}\mathfrak{g})|,$$

where N denotes the absolute norm, so $\pi(\mathfrak{p}^{\alpha-1}\mathfrak{g}) \subset \pi(\mathcal{O}_{K_0}) \subset \pi(\mathcal{O})$. Finally,

$$\mathfrak{p}^{\alpha-1}\mathfrak{g} = \pi^{-1}(\pi(\mathfrak{p}^{\alpha-1}\mathfrak{g})) \subset \pi^{-1}(\pi(\mathcal{O})) = \mathcal{O},$$

which contradicts the fact that $\mathfrak{f}$ is the biggest ideal of $\mathcal{O}_K$ contained in $\mathcal{O}$. □

Lemma 2.5. *Let $\mathfrak{f}_0$ be an ideal in $\mathcal{O}_{K_0}$, and $R = \mathcal{O}_{K_0}/\mathfrak{f}_0$. There is an element $\alpha \in \mathcal{O}_K$ such that $\mathcal{O}_K/\mathfrak{f}_0\mathcal{O}_K = R \oplus R\alpha$.*

Proof. The order $\mathcal{O}_K$ is a module over $\mathcal{O}_{K_0}$. It is locally free, and finitely generated, thus it is projective. Since $\mathcal{O}_{K_0}$ is a regular ring, the submodule $\mathcal{O}_{K_0}$ in $\mathcal{O}_K$ is a direct summand, i.e., there is an $\mathcal{O}_{K_0}$-submodule M of $\mathcal{O}_K$ such that $\mathcal{O}_K = \mathcal{O}_{K_0} \oplus M$. Then, $\mathcal{O}_K/\mathfrak{f}_0\mathcal{O}_K = R \oplus M/\mathfrak{f}_0 M$. Let A be $\mathbb{Z}$ if K is a number field and $\mathbb{Z}_p$ if it is a finite product of extensions of $\mathbb{Q}_p$. In the former case write n for $[K : \mathbb{Q}]$ and in the latter for the dimension of K_p as a $\mathbb{Q}_p$-vector space. As modules over A, $\mathcal{O}_K$ is of rank $2n$ and $\mathcal{O}_{K_0}$ of rank n, hence M must be of rank n. Therefore, as an $\mathcal{O}_{K_0}$-module, M is isomorphic to an ideal $\mathfrak{a}$ in $\mathcal{O}_{K_0}$, so $M/\mathfrak{f}_0 M \cong \mathfrak{a}/\mathfrak{f}_0\mathfrak{a} \cong R$. So there is an element $\alpha \in M$ such that $M/\mathfrak{f}_0 M = R\alpha$. □

Proof of Theorem 4. For (i), let $\mathfrak{f}_0$ be an ideal in $\mathcal{O}_{K_0}$, and write $\mathfrak{f} = \mathfrak{f}_0\mathcal{O}_K$. Let $\mathfrak{c}$ be the conductor of $\mathcal{O}_{K_0} + \mathfrak{f}$. From Lemma 2.4, $\mathfrak{c}$ is of the form $\mathfrak{c}_0\mathcal{O}_K$ where $\mathfrak{c}_0 = \mathcal{O}_{K_0} \cap \mathfrak{c}$. Clearly $\mathfrak{f} \subset \mathfrak{c}$, so $\mathfrak{c}_0 \mid \mathfrak{f}_0$ and we can write $\mathfrak{f}_0 = \mathfrak{c}_0\mathfrak{g}_0$. Let $\pi : \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{f}$ be the canonical projection. Since $\mathfrak{c} \subset \mathcal{O}_{K_0} + \mathfrak{f}$, we have $\pi(\mathfrak{c}) \subset \pi(\mathcal{O}_{K_0})$. From Lemma 2.3,

$$|\pi(\mathfrak{c})| = |\pi(\mathcal{O}_{K_0}) \cap \pi(\mathfrak{c})| = |\mathfrak{c}_0/\mathfrak{f}_0| = N(\mathfrak{g}_0).$$

On the other hand, $|\pi(\mathfrak{c})| = |\mathfrak{c}/\mathfrak{f}| = N(\mathfrak{g}_0\mathcal{O}_K) = N(\mathfrak{g}_0)^2$, so $N(\mathfrak{g}_0) = 1$, hence $\mathfrak{c} = \mathfrak{f}$. To prove (ii), let $\mathcal{O}$ be an order in K with maximal real multiplication and conductor $\mathfrak{f}$. From Lemma 2.4, $\mathcal{O}$ is †-stable and $\mathfrak{f} = \mathfrak{f}_0\mathcal{O}_K$, where $\mathfrak{f}_0 = \mathfrak{f} \cap \mathcal{O}_{K_0}$. We claim that if $x \in \mathcal{O}$ then $x \in \mathcal{O}_{K_0} + \mathfrak{f}$. Let $R = \mathcal{O}_{K_0}/\mathfrak{f}_0$. By Lemma 2.5, $\mathcal{O}_K/\mathfrak{f} = R \oplus R\alpha$. The quotient $\mathcal{O}/\mathfrak{f}$ is an R-submodule of $\mathcal{O}_K/\mathfrak{f}$. There are two elements $y, z \in R$ such that $x + \mathfrak{f} = y + z\alpha$. Then, $z\alpha \in \mathcal{O}/\mathfrak{f}$, and we obtain that $(zR)\alpha \subset \mathcal{O}/\mathfrak{f}$. There exists an ideal $\mathfrak{g}_0$ dividing $\mathfrak{f}_0$ such that $zR = \mathfrak{g}_0/\mathfrak{f}_0$. Therefore $(\mathfrak{g}_0/\mathfrak{f}_0)\alpha \subset \mathcal{O}/\mathfrak{f}$. Then,

$$\mathfrak{g}/\mathfrak{f} \subset R + (\mathfrak{g}_0/\mathfrak{f}_0)\alpha \subset \mathcal{O}/\mathfrak{f},$$

where $\mathfrak{g} = \mathfrak{g}_0\mathcal{O}_K$, which implies that $\mathfrak{g} \subset \mathcal{O}$. But $\mathfrak{g}$ divides $\mathfrak{f}$, and $\mathfrak{f}$ is the largest $\mathcal{O}_K$-ideal in $\mathcal{O}$, so $\mathfrak{g} = \mathfrak{f}$. Hence $z \in \mathfrak{f}$, and $x \in \mathcal{O}_{K_0} + \mathfrak{f}$. □

3. From abelian surfaces to lattices, and vice-versa

3.1. **Tate modules and isogenies.** Consider again the setting introduced in Subsection 1.2, with $\mathscr{A}$ an abelian variety over the finite field k in the fixed isogeny class — ordinary, absolutely simple, and of dimension g. Write $T = T_\ell\mathscr{A}$ for the ℓ-adic Tate module of $\mathscr{A}$, and V for $T \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. Then V is a $2g$-dimensional $\mathbb{Q}_\ell$-vector space with an action of the algebra K_ℓ, over which it has rank one, and T is similarly of rank one over the ring $\mathfrak{o}(\mathscr{A}) = \mathcal{O}(\mathscr{A}) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. Write π for the Frobenius endomorphism of $\mathscr{A}$, viewed as an element of $\mathcal{O}(\mathscr{A})$.

The elements of T are the sequences $(Q_n)_{n\geq 0}$ with $Q_n \in \mathscr{A}[\ell^n]$, $\ell Q_n = Q_{n-1}$ for all $n \geq 1$. An element of V identifies with a sequence $(P_n)_{n\geq 0}$ with $P_n \in \mathscr{A}[\ell^\infty]$ and $\ell P_n = P_{n-1}$ for $n \geq 1$ as follows:

$$(Q_n)_{n\geq 0} \otimes \ell^{-m} \longmapsto (Q_{n+m})_{n\geq 0},$$

and under this identification, T is the subgroup of V where $P_0 = 0 \in \mathscr{A}[\ell^\infty]$. The projection to the zeroth coordinate then yields a canonical identification

$$V/T \xrightarrow{\sim} \mathscr{A}[\ell^\infty](\bar{k}), \tag{1}$$

under which the action of π on the left-hand side corresponds to the action of the arithmetic Frobenius element in $\mathrm{Gal}(\overline{k}/k)$ on the right-hand side.

We are now ready to state the main correspondence between lattices in V containing the Tate module T and ℓ-power isogenies from $\mathscr{A}$.

Proposition 3.1. *There is a one-to-one correspondence*

$$\{\textit{Lattices in } V \textit{ containing } T\} \cong \{\textit{finite subgroups of } \mathscr{A}[\ell^\infty]\},$$

where a lattice Γ is sent to the subgroup Γ/T, through the identification (1)*. Under this correspondence,*

- *(i) A lattice is stable under π^n if and only if the corresponding subgroup is defined over the degree n extension $\mathbb{F}_{q^n}$ of k.*
- *(ii) If a subgroup $\kappa \subset \mathscr{A}[\ell^\infty]$ corresponds to a lattice Γ, then the order of K_ℓ of elements stabilizing Γ is $\mathfrak{o}(\mathscr{A}/\kappa)$.*

Proof. A lattice Γ in V is sent to the subgroup κ of $\mathscr{A}[\ell^\infty]$ corresponding to Γ under (1). Conversely, give a subgroup $\kappa \subset \mathscr{A}[\ell^\infty]$, let Γ be the set of sequences in V whose zeroth coordinate is in κ. It follows that the subgroup of $\mathscr{A}[\ell^\infty]$ corresponding to this lattice under (1) is κ, so that this process is indeed bijective.

The claim about fields of definition follows from the previously-discussed Frobenius equivariance of (1). The claim about endomorphism rings is Tate's isogeny theorem applied to $\mathrm{Hom}(\mathscr{A}/\kappa, \mathscr{A}/\kappa)$. □

Remark 3.2. Observe that given a subgroup $\kappa \subset \mathscr{A}[\ell^\infty]$, any two isogenies of kernel κ differ only by an isomorphism between the targets. Therefore if $\varphi : \mathscr{A} \to \mathscr{B}$ is any isogeny of kernel κ, then $\mathfrak{o}(\mathscr{A}/\kappa) = \mathfrak{o}(\mathscr{B})$.

Remark 3.3. Recall that all varieties and morphisms are considered over $\overline{k}$. We are however also interested in the structures arising when restricting to varieties and morphisms defined over k, in the sense of Subsection 1.2. To this end, the most important fact (which is special to the case of simple, ordinary abelian varieties) is that if a variety $\mathscr{B}$ is k-isogenous to $\mathscr{A}$, then any isogeny $\mathscr{A} \to \mathscr{B}$ is defined over k (this is an easy consequence of [Wat69, Thm.7.2.]: if $\mathscr{B}$ is defined over k, and $\varphi, \psi : \mathscr{A} \to \mathscr{B}$ are two isogenies then $\varphi \circ \psi^{-1}$ is an element of $\mathrm{End}(\mathscr{B}) \otimes_{\mathbb{Z}} \mathbb{Q}$, hence defined over k, so φ is defined over k if and only if ψ is). Similarly to Remark 3.2, if κ is defined over k, any two k-isogenies of kernel κ differ by a k-isomorphism between the targets. From Proposition 3.1(ii), if $\pi \in \mathfrak{o}(\mathscr{A}/\kappa)$, then κ is defined over k, and is thereby the kernel of a k-isogeny[3]. We obtain a correspondence between subgroups κ defined over k and Γ lattices stabilized by π.

The following proposition justifies the strategy of working locally at ℓ, as it guarantees that ℓ-power isogenies do not affect endomorphism rings at primes $\ell' \neq \ell$.

Proposition 3.4. *Let $\varphi : \mathscr{A} \to \mathscr{B}$ be an isogeny of abelian varieties of ℓ-power degree. Then for any prime $\ell' \neq \ell$ of $\mathscr{A}$, one has $\mathcal{O}(\mathscr{A}) \otimes_{\mathbb{Z}} \mathbb{Z}_{\ell'} = \mathcal{O}(\mathscr{B}) \otimes_{\mathbb{Z}} \mathbb{Z}_{\ell'}$.*

Proof. Let $\mathcal{C}_{\ell'}$ be the category whose objects are abelian varieties over $\overline{k}$ and whose morphisms are $\mathrm{Hom}_{\mathcal{C}_{\ell'}}(\mathscr{A}_1, \mathscr{A}_2) = \mathrm{Hom}(\mathscr{A}_1, \mathscr{A}_2) \otimes_{\mathbb{Z}} \mathbb{Z}_{\ell'}$. There exists an isogeny $\hat{\varphi} : \mathscr{B} \to \mathscr{A}$ such that $\hat{\varphi} \circ \varphi = [\ell^n]$, so φ induces an isomorphism in $\mathcal{C}_{\ell'}$; it follows that the endomorphism rings of $\mathscr{A}$ and $\mathscr{B}$ in this category are identified. □

[3] Note that in general, if $\mathscr{B}$ is $\overline{k}$-isogenous to $\mathscr{A}$ and $\pi \in \mathcal{O}(\mathscr{B})$, then π does not necessarily correspond to the k-Frobenius of $\mathscr{B}$ unless $\mathscr{B}$ is actually k-isogenous to $\mathscr{A}$.

3.2. Polarizations and symplectic structures.

Fix a polarization ξ of $\mathscr{A}$. It induces a polarization isogeny $\lambda : \mathscr{A} \to \mathscr{A}^\vee$, which in turn gives a map $T \to T_\ell(\mathscr{A}^\vee)$. Therefore the Weil pairing equips T with a natural $\mathbb{Z}_\ell$-linear pairing $\langle -, - \rangle$, which extends to a pairing on V. We gather standard facts about this pairing in the following lemma.

Lemma 3.5. *One has:*

(i) The pairing $\langle -, - \rangle$ is symplectic.

(ii) For any $\alpha \in K$, one has

$$\langle \alpha x, y \rangle = \langle x, \alpha^\dagger y \rangle,$$

where $\dagger$ denotes the complex conjugation.

(iii) For Γ a lattice in V, write

$$\Gamma^* = \{\alpha \in V \mid \langle \alpha, \Gamma \rangle \subset \mathbb{Z}_\ell\}$$

for the dual lattice of Γ. Then $T \subset T^*$, and the quotient is isomorphic to $(\ker \lambda)[\ell^\infty]$. In particular, T is self-dual if and only if the degree of λ is coprime to ℓ.

Proof. The first two claims are standard — see [Mil86, Lemma 16.2e, and §167]. For the third, note that T^* identifies with $\lambda_*^{-1}(T_\ell \mathscr{A}^\vee)$, and λ_* induces an isomorphism

$$\lambda_*^{-1}(T_\ell \mathscr{A}^\vee)/T \xrightarrow{\sim} \ker(\lambda)[\ell^\infty].$$

□

4. Graphs of $\mathfrak{l}$-isogenies

In this section we study $\mathfrak{l}$-isogenies through the lens of lattices in an ℓ-adic vector space, endowed with an action of the algebra K_ℓ.

4.1. Lattices with locally maximal real multiplication.

Throughout this subsection, V is a $\mathbb{Q}_\ell$-vector space of dimension $2g$, ℓ is a prime number, K is a quartic CM-field, with K_0 its maximal real subfield. The algebra K_ℓ is a $\mathbb{Q}_\ell$-algebra of dimension $2g$. Suppose that it acts ($\mathbb{Q}_\ell$-linearly) on V. Define the *order* of a full-rank $\mathbb{Z}_\ell$-lattice $\Lambda \subset V$ as

$$\mathfrak{o}(\Lambda) = \{x \in K_\ell \mid x\Lambda \subset \Lambda\}.$$

For any order $\mathfrak{o}$ in K_ℓ, say that Λ is an $\mathfrak{o}$-lattice if $\mathfrak{o}(\Lambda) = \mathfrak{o}$. Let $\mathfrak{o} = \mathfrak{o}(\Lambda)$ be the order of Λ, and suppose that it has maximal real multiplication, i.e., that $\mathfrak{o}$ contains the maximal order $\mathfrak{o}_0$ of $K_{0,\ell} = K_0 \otimes_\mathbb{Q} \mathbb{Q}_\ell$. We now need some commutative algebra:

Lemma 4.1. *Let A be a Dedekind domain with field of fractions F, and let L be a quadratic extension of F. If $\mathcal{O}$ is any A-subalgebra of the integral closure of A in L, with $\mathcal{O} \otimes K = L$, then $\mathcal{O}$ is Gorenstein.*

Proof. The hypotheses and result are local on Spec$A$, so we may take A a principal ideal domain. Then $\mathcal{O}$ is a free A-module, which must be 2-dimensional. The element $1 \in \mathcal{O}$ is not an A-multiple of any element of $\mathcal{O}$, so there is a basis $\{1, \alpha\}$ for $\mathcal{O}$ as an A-module; clearly $\mathcal{O} = A[\alpha]$ as A-algebras. The result then follows from [BL94, Ex.2.8]. □

By Lemma 4.1, the order $\mathfrak{o}$, which has maximal real multiplication, is a Gorenstein ring and Λ is a free $\mathfrak{o}$-module of rank 1. Recall the notations $\mathfrak{o}_K = \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ and $\mathfrak{o}_0 = \mathcal{O}_{K_0} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ from Section 1.2. For any ideal $\mathfrak{f}$ in $\mathfrak{o}_0$, let $\mathfrak{o}_\mathfrak{f} = \mathfrak{o}_0 + \mathfrak{f}\mathfrak{o}_K$. From Theorem 4, all the orders containing $\mathfrak{o}_0$ are of this form.

Definition 4.2 ($\mathfrak{l}$-neighbors)**.** *Let Λ be a lattice with maximal real multiplication, and let $\mathfrak{l}$ be a prime ideal in $\mathfrak{o}_0$. The set $\mathscr{L}_\mathfrak{l}(\Lambda)$ of* $\mathfrak{l}$-neighbors *of Λ consists of all the lattices Γ such that $\mathfrak{l}\Lambda \subset \Gamma \subset \Lambda$, and $\Gamma/\mathfrak{l}\Lambda \cong \mathfrak{o}_0/\mathfrak{l}$, i.e., $\Gamma/\mathfrak{l}\Lambda \in \mathbb{P}^1(\Lambda/\mathfrak{l}\Lambda)$.*

Remark 4.3. Consider the lattice $T = T_\ell\mathscr{A}$. Then, $\mathfrak{l}$-isogenies $\mathscr{A} \to \mathscr{B}$ (see Definition 1.1) correspond under Proposition 3.1 to lattices Γ with $T \subset \Gamma \subset \mathfrak{l}^{-1}T$ and Γ/T is an $\mathfrak{o}_0/\mathfrak{l}$-subspace of dimension one of $(\mathfrak{l}^{-1}T)/T$.

The following lemma is key to understanding $\mathfrak{l}$-neighbors. It arises from the technique employed by Cornut and Vatsal [CV04, §6] to study the action of a certain Hecke algebra on quadratic CM-lattices.

Lemma 4.4. *Let K be a CM-field, and K_0 its maximal real subfield. Let $\mathfrak{l}$ be a prime ideal in $\mathfrak{o}_0$, and $\mathbb{F} = \mathfrak{o}_0/\mathfrak{l}$. Let $\mathfrak{f}$ be an ideal in $\mathfrak{o}_0$ and $\mathfrak{o}_\mathfrak{f} = \mathfrak{o}_0 + \mathfrak{f}\mathfrak{o}_K$. The action of $\mathfrak{o}_\mathfrak{f}^\times$ on the set of $\mathbb{F}$-lines $\mathbb{P}^1(\mathfrak{o}_\mathfrak{f}/\mathfrak{l}\mathfrak{o}_\mathfrak{f})$ factors through $\mathfrak{o}_\mathfrak{f}^\times/\mathfrak{o}_{\mathfrak{l}\mathfrak{f}}^\times$. Let $\mathfrak{L}$ be a prime in $\mathfrak{o}_\mathfrak{f}$ above $\mathfrak{l}$. The fixed points are*

$$\mathbb{P}^1(\mathfrak{o}_\mathfrak{f}/\mathfrak{l}\mathfrak{o}_\mathfrak{f})^{\mathfrak{o}_\mathfrak{f}^\times} = \begin{cases} \emptyset & \text{if } \mathfrak{l} \nmid \mathfrak{f} \text{ and } \mathfrak{l}\mathfrak{o}_\mathfrak{f} = \mathfrak{L}, \\ \{\mathfrak{L}/\mathfrak{l}\mathfrak{o}_\mathfrak{f}, \mathfrak{L}^\dagger/\mathfrak{l}\mathfrak{o}_\mathfrak{f}\} & \text{if } \mathfrak{l} \nmid \mathfrak{f} \text{ and } \mathfrak{l}\mathfrak{o}_\mathfrak{f} = \mathfrak{L}\mathfrak{L}^\dagger, \\ \{(\mathfrak{l}\mathfrak{o}_{\mathfrak{l}^{-1}\mathfrak{f}})/\mathfrak{l}\mathfrak{o}_\mathfrak{f}\} & \text{if } \mathfrak{l} \mid \mathfrak{f}. \end{cases}$$

The remaining points are permuted simply transitively by $\mathfrak{o}_\mathfrak{f}^\times/\mathfrak{o}_{\mathfrak{l}\mathfrak{f}}^\times$.

Proof. The ring $\mathfrak{o}_{\mathfrak{l}\mathfrak{f}}^\times$ acts trivially on $\mathbb{P}^1(\mathfrak{o}_\mathfrak{f}/\mathfrak{l}\mathfrak{o}_\mathfrak{f})$, which proves the first statement. Observe that the projection $\mathfrak{o}_\mathfrak{f} \to \mathfrak{o}_\mathfrak{f}/\mathfrak{o}_{\mathfrak{l}\mathfrak{f}}$ induces a canonical isomorphism between $\mathfrak{o}_\mathfrak{f}^\times/\mathfrak{o}_{\mathfrak{l}\mathfrak{f}}^\times$ and $(\mathfrak{o}_\mathfrak{f}/\mathfrak{l}\mathfrak{o}_\mathfrak{f})^\times/\mathbb{F}^\times$. Suppose that $\mathfrak{l}$ divides $\mathfrak{f}$. Then, there exists an element $\epsilon \in \mathfrak{o}_\mathfrak{f}/\mathfrak{l}\mathfrak{o}_\mathfrak{f}$ such that $\mathfrak{o}_\mathfrak{f}/\mathfrak{l}\mathfrak{o}_\mathfrak{f} = \mathbb{F}[\epsilon]$ and $\epsilon^2 = 0$. But the only $\mathbb{F}$-line in $\mathbb{F}[\epsilon]$ fixed by the action of $\mathbb{F}[\epsilon]^\times$ is $\epsilon\mathbb{F} = (\mathfrak{l}\mathfrak{o}_{\mathfrak{l}^{-1}\mathfrak{f}})/\mathfrak{l}\mathfrak{o}_\mathfrak{f}$, and this action is transitive on the ℓ other lines. Therefore the action of $\mathbb{F}[\epsilon]^\times/\mathbb{F}^\times = (\mathfrak{o}_\mathfrak{f}/\mathfrak{l}\mathfrak{o}_\mathfrak{f})^\times/\mathbb{F}^\times$ on these ℓ lines is simply transitive.

Now, suppose that $\mathfrak{l}$ does not divide $\mathfrak{f}$. If $\mathfrak{l}$ is inert in $\mathfrak{o}_\mathfrak{f}$, then $\mathfrak{o}_\mathfrak{f}/\mathfrak{l}\mathfrak{o}_\mathfrak{f} = \mathbb{K}$ is a quadratic field extension of $\mathbb{F}$, and $\mathbb{K}^\times/\mathbb{F}^\times$ acts simply transitively on the $\mathbb{F}$-lines $\mathbb{P}^1(\mathbb{K})$. To statement follows from the isomorphism between $\mathbb{K}^\times/\mathbb{F}^\times$ and $\mathfrak{o}_\mathfrak{f}^\times/\mathfrak{o}_{\mathfrak{l}\mathfrak{f}}^\times$. The cases where $\mathfrak{l}$ splits or ramifies in K are treated similarly, with $\mathfrak{o}_\mathfrak{f}/\mathfrak{l}\mathfrak{o}_\mathfrak{f} \cong \mathbb{F}^2$ in the first case, and $\mathfrak{o}_\mathfrak{f}/\mathfrak{l}\mathfrak{o}_\mathfrak{f} \cong \mathbb{F}[X]/(X^2)$ in the second case. □

Proposition 4.5 (Structure of $\mathscr{L}_\mathfrak{l}(\Lambda)$)**.** *Suppose Λ is an $\mathfrak{o}_\mathfrak{f}$-lattice, for some $\mathfrak{o}_0$-ideal $\mathfrak{f}$, and let $\mathfrak{l}$ be a prime ideal in $\mathfrak{o}_0$. The lattice Λ has $N(\mathfrak{l}) + 1$ $\mathfrak{l}$-neighbors. The $\mathfrak{l}$-neighbors that have order $\mathfrak{o}_{\mathfrak{l}\mathfrak{f}}$ are permuted simply transitively by $(\mathfrak{o}_\mathfrak{f}/\mathfrak{o}_{\mathfrak{l}\mathfrak{f}})^\times$. The other $\mathfrak{l}$-neighbors have order $\mathfrak{o}_{\mathfrak{l}^{-1}\mathfrak{f}}$ if $\mathfrak{l}$ divides $\mathfrak{f}$, or $\mathfrak{o}_K$ otherwise.*

More explicitly, if $\mathfrak{l}$ divides $\mathfrak{f}$, there is one $\mathfrak{l}$-neighbor of order $\mathfrak{o}_{\mathfrak{l}^{-1}\mathfrak{f}}$, namely $\mathfrak{l}\mathfrak{o}_{\mathfrak{l}^{-1}\mathfrak{f}}\Lambda$, and $N(\mathfrak{l})$ $\mathfrak{l}$-neighbors of order $\mathfrak{o}_{\mathfrak{l}\mathfrak{f}}$. If $\mathfrak{l}$ does not divide $\mathfrak{f}$, we have:

(i) If $\mathfrak{l}$ is inert in K, all $N(\mathfrak{l}) + 1$ lattices of $\mathscr{L}_\mathfrak{l}(\Lambda)$ have order $\mathfrak{o}_\mathfrak{l}$,

(ii) If $\mathfrak{l}$ splits in K into prime ideals $\mathfrak{L}_1$ and $\mathfrak{L}_2$, $\mathscr{L}_\mathfrak{l}(\Lambda)$ consists of two lattices of order $\mathfrak{o}_K$, namely $\mathfrak{L}_1\Lambda$ and $\mathfrak{L}_2\Lambda$, and $N(\mathfrak{l}) - 1$ lattices of order $\mathfrak{o}_\mathfrak{l}$,

(iii) If $\mathfrak{l}$ ramifies in K as $\mathfrak{L}^2$, $\mathscr{L}_\mathfrak{l}(\Lambda)$ consists of one lattice of order $\mathfrak{o}_K$, namely $\mathfrak{L}\Lambda$, and $N(\mathfrak{l})$ lattices of order $\mathfrak{o}_\mathfrak{l}$.

Proof. This is a direct consequence of Lemma 4.4, together with the fact that Λ is a free $\mathfrak{o}_{\mathfrak{f}}$-module of rank 1. □

4.2. **Graphs of $\mathfrak{l}$-isogenies.** Fix again a principally polarizable absolutely simple ordinary abelian variety $\mathscr{A}$ of dimension g over k, with endomorphism algebra K. Suppose that $\mathscr{A}$ has locally maximal real multiplication at ℓ (i.e., $\mathfrak{o}_0 \subset \mathfrak{o}(\mathscr{A})$). The $\mathfrak{l}$-neighbors correspond in the world of varieties to $\mathfrak{l}$-isogenies (see Remark 4.3).

Definition 4.6. *Suppose $\mathscr{A}$ has local order $\mathfrak{o}_{\mathfrak{f}}$, for some $\mathfrak{o}_0$-ideal $\mathfrak{f}$ and let $\mathfrak{l}$ be a prime ideal in $\mathfrak{o}_0$. An $\mathfrak{l}$-isogeny $\varphi : \mathscr{A} \to \mathscr{B}$ is* $\mathfrak{l}$-ascending *if $\mathfrak{o}(\mathscr{B}) = \mathfrak{o}_{\mathfrak{l}^{-1}\mathfrak{f}}$, it is* $\mathfrak{l}$-descending *if $\mathfrak{o}(\mathscr{B}) = \mathfrak{o}_{\mathfrak{l}\mathfrak{f}}$, and it is* $\mathfrak{l}$-horizontal *if $\mathfrak{o}(\mathscr{B}) = \mathfrak{o}_{\mathfrak{f}}$.*

Proposition 4.7. *Suppose $\mathscr{A}$ has local order $\mathfrak{o}_{\mathfrak{f}}$ for some $\mathfrak{o}_0$-ideal $\mathfrak{f}$ and let $\mathfrak{l}$ be a prime ideal in $\mathfrak{o}_0$. There are $N(\mathfrak{l})+1$ kernels of $\mathfrak{l}$-isogenies from $\mathscr{A}$. The kernels of $\mathfrak{l}$-descending $\mathfrak{l}$-isogenies are permuted simply transitively by the action of $(\mathfrak{o}_{\mathfrak{f}}/\mathfrak{o}_{\mathfrak{l}\mathfrak{f}})^{\times}$. The other $\mathfrak{l}$-isogenies are $\mathfrak{l}$-ascending if $\mathfrak{l}$ divides $\mathfrak{f}$, and $\mathfrak{l}$-horizontal otherwise.*

More explicitely, if $\mathfrak{l}$ divides $\mathfrak{f}$, there is a unique $\mathfrak{l}$-ascending $\mathfrak{l}$-kernel from $\mathscr{A}$, and $N(\mathfrak{l})$ $\mathfrak{l}$-descending $\mathfrak{l}$-kernels. If $\mathfrak{l}$ does not divide $\mathfrak{f}$, we have:

- *(i) If $\mathfrak{l}$ is inert in K, all $N(\mathfrak{l})+1$ $\mathfrak{l}$-kernels are $\mathfrak{l}$-descending;*
- *(ii) If $\mathfrak{l}$ splits in K into two prime ideals $\mathfrak{L}_1$ and $\mathfrak{L}_2$, there are two $\mathfrak{l}$-horizontal $\mathfrak{l}$-kernels, namely $\mathscr{A}[\mathfrak{L}_1]$ and $\mathscr{A}[\mathfrak{L}_2]$, and $N(\mathfrak{l})-1$ $\mathfrak{l}$-descending ones;*
- *(iii) If $\mathfrak{l}$ ramifies in K as $\mathfrak{L}^2$, there is one $\mathfrak{l}$-horizontal $\mathfrak{l}$-kernel, namely $\mathscr{A}[\mathfrak{L}]$, and $N(\mathfrak{l})$ $\mathfrak{l}$-descending ones.*

Proof. This proposition follows from Proposition 4.5 together with Remark 4.3. □

Definition 4.8 ($\mathfrak{l}$-predecessor)**.** *When it exists, let κ be the unique $\mathfrak{l}$-ascending kernel of Proposition 4.7. We call $\mathrm{pr}_{\mathfrak{l}}(\mathscr{A}) = \mathscr{A}/\kappa$ the* $\mathfrak{l}$-predecessor *of $\mathscr{A}$, and denote by $\mathrm{up}^{\mathfrak{l}}_{\mathscr{A}} : \mathscr{A} \to \mathrm{pr}_{\mathfrak{l}}(\mathscr{A})$ the canonical projection.*

The following notion of volcano was introduced in [FM02] to describe the structure of graphs of ℓ-isogenies between elliptic curves.

Definition 4.9 (volcano)**.** *Let n be a positive integer. An (infinite) n-*volcano *$\mathscr{V}$ is an $(n+1)$-regular, connected, undirected graph whose vertices are partitioned into* levels *$\{\mathscr{V}_i\}_{i\in\mathbb{Z}_{\geq 0}}$ such that:*

- *(i) The subgraph $\mathscr{V}_0$, the* surface*, is a finite regular graph of degree at most 2,*
- *(ii) For each $i > 0$, each vertex in $\mathscr{V}_i$ has exactly one neighbor in $\mathscr{V}_{i-1}$, and these are exactly the edges of the graph that are not on the surface.*

For any positive integer h, the corresponding (finite) volcano of height h is the restriction of $\mathscr{V}$ to its first h levels.

Let $\mathfrak{l}$ be a prime of K_0 above ℓ. Consider the $\mathfrak{l}$-isogeny graph $\mathscr{W}_{\mathfrak{l}}$ as defined in Section 1.3.1. Note that it is a directed multigraph; we say that such a graph is *undirected* if for any vertices u and v, the multiplicity of the edge from u to v is the same as the multiplicity from v to u. The remainder of this section is a proof of Theorem 1, which provides a complete description of the structure of the leveled $\mathfrak{l}$-isogeny graph $(\mathscr{W}_{\mathfrak{l}}, v_{\mathfrak{l}})$, closely related to volcanoes.

Lemma 4.10. *Suppose that $\mathcal{O}(\mathscr{B}) \subset \mathcal{O}(\mathscr{A})$. If there exists an $\mathfrak{l}$-isogeny $\varphi : \mathscr{A} \to \mathscr{B}$, then there are at least $[\mathcal{O}(\mathscr{A})^{\times} : \mathcal{O}(\mathscr{B})^{\times}]$ pairwise distinct kernels of $\mathfrak{l}$-isogenies from $\mathscr{A}$ to $\mathscr{B}$.*

Proof. The elements $\alpha \in \mathcal{O}(\mathscr{A})$ act on the subgroups of $\mathscr{A}$ via the isomorphism $\mathcal{O}(\mathscr{A}) \cong \mathrm{End}(\mathscr{A})$, and we denote this action $\kappa \mapsto \kappa^{\alpha}$. Let $\kappa = \ker\varphi$. If $u \in \mathcal{O}(\mathscr{A})^{\times}$ is a unit, then κ^u is also the kernel of an $\mathfrak{l}$-isogeny. Furthermore, u canonically induces an isomorphism $\mathscr{A}/\kappa \to \mathscr{A}/\kappa^u$, so κ^u is the kernel of a $\mathfrak{l}$-isogeny with target $\mathscr{B}$.

It only remains to prove that the orbit of κ for the action of $\mathcal{O}(\mathscr{A})^{\times}$ contains at least $[\mathcal{O}(\mathscr{A})^{\times} : \mathcal{O}(\mathscr{B})^{\times}]$ distinct kernels. It suffices to show that if $\kappa^u = \kappa$, then $u \in \mathcal{O}(\mathscr{B})^{\times}$. Let $u \in \mathcal{O}(\mathscr{A})^{\times}$ such that $\kappa^u = \kappa$. Recall that for any variety $\mathscr{C}$ in our isogeny class, we have fixed an isomorphism $\imath_{\mathscr{C}} : \mathrm{End}(\mathscr{C}) \to \mathcal{O}(\mathscr{C})$, and that these isomorphisms are all compatible in the sense that for any isogeny $\psi : \mathscr{C} \to \mathscr{D}$, and $\gamma \in \mathrm{End}(\mathscr{C})$, we have $\imath_{\mathscr{C}}(\gamma) = \imath_{\mathscr{D}}(\psi \circ \gamma \circ \hat{\psi})/\deg\psi$. Let $u_{\mathscr{A}} \in \mathrm{End}(\mathscr{A})$ be the endomorphism of $\mathscr{A}$ corresponding to u. It induces an isomorphism $\tilde{u}_{\mathscr{A}} : \mathscr{A}/\kappa \to \mathscr{A}/\kappa^u$, which is actually an automorphism of $\mathscr{A}/\kappa$ since $\kappa^u = \kappa$. Let $\varphi : \mathscr{A} \to \mathscr{A}/\kappa$ be the natural projection. We obtain the following commutative diagram:

$$\begin{tikzcd}
\mathscr{A}/\kappa \arrow[r, "\tilde{u}_{\mathscr{A}}"] & \mathscr{A}/\kappa \arrow[rd, "\hat{\varphi}"] & \\
\mathscr{A} \arrow[u, "\varphi"] \arrow[r, "u_{\mathscr{A}}"] & \mathscr{A} \arrow[u, "\varphi"] \arrow[r, "{[\deg\varphi]}"'] & \mathscr{A}.
\end{tikzcd}$$

Finally, we obtain

$$u = \imath_{\mathscr{A}}([\deg\varphi] \circ u_{\mathscr{A}})/\deg\varphi = \imath_{\mathscr{A}}(\hat{\varphi} \circ \tilde{u}_{\mathscr{A}} \circ \varphi)/\deg\varphi = \imath_{\mathscr{B}}(\tilde{u}_{\mathscr{A}}) \in \mathcal{O}(\mathscr{B}).$$

□

Lemma 4.11. *Let K be a CM-field and K_0 its maximal real subfield. Let $\mathcal{O}$ be an order in K of conductor $\mathfrak{f}$ such that $\mathfrak{o}_0 \subset \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. Let $\mathcal{O}'$ be the order such that $\mathcal{O}' \otimes_{\mathbb{Z}} \mathbb{Z}_{\ell'} = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_{\ell'}$ for all prime $\ell' \neq \ell$, and $\mathcal{O}' \otimes_{\mathbb{Z}} \mathbb{Z}_\ell = \mathfrak{o}_0 + \mathfrak{l}\mathfrak{f}\mathfrak{o}_K$. Then,*

$$|\operatorname{Pic}(\mathcal{O}')| = \frac{[(\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell)^{\times} : (\mathcal{O}' \otimes_{\mathbb{Z}} \mathbb{Z}_\ell)^{\times}]}{[\mathcal{O}^{\times} : \mathcal{O}'^{\times}]} |\operatorname{Pic}(\mathcal{O})|.$$

Proof. First, for any order $\mathcal{O}$ in K of conductor $\mathfrak{f}$ we have the classical formula (see [NS99, Th.12.12 and Prop.12.11])

$$\begin{aligned}
|\operatorname{Pic}(\mathcal{O})| &= \frac{h_K}{[\mathcal{O}_K^{\times} : \mathcal{O}^{\times}]} \frac{|(\mathcal{O}_K/\mathfrak{f})^{\times}|}{|(\mathcal{O}/\mathfrak{f})^{\times}|} \\
&= \frac{h_K}{[\mathcal{O}_K^{\times} : \mathcal{O}^{\times}]} \prod_{\ell' \text{ prime}} [(\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_{\ell'})^{\times} : (\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_{\ell'})^{\times}].
\end{aligned}$$

Now, consider $\mathcal{O}$ and $\mathcal{O}'$ as in the statement of the lemma. We obtain

$$\begin{aligned}
\frac{|\operatorname{Pic}(\mathcal{O}')|}{|\operatorname{Pic}(\mathcal{O})|} &= \frac{[\mathcal{O}_K^{\times} : \mathcal{O}^{\times}]}{[\mathcal{O}_K^{\times} : \mathcal{O}'^{\times}]} [(\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell)^{\times} : (\mathcal{O}' \otimes_{\mathbb{Z}} \mathbb{Z}_\ell)^{\times}] \\
&= \frac{[(\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell)^{\times} : (\mathcal{O}' \otimes_{\mathbb{Z}} \mathbb{Z}_\ell)^{\times}]}{[\mathcal{O}^{\times} : \mathcal{O}'^{\times}]}.
\end{aligned}$$

□

Remark 4.12. If one supposes that $\mathcal{O}_K^{\times} = \mathcal{O}_{K_0}^{\times}$, then $[\mathcal{O}^{\times} : \mathcal{O}'^{\times}]$ is always 1 in the above lemma. Indeed, one has $\mathcal{O}^{\times} \subset \mathcal{O}_{K_0}^{\times} \subset \mathfrak{o}_0^{\times} \subset (\mathcal{O}' \otimes_{\mathbb{Z}} \mathbb{Z}_\ell)^{\times}$, and therefore, since $\mathcal{O}$ and $\mathcal{O}'$ coincide at every other prime, we obtain $\mathcal{O}^{\times} \subset \mathcal{O}'^{\times}$, hence $\mathcal{O}^{\times} = \mathcal{O}'^{\times}$.

Remark 4.13. For $g = 2$, the field K is a primitive quartic CM-field. Then, the condition $\mathcal{O}_K^\times = \mathcal{O}_{K_0}^\times$ is simply equivalent to $K \neq \mathbb{Q}(\zeta_5)$ by [Str10, Lem.3.3]. So in dimension 2, if $K \neq \mathbb{Q}(\zeta_5)$, one always has $[\mathcal{O}^\times : \mathcal{O}'^\times] = 1$ in the above lemma.

Proof of Theorem 1. Let $\mathscr{V}$ be any of connected component of $\mathscr{W}_\mathfrak{l}$. First, it follows from Proposition 3.4 that locally at any prime other than ℓ, the endomorphism rings occurring in $\mathscr{V}$ all coincide. Also, locally at ℓ, Proposition 4.7 implies that an $\mathfrak{l}$-isogeny can only change the valuation at $\mathfrak{l}$ of the conductor. Therefore within $\mathscr{V}$, the endomorphism ring of a variety $\mathscr{A}$ is uniquely determined by its level $v_\mathfrak{l}(\mathscr{A})$. Let $\mathcal{O}_i$ be the endomorphism of any (and therefore every) variety $\mathscr{A}$ in $\mathscr{V}$ at level $v_\mathfrak{l}(\mathscr{A}) = i$. Write $\mathscr{V}_i$ for the corresponding subset of $\mathscr{V}$. Proposition 4.7 implies that, except at the surface, all the edges connect consecutive levels of the graph, and each vertex at level i has exactly one edge to the level $i-1$.

The structure of the connected components of the level $\mathscr{V}_0$ is already a consequence of the well-known free CM-action of $\mathrm{Pic}(\mathcal{O}_0)$ on ordinary abelian varieties with endomorphism ring $\mathcal{O}_0$. Note that if $\varphi : \mathscr{A} \to \mathscr{B}$ is a descending $\mathfrak{l}$-isogeny within $\mathscr{V}$, then the unique ascending $\mathfrak{l}$-isogeny from $\mathscr{B}$ is $\mathrm{up}_\mathscr{B}^\mathfrak{l} : \mathscr{B} \to \mathrm{pr}_\mathfrak{l}(\mathscr{B})$, and we have $\mathrm{pr}_\mathfrak{l}(\mathscr{B}) \cong \mathscr{A}/\mathscr{A}[\mathfrak{l}]$; also, we have $\mathrm{pr}_\mathfrak{l}(\mathscr{B}/\mathscr{B}[\mathfrak{l}]) \cong \mathrm{pr}_\mathfrak{l}(\mathscr{B})/\mathrm{pr}_\mathfrak{l}(\mathscr{B})[\mathfrak{l}]$. These facts easily follow from the lattice point of view (see Proposition 4.5, and observe that if $\Gamma \in \mathscr{L}_\mathfrak{l}(\Lambda)$, then $\mathfrak{l}\Gamma \in \mathscr{L}_\mathfrak{l}(\mathfrak{l}\Lambda)$). We can deduce in particular that $\mathscr{V}_0$ is connected: a path from $\mathscr{A} \in \mathscr{V}_0$ to another vertex of $\mathscr{V}_0$ containing only vertical isogenies can only end at a vertex $\mathscr{A}/\mathscr{A}[\mathfrak{l}^i]$, which can also be reached within $\mathscr{V}_0$.

We now need to look at a bigger graph. For each $i \geq 0$, let $\mathscr{U}_i$ be the orbit of the level $\mathscr{V}_i$ for the CM-action of $\mathrm{Pic}(\mathcal{O}_i)$. The action is transitive on $\mathscr{U}_0$ since the connected graph $\mathscr{V}_0$ is in a single orbit of the action of $\mathrm{Pic}(\mathcal{O}_0)$. Let us show by induction that each $\mathscr{U}_{i+1}$ consists of a single orbit, and that each vertex of $\mathscr{U}_{i+1}$ is reachable by an edge from $\mathscr{U}_i$. First, $\mathscr{U}_{i+1}$ is non-empty because, by induction, $\mathscr{U}_i$ is non-empty, and each vertex in $\mathscr{U}_i$ has neighbors in $\mathscr{U}_{i+1}$. Choose any isogeny $\varphi : \mathscr{A}' \to \mathscr{A}$ from $\mathscr{U}_i$ to $\mathscr{U}_{i+1}$. For any vertex $\mathscr{B}$ in the orbit of $\mathscr{A}$, there is an isogeny $\psi : \mathscr{A} \to \mathscr{B}$ of degree coprime to ℓ. The isogeny $\psi \circ \varphi$ factors through a variety $\mathscr{B}'$ via an isogeny $\psi' : \mathscr{A}' \to \mathscr{B}'$ of same degree as ψ, and an isogeny $\nu : \mathscr{B}' \to \mathscr{B}$ of kernel $\psi'(\ker \varphi)$. In particular, ν is an $\mathfrak{l}$-isogeny, and $\mathscr{B}'$ is in the orbit of $\mathscr{A}'$ for the CM-action, so it is in $\mathscr{U}_i$. This proves that any vertex in the orbit of $\mathscr{A}$ is reachable by an isogeny down from $\mathscr{U}_i$.

Let $\mathscr{E}_i$ be the set of all edges (counted with multiplicities) from $\mathscr{U}_i$ to $\mathscr{U}_{i+1}$. From Proposition 4.7, we have

$$|\mathscr{E}_i| = \left[(\mathcal{O}_i \otimes_\mathbb{Z} \mathbb{Z}_\ell)^\times : (\mathcal{O}_{i+1} \otimes_\mathbb{Z} \mathbb{Z}_\ell)^\times\right] \cdot |\mathscr{U}_i|. \tag{2}$$

For any $\mathscr{B} \in \mathscr{U}_{i+1}$, let $d(\mathscr{B})$ be the number of edges in $\mathscr{E}_i$ targeting $\mathscr{B}$ (with multiplicities). We have seen that any $\mathscr{B}$ is reachable from $\mathscr{U}_i$, therefore $d(\mathscr{B}) \geq 1$, and we deduce from Lemma 4.10 that $d(\mathscr{B}) \geq \left[\mathcal{O}_i^\times : \mathcal{O}_{i+1}^\times\right]$. We deduce

$$|\mathscr{E}_i| = \sum_{\mathscr{B} \in \mathscr{U}_{i+1}} d(\mathscr{B}) \geq \left[\mathcal{O}_i^\times : \mathcal{O}_{i+1}^\times\right] \cdot |\mathscr{U}_{i+1}|.$$

Together with Equation (2), we obtain the inequality

$$|\mathscr{U}_{i+1}| \leq \frac{\left[(\mathcal{O}_i \otimes_\mathbb{Z} \mathbb{Z}_\ell)^\times : (\mathcal{O}_{i+1} \otimes_\mathbb{Z} \mathbb{Z}_\ell)^\times\right]}{\left[\mathcal{O}_i^\times : \mathcal{O}_{i+1}^\times\right]} \cdot |\mathscr{U}_i|. \tag{3}$$

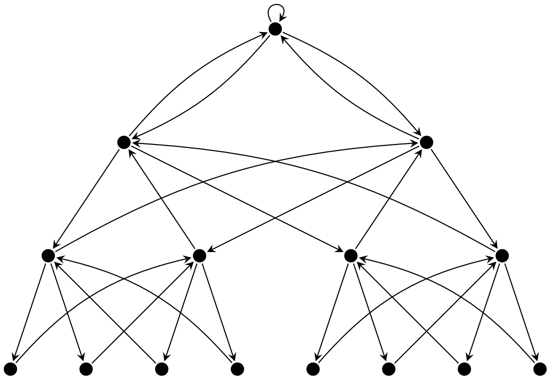

FIGURE 1. An example of an $\mathfrak{l}$-isogeny graph which is not a volcano, because the ideal $\mathfrak{l}$ is not principal.

Since the CM-action of the Picard group of $\mathcal{O}_i$ is free, we obtain from Lemma 4.11 that the right-hand side of Equation (3) is exactly the size of the orbit of any vertex in $\mathscr{U}_{i+1}$. So $\mathscr{U}_{i+1}$ contains at most one orbit, and thereby contains exactly one, turning Equation (3) into an actual equality. In particular, all the edges in $\mathscr{E}_i$ must have multiplicity precisely $[\mathcal{O}_i^\times : \mathcal{O}_{i+1}^\times]$. This conclude the recursion.

Note that with all these properties, the graph is a volcano if and only if it is undirected, and all the vertical multiplicities are 1. The latter is true if and only if $[\mathcal{O}_i^\times : \mathcal{O}_{i+1}^\times] = 1$ for any i, i.e., if $\mathcal{O}_0^\times \subset K_0$. For the following, suppose it is the case; it remains to decide when the graph is undirected. If $\mathfrak{l}$ is principal in $\mathcal{O}_0 \cap K_0$, the surface $\mathscr{V}_0$ is undirected because the primes above $\mathfrak{l}$ in $\mathcal{O}_0$ are inverses of each other. If $\varphi : \mathscr{A} \to \mathscr{B}$ is a descending $\mathfrak{l}$-isogeny within $\mathscr{V}$, then the unique ascending $\mathfrak{l}$-isogeny from $\mathscr{B}$ points to $\mathscr{A}/\mathscr{A}[\mathfrak{l}]$, which is isomorphic to $\mathscr{A}$ if and only if $\mathfrak{l}$ is principal in $\mathcal{O}(\mathscr{A})$. So for each descending edge $\mathscr{A} \to \mathscr{B}$ there is an ascending edge $\mathscr{B} \to \mathscr{A}$, and since we have proven above that each vertical edge has multiplicity 1, we conclude that the graph is undirected (so is a volcano) if and only if $\mathfrak{l}$ is principal in $\mathcal{O}_0 \cap K_0$ (if $\mathfrak{l}$ is not principal in $\mathcal{O}_0 \cap K_0$, there is a level i where $\mathfrak{l}$ is not principal in $\mathcal{O}_i$).

For Point (vi), choose a descending edge $\mathscr{A} \to \mathscr{B}$. We get that $\mathscr{C} \cong \mathscr{A}/\mathscr{A}[\mathfrak{l}]$. It is then easy to see that the isogeny $\mathscr{A} \to \mathscr{B}$ induces an isogeny $\mathscr{C} \to \mathscr{B}/\mathscr{B}[\mathfrak{l}]$. □

Theorem 1 gives a complete description of the graph: it allows one to construct an abstract model of any connected component corresponding to an order $\mathcal{O}_0$ from the knowledge of the norm of $\mathfrak{l}$, of the (labeled) Cayley graph of the subgroup of $\mathrm{Pic}(\mathcal{O}_0)$ with generators the prime ideals in $\mathcal{O}_0$ above $\mathfrak{l}$, of the order of $\mathfrak{l}$ in each Picard group $\mathrm{Pic}(\mathcal{O}_i)$, and of the indices $[\mathcal{O}_i^\times : \mathcal{O}_{i+1}^\times]$.

Example 4.14. For instance, suppose that $\ell = 2$ ramifies in K_0 as $\mathfrak{l}^2$, and $\mathfrak{l}$ is principal in $\mathcal{O}_K$, but is of order 2 in both $\mathrm{Pic}(\mathcal{O}_{K_0} + \mathfrak{l}\mathcal{O}_K)$ and $\mathrm{Pic}(\mathcal{O}_{K_0} + \mathfrak{l}^2\mathcal{O}_K)$, and that $\mathcal{O}_K^\times \subset K_0$. Then, the first four levels of any connected component of the $\mathfrak{l}$-isogeny graph for which the largest order is $\mathcal{O}_K$ are isomorphic to the graph of Figure 1. It is not a volcano since $\mathfrak{l}$ is not principal in every order $\mathcal{O}_{K_0} + \mathfrak{l}^i\mathcal{O}_K$.

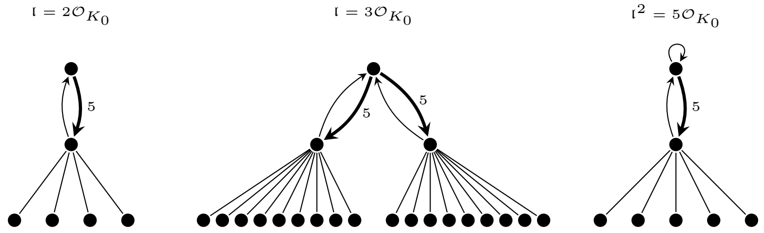
$\mathfrak{l} = 2\mathcal{O}_{K_0}$
5
$\mathfrak{l} = 3\mathcal{O}_{K_0}$
5
5
$\mathfrak{l}^2 = 5\mathcal{O}_{K_0}$
5

FIGURE 2. Some $\mathfrak{l}$-isogeny graphs for $K = \mathbb{Q}(\zeta_5)$, when the endomorphism ring at the surface is the maximal order $\mathbb{Z}[\zeta_5]$. All edges are simple except the thick ones, of multiplicity 5. The undirected edges are actually directed in both directions.

Example 4.15. When K is a primitive quartic CM-field, we have seen in Remark 4.13 that the multiplicities $[\mathcal{O}_i^\times : \mathcal{O}_{i+1}^\times]$ are always one, except maybe if $K = \mathbb{Q}(\zeta_5)$. Actually, even for $K = \mathbb{Q}(\zeta_5)$, only the maximal order $\mathcal{O}_K$ has units that are not in K_0. We give in Figure 2 examples of $\mathfrak{l}$-isogeny graphs when the order at the surface is $\mathcal{O}_K = \mathbb{Z}[\zeta_5]$ (which is a principal ideal domain). The primes 2 and 3 are inert in K, so we consider $\mathfrak{l} = 2\mathcal{O}_{K_0}$ and $\mathfrak{l} = 3\mathcal{O}_{K_0}$, and the prime number 5 is ramified in K_0 so $\mathfrak{l}^2 = 5\mathcal{O}_{K_0}$ (and $\mathfrak{l}$ is also ramified in K, explaining the self-loop at the surface of the last graph).

Notation 4.16. *Let $\mathcal{O}$ be any order in K with locally maximal real multiplication at ℓ, whose conductor is not divisible by $\mathfrak{l}$. We denote by $\mathscr{V}_{\mathfrak{l}}(\mathcal{O})$ the connected graph $\mathscr{V}$ described in Theorem 1. If $\mathfrak{l}$ does divide the conductor of $\mathcal{O}$, let $\mathcal{O}'$ be the smallest order containing $\mathcal{O}$, whose order is not divisible by $\mathfrak{l}$. Then, we also write $\mathscr{V}_{\mathfrak{l}}(\mathcal{O})$ for the graph $\mathscr{V}_{\mathfrak{l}}(\mathcal{O}')$.*

5. GRAPHS OF $\mathfrak{l}$-ISOGENIES WITH POLARIZATION

When $\mathfrak{l}$ is trivial in the narrow class group of K_0, then $\mathfrak{l}$-isogenies preserve principal polarizability. The graphs of $\mathfrak{l}$-isogenies studied in Section 4.2 do not account for polarizations. The present section fills this gap, by describing polarized graphs of β-isogenies, where $\beta \in K_0$ is a totally positive generator of $\mathfrak{l}$. The main result of this section is Theorem 5 according to which the connected components of polarized isogeny graphs are either isomorphic to the corresponding components of the non-polarized isogeny graphs, or non-trivial double-covers thereof. Yet, this description is not quite exact due to problems arising when the various abelian varieties occurring in a connected component have different automorphism groups.

5.1. Graphs with polarization.

Before defining the graph, we record the following proposition, which implies that one vertex of a fixed connected component of $(\mathscr{W}_\beta, v_\beta)$ is principally polarizable if and only if all of them are. Note that since β is a generator of $\mathfrak{l}$, we will write β-isogeny to mean $\mathfrak{l}$-isogeny.

Proposition 5.1. *If $\varphi : \mathscr{A} \to \mathscr{B}$ is a β-isogeny, then there is a unique principal polarization $\xi_{\mathscr{B}}$ on $\mathscr{B}$ satisfying*

$$\varphi^* \xi_{\mathscr{B}} = \xi_{\mathscr{A}}^{\beta}.$$

Proof. Writing $\varphi_{\xi_{\mathscr{A}}}$ the polarization isogeny, then $\ker(\varphi) \subset \ker(\varphi_{\xi^{\beta}_{\mathscr{A}}})$ is a maximal isotropic subgroup for the commutator pairing and hence by Grothendieck descent (see [Rob10a, Lem.2.4.7]); the proof there is in characteristic 0, but it extends to ordinary abelian varieties in characteristic p via to canonical lifts), it follows that $\xi^{\beta}_{\mathscr{A}}$ is a pullback of a principal polarization $\xi_{\mathscr{B}}$ on $\mathscr{B}$. For uniqueness, note that the homomorphism $\varphi^*\colon \mathbf{NS}(\mathscr{B}) \to \mathbf{NS}(\mathscr{A})$ of free abelian groups of the same rank becomes an isomorphism after tensoring with $\mathbb{Q}$, hence is injective. □

We define the principally polarized, leveled, β-isogeny graph $(\mathscr{W}^{\mathrm{pp}}_{\beta}, v_{\beta})$ as follows. A point is an isomorphism class[4] of pair $(\mathscr{A}, \xi_{\mathscr{A}})$, where $\mathscr{A}$ is a principally polarizable abelian variety occuring in $(\mathscr{W}_{\beta}, v_{\beta})$, and $\xi_{\mathscr{A}}$ is a principal polarization on $\mathscr{A}$. There is an edge of multiplicity m from the isomorphism class of $(\mathscr{A}, \xi_{\mathscr{A}})$ to the isomorphism class of $(\mathscr{B}, \xi_{\mathscr{B}})$ if there are m distinct subgroups of $\mathscr{A}$ that are kernels of β-isogenies $\varphi : \mathscr{A} \to \mathscr{B}$ such that $\varphi^*\xi'_{\mathscr{B}}$ is isomorphic to $\xi^{\beta}_{\mathscr{A}}$, for some polarization $\xi'_{\mathscr{B}}$ isomorphic to $\xi_{\mathscr{B}}$. The graph $\mathscr{W}^{\mathrm{pp}}_{\beta}$ admits a forgetful map to $\mathscr{W}_{\beta}$, and in particular inherits the structure of a leveled graph $(\mathscr{W}^{\mathrm{pp}}_{\beta}, v_{\beta})$.

Remark 5.2. It can be the case that there is no β-isogeny $\varphi : \mathscr{A} \to \mathscr{B}$ such that $\varphi^*\xi_{\mathscr{B}} \cong \xi^{\beta}_{\mathscr{A}}$, but that there is nonetheless an edge (because there is a map with this property for some other polarization $\xi'_{\mathscr{B}}$, isomorphic to $\xi_{\mathscr{B}}$). This can happen because pullbacks of isomorphic polarizations are not necessarily isomorphic, when $\mathscr{A}$ and $\mathscr{B}$ have different automorphism groups.

We note that this graph is undirected:

Proposition 5.3. *If $\varphi : \mathscr{A} \to \mathscr{B}$ is a β-isogeny, then there is a unique β-isogeny $\tilde{\varphi} : \mathscr{B} \to \mathscr{A}$ satisfying $\tilde{\varphi}\varphi = \beta$, called the β-dual of φ.*

Proof. Let κ be the kernel of φ. The group $\mathscr{A}[\beta]$ is an $\mathcal{O}_0(\mathscr{A})/(\beta)$-vector space of dimension 2, of which the kernel κ is a vector subspace of dimension 1. Therefore there is another vector subspace κ' such that $\mathscr{A}[\beta] = \kappa \oplus \kappa'$, and $\varphi(\kappa')$ is the kernel of a β-isogeny $\psi : \mathscr{B} \to \mathscr{C}$. Then, the kernel of the composition $\psi \circ \varphi$ is $\mathscr{A}[\beta]$ so there is an isomorphism $u : \mathscr{C} \to \mathscr{A}$ such that $u \circ \psi \circ \varphi = \beta$. The isogeny $u \circ \psi$ is the β-dual of φ (which is trivially unique). □

5.2. Counting polarizations.

To describe $(\mathscr{W}^{\mathrm{pp}}_{\beta}, v_{\beta})$, we need to count principal polarizations on any fixed variety. If $\mathcal{O}$ is an order in K, write $\mathcal{O}^{+\times}$ for the group of totally positive units in $\mathcal{O} \cap K_0$.

Proposition 5.4. *Let $\mathscr{A}$ be a simple ordinary abelian variety over $\mathbb{F}_q$ with endomorphism ring $\mathcal{O}$. Then the set of isomorphism classes of principal polarizations (when non-empty) on $\mathscr{A}$ is a torsor for the group*

$$U(\mathcal{O}) := \frac{\mathcal{O}^{+\times}}{\mathbf{N} : \mathcal{O}^{\times} \to (\mathcal{O} \cap K_0)^{\times}}.$$

Proof. See [BL04, Cor.5.2.7] for a proof in characteristic 0. That the result remains true for ordinary abelian varieties in characteristic p follows from the theory of canonical lifts. □

The following lemma recalls some well-known facts about $U(\mathcal{O})$.

[4] Recall that two polarizations $\xi_{\mathscr{A}}$ and $\xi'_{\mathscr{A}}$ on $\mathscr{A}$ are isomorphic if and only if there is a unit $u \in \mathcal{O}(\mathscr{A})^{\times}$ such that $\xi'_{\mathscr{A}} = u^*\xi_{\mathscr{A}}$.

Lemma 5.5. *The group $U(\mathcal{O})$ is an $\mathbb{F}_2$-vector space of dimension d, where $0 \leq d \leq g-1$. If $\mathcal{O} \subset \mathcal{O}'$ and $\mathcal{O} \cap K_0 = \mathcal{O}' \cap K_0$, then the natural map $U(\mathcal{O}) \to U(\mathcal{O}')$ is surjective.*

Proof. Writing $\mathbf{N}$ for the norm from K to K_0, we have the following hierarchy, the last containment following because for $\beta \in \mathcal{O}_r$ one has $\beta^2 = \mathbf{N}\beta$:

$$(\mathcal{O} \cap K_0)^\times \supseteq \mathcal{O}^{+\times} \supseteq \mathbf{N}(\mathcal{O}^\times) \supseteq (\mathcal{O} \cap K_0)^{\times 2} \tag{4}$$

By Dirichlet's unit theorem (and its extension to non-maximal orders), the group $\mathcal{O}_0^\times$ is of the form $\{\pm 1\} \times A$, where A is a free abelian group of cardinality 2^{g-1}, so the quotient $(\mathcal{O} \cap K_0)^\times/(\mathcal{O} \cap K_0)^{\times 2}$ is an $\mathbb{F}_2$-vector space of dimension at most g. Since -1 is never a totally positive unit, the first claim follows. The second sentence of the lemma is clear. □

Remark 5.6. We remark that, other than the simple calculations described, there is little one can say in great generality about the indices of the containments in (4), which vary depending on the specific fields K and orders $\mathcal{O}$ chosen. For example, if $g = 2$, the total index in (4) is 4, and one has examples with the "missing" factor of 2 (i.e., the one unaccounted for by the totally negative unit -1) occurring in any of the three containments.

5.3. Structure of $(\mathscr{W}_\beta^{\mathrm{pp}}, v_\beta)$.

We may now state the main theorem.

Theorem 5. *Let $\mathscr{V}^{\mathrm{pp}}$ be any connected component of the leveled β-isogeny graph $(\mathscr{W}_\beta^{\mathrm{pp}}, v_\beta)$. For each $i \geq 0$, let $\mathscr{V}_i^{\mathrm{pp}}$ be the subgraph of $\mathscr{V}^{\mathrm{pp}}$ at level i. We have:*

(i) For each $i \geq 0$, the varieties in $\mathscr{V}_i^{\mathrm{pp}}$ share a common endomorphism ring $\mathcal{O}_i$. The order $\mathcal{O}_0$ can be any order with locally maximal real multiplication at ℓ, whose conductor is not divisible by β;

(ii) The level $\mathscr{V}_0^{\mathrm{pp}}$ is isomorphic to the Cayley graph of the subgroup of $\mathfrak{C}(\mathcal{O}_0)$ with generators $(\mathfrak{L}_i, \beta)$ where $\mathfrak{L}_i$ are the prime ideals in $\mathcal{O}_0$ above β;

(iii) For any $\mathscr{A} \in \mathscr{V}_0^{\mathrm{pp}}$, there are

$$\frac{N(\mathfrak{l}) - \left(\frac{K}{\beta}\right)}{[\mathcal{O}_0^\times : \mathcal{O}_1^\times]} \frac{U(\mathcal{O}_1)}{U(\mathcal{O}_0)}$$

edges of multiplicity $[\mathcal{O}_0^\times : \mathcal{O}_1^\times]$ from $\mathscr{A}$ to distinct vertices of $\mathscr{V}_1^{\mathrm{pp}}$ (where $\left(\frac{K}{\beta}\right)$ is -1, 0 or 1 if β is inert, ramified, or split in K);

(iv) For each $i > 0$, and any $x \in \mathscr{V}_i^{\mathrm{pp}}$, there is one simple edge from x to a vertex of $\mathscr{V}_{i-1}^{pp}$, and

$$\frac{N(\mathfrak{l})}{[\mathcal{O}_i^\times : \mathcal{O}_{i+1}^\times]} \frac{U(\mathcal{O}_{i+1})}{U(\mathcal{O}_i)}$$

edges of multiplicity $[\mathcal{O}_i^\times : \mathcal{O}_{i+1}^\times]$ to distinct vertices of $\mathscr{V}_{i+1}^{\mathrm{pp}}$;

(v) For each edge $x \to y$, there is an edge $y \to x$.

In particular, the graph $\mathscr{V}^{\mathrm{pp}}$ is an $N(\beta)$-volcano if and only if $\mathcal{O}_0^\times \subset K_0$. Also, if $\mathscr{V}^{\mathrm{pp}}$ contains a variety defined over the finite field k, the subgraph containing only the varieties defined over k consists of the subgraph of the first v levels, where v is the valuation at β of the conductor of $\mathcal{O}_{K_0}[\pi] = \mathcal{O}_{K_0}[\pi, \pi^\dagger]$.

Before proving this theorem, we need some preliminary results. First, we recall the action of the Shimura class group. For $\mathcal{O}$ an order, write $\mathscr{I}(\mathcal{O})$ for the group of invertible $\mathcal{O}$-ideals, and define the Shimura class group as

$$\mathfrak{C}(\mathcal{O}) = \{(\mathfrak{a}, \alpha) \mid \mathfrak{a} \in \mathscr{I}(\mathcal{O}) : \mathbf{N}\mathfrak{a} = \alpha\mathcal{O}, \alpha \in K_0 \text{ totally positive } \}/\sim$$

where two pairs $(\mathfrak{a}, \alpha), (\mathfrak{a}', \alpha')$ are equivalent if there exists $u \in K^\times$ with $\mathfrak{a}' = u\mathfrak{a}$ and $\alpha' = uu^\dagger\alpha$. The Shimura class group acts freely on the set of isomorphism classes of principally polarized abelian varieties whose endomorphism ring is $\mathcal{O}$ (see [ST61, §17] for the result in characteristic 0, which extends via canonical lifts to the ordinary characteristic p case). If β is coprime to the conductor of $\mathcal{O}$, then an element of $\mathfrak{C}(\mathcal{O})$ acts by a β-isogeny if and only if it is of the form $(\mathfrak{L}, \beta)$, for some prime ideal $\mathfrak{L}$ of $\mathcal{O}$ dividing (β).

Lemma 5.7. *Let $\varphi : \mathscr{A} \to \mathscr{B}$ be a β-isogeny, and let $\xi_{\mathscr{A}}$ be a principal polarization on $\mathscr{A}$. We have:*

(i) If φ is β-ascending, there is, up to isomorphism, a unique polarization $\xi_{\mathscr{B}}$ on $\mathscr{B}$ such that $\varphi^*\xi_{\mathscr{B}}$ is isomorphic to $\xi_{\mathscr{A}}^{\beta}$;

(ii) It φ is β-descending, there are, up to isomorphism, exactly

$$\frac{|U(\mathcal{O}(\mathscr{B}))|}{|U(\mathcal{O}(\mathscr{A}))|}$$

distinct polarizations $\xi_{\mathscr{B}}$ on $\mathscr{B}$ such that $\varphi^*\xi_{\mathscr{B}}$ is isomorphic to $\xi_{\mathscr{A}}^{\beta}$.

Proof. Let us first prove (i). From Proposition 5.1, there exists a polarization $\xi_{\mathscr{B}}$ on $\mathscr{B}$ such that $\varphi^*\xi_{\mathscr{B}} = \xi_{\mathscr{A}}^{\beta}$. Suppose $\xi'_{\mathscr{B}}$ is a polarization such that $\varphi^*\xi'_{\mathscr{B}} \cong \xi_{\mathscr{A}}^{\beta}$. Then, there is a unit $u \in \mathcal{O}(\mathscr{A})^\times$ such that $\varphi^*\xi'_{\mathscr{B}} = u^*\xi_{\mathscr{A}}^{\beta}$. But φ is ascending, so $u \in \mathcal{O}(\mathscr{B})^\times$ and therefore

$$\varphi^*\xi'_{\mathscr{B}} = u^*\xi_{\mathscr{A}}^{\beta} = u^*(\varphi^*\xi_{\mathscr{B}}) = \varphi^*(u^*\xi_{\mathscr{B}}).$$

From the uniqueness in Proposition 5.1, we obtain $\xi'_{\mathscr{B}} = u^*\xi_{\mathscr{B}}$, so $\xi_{\mathscr{B}}$ and $\xi'_{\mathscr{B}}$ are two isomorphic polarizations.

For (ii), again apply Proposition 5.1, and observe that the kernel of the surjection $U(\mathcal{O}(\mathscr{B})) \to U(\mathcal{O}(\mathscr{A}))$ of Lemma 5.5 acts simply transitively on the set of isomorphism classes of polarizations $\xi_{\mathscr{B}}$ on $\mathscr{B}$ satisfying $\varphi^*\xi_{\mathscr{B}} \cong \xi_{\mathscr{A}}^{\beta}$. □

Proof of Theorem 5. First observe that (i) is immediate from Theorem 1(i), since the leveling on $\mathscr{V}^{\mathrm{pp}}$ is induced from that of $\mathscr{V}$. Also, (v) is a direct consequence of the existence of β-duals, established in Proposition 5.3. Now, let us prove that for any class $(\mathscr{A}, \xi_{\mathscr{A}})$ at a level $i > 0$, there is a unique edge to the level $i - 1$. From Theorem 1, there exists an ascending isogeny $\varphi : \mathscr{A} \to \mathscr{B}$ (unique up to isomorphism of $\mathscr{B}$), and from Lemma 5.7(i), there is a unique polarization $\xi_{\mathscr{B}}$ on $\mathscr{B}$ (up to isomorphism) such that $(\mathscr{A}, \xi_{\mathscr{A}}) \to (\mathscr{B}, \xi_{\mathscr{B}})$ is an edge in $\mathscr{V}^{\mathrm{pp}}$.

These results, and the fact that $\mathscr{V}_0$ is connected, imply that $\mathscr{V}_0^{\mathrm{pp}}$ is connected. We can then deduce (ii) from the action of the Shimura class group $\mathfrak{C}(\mathcal{O}_0)$.

Now, (iii) (respectively, (iv)) is a consequence of Theorem 1(iii) (respectively, Theorem 1(iv)) together with Lemma 5.7. The statement on multiplicities of the edges also uses the fact that if $\varphi, \psi : \mathscr{A} \to \mathscr{B}$ are two β-isogenies with same kernel, and $\xi_{\mathscr{A}}$ is a principal polarization on $\mathscr{A}$, then the two principal polarizations on $\mathscr{B}$ induced via φ and ψ are isomorphic.

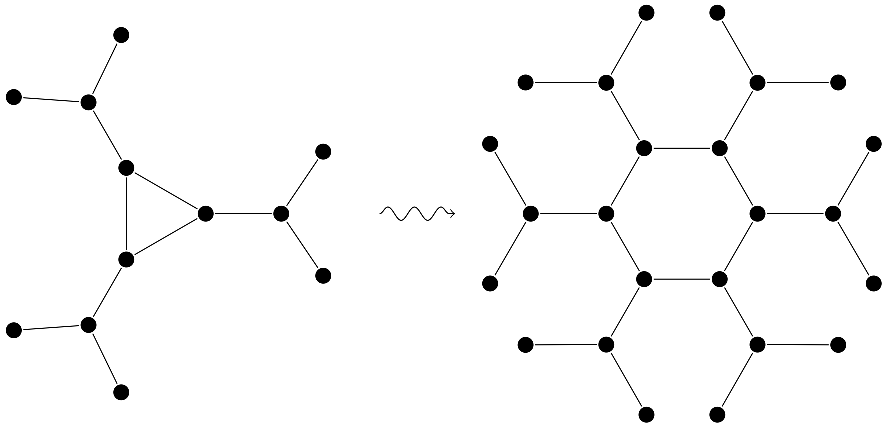

FIGURE 3. An example of how adding the polarization data to a volcano of β-isogenies can double the length of the cycle.

The volcano property follows from the corresponding phrase in the statement of Theorem 1, and the statement on fields of definition follows from Remark 3.3, which shows that the isomorphism from a principally polarized absolutely simple ordinary abelian variety to its dual, and hence the polarization, is defined over the field of definition of the variety. □

5.4. **Principally polarizable surfaces.** The result of Theorem 5 for abelian surfaces is a bit simpler than the general case, thanks to the following lemma.

Lemma 5.8. *Suppose $g = 2$. With all notations as in Theorem 5, we have $U(\mathcal{O}_i) = U(\mathcal{O}_0)$ for any non-negative integer i.*

Proof. In these cases, one has $\mathcal{O}_K^\times = \mathcal{O}_{K_0}^\times$ except in the case $K = \mathbb{Q}(\zeta_5)$ (see Remark 4.13); but even when $K = \mathbb{Q}(\zeta_5)$ the equality is true up to units of norm 1. Therefore for any order $\mathcal{O}$ in K, one has $\mathbf{N}\mathcal{O}^\times = \mathbf{N}(\mathcal{O} \cap K_0)^\times$. Thus, none of the groups $U(\mathcal{O}_i)$ actually depend on i. □

Therefore, the factors $|U(\mathcal{O}_{i+1})|/|U(\mathcal{O}_i)|$ disappear when $g = 2$. It follows that each component $\mathscr{W}^{\mathrm{pp}}$ is either isomorphic to its image in $(\mathscr{W}_\beta, v_\beta)$, or is isomorphic to the natural double cover of this image constructed by doubling the length of the cycle $\mathscr{V}_0$ (as illustrated in Figure 3). The first case occurs when (β) is inert in K/K_0, or when the order of $(\mathfrak{L}, \beta)$ in $\mathfrak{C}(\mathcal{O}_0)$ equals the order of $\mathfrak{L}$ in $\mathrm{Cl}(\mathcal{O}_0)$ (where $\mathfrak{L}$ is a prime ideal of $\mathcal{O}_0$ above (β)). The second case occurs when the order of $(\mathfrak{L}, \beta)$ is twice that of $\mathfrak{L}$.

6. LEVELS FOR THE REAL MULTIPLICATION IN DIMENSION 2

We now specialize to the case $g = 2$. Then, $\mathscr{A}$ is of dimension 2, and K is a primitive quartic CM-field. The subfield K_0 is a real quadratic number field. The orders in $K_{0,\ell}$ are linearly ordered since they are all of the form $\mathbb{Z}_\ell + \ell^n \mathfrak{o}_0$. These n's can be seen as "levels" of real multiplication. Taking advantage of this simple structure, the goal of this section is to prove Theorem 3.

6.1. **Preliminaries on symplectic lattices.** Let $\mathbb{F}_\ell$ be the finite field with ℓ elements.

Lemma 6.1. *Let W be a symplectic $\mathbb{F}_\ell$-vector space of dimension 4. It contains exactly $\ell^3+\ell^2+\ell+1$ maximal isotropic subspaces.*

Proof. In the following, a *line* or a *plane* means a dimension 1 or 2 subspace of a vector space (i.e., they contain the origin of the vector space). Fix any line L in W. We will count the number of maximal isotropic subspaces of W containing L. The line L is itself isotropic (yet not maximal), so $L \subset L^\perp$. Also, $\dim L + \dim L^\perp = 4$, so $\dim L^\perp = 3$. Since any maximal isotropic subspace of W is of dimension 2, it is easy to see that those containing L are exactly the planes in $L^\perp$ containing L. There are $\ell+1$ such planes, because they are in natural correspondence with the lines in the dimension 2 vector space $L^\perp/L$. It follows that there are $\ell+1$ maximal isotropic subspaces of W containing L. There are $\ell^3+\ell^2+\ell+1$ lines L in W, and each maximal isotropic subspace of W contains $\ell+1$ lines, we conclude that there are $\ell^3+\ell^2+\ell+1$ maximal isotropic subspaces. □

Lemma 6.2. *Let V be a symplectic $\mathbb{Q}_\ell$-vector space of dimension 4. Let $\Lambda \subset V$ be a lattice in V such that $\Lambda^* = \Lambda$. Then $\Lambda/\ell\Lambda$ is a symplectic $\mathbb{F}_\ell$-vector space of dimension 4 for the symplectic form*

$$\langle \lambda + \ell\Lambda, \mu + \ell\Lambda\rangle_\ell = \langle \lambda, \mu\rangle \mod \ell.$$

Proof. The fact that the form $\langle -,-\rangle_\ell$ is bilinear and alternating easily follows from the fact that the form $\langle -,-\rangle$ is symplectic. It only remains to prove that it is non-degenerate. Let $\lambda \in \Lambda$, and suppose that $\langle \lambda + \ell\Lambda, \mu + \ell\Lambda\rangle_\ell = 0$ for any $\mu \in \Lambda$. We now prove that $\lambda \in \ell\Lambda$. For any $\mu \in \Lambda$, we have $\langle \lambda, \mu\rangle \in \ell\mathbb{Z}_\ell$, and therefore $\langle \ell^{-1}\lambda, \mu\rangle \in \mathbb{Z}_\ell$. So $\ell^{-1}\lambda \in \Lambda^* = \Lambda$, whence $\lambda \in \ell\Lambda$, concluding the proof. □

Lemma 6.3. *Let V be a symplectic $\mathbb{Q}_\ell$-vector space of dimension 4, and Λ a self-dual lattice in V. Let $\ell\Lambda \subset \Gamma \subset \Lambda$ be an intermediate lattice. Then $\Gamma/\ell\Lambda$ is maximal isotropic in $\Lambda/\ell\Lambda$ if and only if $\Gamma^* = \ell^{-1}\Gamma$.*

Proof. First, suppose that $\Gamma/\ell\Lambda$ is maximal isotropic. Fix $\gamma \in \Gamma$. For any $\delta \in \Gamma$, since $\Gamma/\ell\Lambda$ is isotropic, we have $\langle \gamma, \delta\rangle \in \ell\mathbb{Z}_\ell$, so $\langle \ell^{-1}\gamma, \delta\rangle \in \mathbb{Z}_\ell$ and therefore $\ell^{-1}\gamma \in \Gamma^*$. This proves that $\ell^{-1}\Gamma \subset \Gamma^*$. Now, let $\alpha \in \Gamma^*$. Observe that $\langle \ell\alpha, \gamma\rangle = \ell\langle \alpha, \gamma\rangle \in \ell\mathbb{Z}_\ell$ for any $\gamma \in \Gamma$. This implies that $\ell^{-1}\alpha$ must be in Γ, because $\Gamma/\ell\Lambda$ is maximally isotropic. This proves that $\ell^{-1}\Gamma^* \subset \Gamma$.

Now, suppose that $\Gamma^* = \ell^{-1}\Gamma$. Then, $\langle \ell^{-1}\Gamma, \Gamma\rangle \subset \mathbb{Z}_\ell$, so $\langle \Gamma, \Gamma\rangle \in \ell\mathbb{Z}_\ell$, and $\Gamma/\ell\Lambda$ is isotropic. Let $\lambda \in \Lambda$ such that $\langle \lambda + \ell\Lambda, \Gamma/\ell\Lambda\rangle_\ell = \{0\}$. Then, $\langle \ell^{-1}\lambda, \Gamma\rangle \subset \ell\mathbb{Z}_\ell$, so $\ell^{-1}\lambda \in \Gamma^* = \ell^{-1}\Gamma$, which implies that $\lambda \in \Gamma$. So $\Gamma/\ell\Lambda$ is maximal isotropic. □

Definition 6.4 ((ℓ,ℓ)-neighbors)**.** *The set $\mathscr{L}(\Lambda)$ of* (ℓ,ℓ)-neighbors *of Λ is the set of lattices Γ such that $\ell\Lambda \subset \Gamma \subset \Lambda$, and $\Gamma/\ell\Lambda$ is maximal isotropic in $\Lambda/\ell\Lambda$.*

Remark 6.5. Consider the lattice $T = T_\ell\mathscr{A}$. Note that (ℓ,ℓ)-isogenies $\mathscr{A} \to \mathscr{B}$ correspond under Proposition 3.1 to lattices Γ with $T \subset \Gamma \subset \frac{1}{\ell}T$ and Γ/T a maximal isotropic subspace of $\frac{1}{\ell}T/T$, i.e., to (ℓ,ℓ)-neighbors of T rescaled by a factor ℓ^{-1}.

6.2. (ℓ,ℓ)**-neighboring lattices.** Throughout this section, V is a symplectic $\mathbb{Q}_\ell$-vector space of dimension 4. Again, we consider a prime number ℓ, a quartic CM-field K, with K_0 its quadratic real subfield. The algebra $K_\ell = K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ is a $\mathbb{Q}_\ell$-algebra of dimension 4, with an involution $x \mapsto x^\dagger$ fixing $K_{0,\ell}$ induced by the generator of $\mathrm{Gal}(K/K_0)$. Suppose that K_ℓ acts ($\mathbb{Q}_\ell$-linearly) on V, and that for any $x \in K_\ell$, $u, v \in V$, we have $\langle xu, v\rangle = \langle u, x^\dagger v\rangle$. For any lattice Λ in V, the *real order* of Λ is the order in $K_{0,\ell} = K_0 \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ defined as

$$\mathfrak{o}_0(\Lambda) = \{x \in K_{0,\ell} \mid x\Lambda \subset \Lambda\}.$$

Any order in $K_{0,\ell}$ is of the form $\mathfrak{o}_n = \mathbb{Z}_\ell + \ell^n \mathfrak{o}_0$, for some non-negative integer n, with $\mathfrak{o}_0$ the maximal order of $K_{0,\ell}$. We say that Λ is an $\mathfrak{o}_n$-lattice if $\mathfrak{o}(\Lambda) = \mathfrak{o}_n$. The goal of this section is to prove Theorem 3 by first proving its lattice counterpart, in the form of the following proposition.

Proposition 6.6. *Let Λ be a self-dual $\mathfrak{o}_n$-lattice, with $n > 0$. The set $\mathscr{L}(\Lambda)$ of its (ℓ,ℓ)-neighbors contains exactly one $\mathfrak{o}_{n-1}$-lattice, namely $\ell\mathfrak{o}_{n-1}\Lambda$, $\ell^2 + \ell$ lattices of real order $\mathfrak{o}_n$, and ℓ^3 lattices of real order $\mathfrak{o}_{n+1}$.*

Lemma 6.7. *Let Λ be a self-dual $\mathfrak{o}_n$-lattice in V, for some non-negative integer n. Then, Λ is a free $\mathfrak{o}_n$-module of rank 2.*

Proof. By Lemma 4.1, the order $\mathfrak{o}_n$ is a Gorenstein ring of dimension 1, and it follows from [Bas63, Thm. 6.2] that Λ is a reflexive $\mathfrak{o}_n$-module. From [Bas63, Prop. 7.2], Λ has a projective direct summand, so $\Lambda = \mathfrak{o}_n e_1 \oplus M$ for some $e_1 \in \Lambda$, and M an $\mathfrak{o}_n$-submodule. This M is still reflexive (any direct summand of a reflexive module is reflexive). So applying [Bas63, Prop. 7.2] again to M, together with the fact that it has $\mathbb{Z}_\ell$-rank 2, there is a non-negative integer $m \leq n$ and an element $e_2 \in \Lambda$ such that $M = \mathfrak{o}_m e_2$. We shall prove that $m = n$. By contradiction, assume $m < n$. We have $\Lambda/\ell\Lambda = (\mathfrak{o}_n e_1/\ell\mathfrak{o}_n) \oplus (\mathfrak{o}_m e_2/\ell\mathfrak{o}_m)$. Observe that $\mathfrak{o}_m e_2/\ell\mathfrak{o}_m$ is maximal isotropic. Indeed, it is of dimension 2, and for any $x, y \in \mathfrak{o}_m$, $\langle xe_2, ye_2\rangle = -\langle ye_2, xe_2\rangle$ because the form is alternating, and $\langle xe_2, ye_2\rangle = \langle ye_2, xe_2\rangle$ because it is K_0-bilinear, so $\langle xe_2, ye_2\rangle = 0$. Also, we have $\mathfrak{o}_{n-1} \subset \mathfrak{o}_m$, so

$$\langle \ell\mathfrak{o}_{n-1}e_1, \mathfrak{o}_m e_2\rangle = \langle \ell e_1, \mathfrak{o}_{n-1}\mathfrak{o}_m e_2\rangle = \ell\langle e_1, \mathfrak{o}_m e_2\rangle \subset \ell\mathbb{Z}_\ell.$$

This proves that $\ell\mathfrak{o}_{n-1}e_1/\ell\mathfrak{o}_n \subset (\mathfrak{o}_m e_2/\ell\mathfrak{o}_m)^\perp = \mathfrak{o}_m e_2/\ell\mathfrak{o}_m$, a contradiction. □

Using a standard abuse of notation, write $\mathbb{F}_\ell[\epsilon]$ for the ring of dual numbers, i.e. an $\mathbb{F}_\ell$-algebra isomorphic to $\mathbb{F}_\ell[X]/X^2$ via an isomorphism sending ϵ to X.

Lemma 6.8. *Let $R = \mathbb{F}_\ell[\epsilon]f_1 \oplus \mathbb{F}_\ell[\epsilon]f_2$ be a free $\mathbb{F}_\ell[\epsilon]$-module of rank 2. The $\mathbb{F}_\ell[\epsilon]$-submodules of R of $\mathbb{F}_\ell$-dimension 2 are exactly the $\ell^2+\ell+1$ modules ϵR, and $\mathbb{F}_\ell[\epsilon]\cdot g$ for any $g \notin \epsilon R$. A complete list of these orbits $\mathbb{F}_\ell[\epsilon]\cdot g$ is given by $\mathbb{F}_\ell[\epsilon]\cdot(b\epsilon f_1 + f_2)$ for any $b \in \mathbb{F}_\ell$, and $\mathbb{F}_\ell[\epsilon]\cdot(f_1 + \alpha f_2 + \beta\epsilon f_2)$, for any $\alpha, \beta \in \mathbb{F}_\ell$.*

Proof. Let $H \subset R$ be a subspace of dimension 2, stable under the action of $\mathbb{F}_\ell[\epsilon]$. For any $g \in H$, write $g = a_g f_1 + b_g\epsilon f_1 + c_g f_2 + d_g\epsilon f_2 \in H$ for $a_g, b_g, c_g, d_g \in \mathbb{F}_\ell$. Since H is $\mathbb{F}_\ell[\epsilon]$-stable, for any $g \in H$, the element $g\epsilon = a_g\epsilon f_1 + c_g\epsilon f_2$ is also in H.

First suppose $a_g = 0$ and $c_g = 0$ for any $g \in H$. Then, as $H = \epsilon R$, it is indeed an $\mathbb{F}_\ell[\epsilon]$-submodule and has $\mathbb{F}_\ell$-dimension 2. Now, suppose $a_g = 0$ for any $g \in H$, but H contains an element g such that $c_g \neq 0$ is non-zero. Then, H contains both $b_g\epsilon f_1 + c_g f_2 + d_g\epsilon f_2$, and $c_g\epsilon f_2$, so H is the $\mathbb{F}_\ell$-vector space spanned by ϵf_2 and $b_g \epsilon f_1 + c_g f_2$. There are $\ell + 1$ such subspaces H (one for each possible $(b_g : c_g) \in \mathbb{P}^1(\mathbb{F}_\ell)$), and all of them are of dimension 2 and R-stable.

Finally, suppose there exists $g \in H$ such that $a_g \neq 0$. Then, it is spanned as an $\mathbb{F}_\ell$-vector spaces by a pair $\{f_1 + \alpha f_2 + \beta\epsilon f_2, \epsilon f_1 + \alpha\epsilon f_2\}$, with $\alpha, \beta \in \mathbb{F}_\ell$, and any of the ℓ^2 subspaces of this form are $\mathbb{F}_\ell[\epsilon]$-submodules. □

Lemma 6.9. *Let Λ be an $\mathfrak{o}_n$-lattice, for some non-negative integer n. For any element $g \in \Lambda/\ell\Lambda$, the orbit $\mathfrak{o}_n \cdot g$ is an isotropic subspace of $\Lambda/\ell\Lambda$.*

Proof. Let $\lambda \in \Lambda$ such that $g = \lambda + \ell\Lambda$. For any $\alpha, \beta \in \mathfrak{o}_n$, we have $\langle \alpha\lambda, \beta\lambda \rangle = -\langle \beta\lambda, \alpha\lambda \rangle$ because the symplectic form on V is alternating, and $\langle \alpha\lambda, \beta\lambda \rangle = \langle \beta\lambda, \alpha\lambda \rangle$ because it is K_0-bilinear. So $\langle \alpha g, \beta g \rangle_\ell = 0$, and the orbit of g is isotropic. □

Proof of Proposition 6.6. From Lemma 6.7, Λ splits as $e_1\mathfrak{o}_n \oplus e_2\mathfrak{o}_n$, for some $e_1, e_2 \in \Lambda$. Observe that there is an element $\epsilon \in \mathfrak{o}_n$ such that $\mathfrak{o}_n/\ell\mathfrak{o}_n = \mathbb{F}_\ell[\epsilon] \cong \mathbb{F}_\ell[X]/(X^2)$, via the isomorphism sending ϵ to X. The quotient $R = \Lambda/\ell\Lambda$ is a free $\mathbb{F}_\ell[\epsilon]$-module of rank 2. Let $\pi : \Lambda \to R$ be the canonical projection. The set $\{f_1, \epsilon f_1, f_2, \epsilon f_2\}$ forms an $\mathbb{F}_\ell$-basis of R, where $f_i = \pi(e_i)$.

From Lemma 6.8, R contains $\ell^2 + \ell + 1$ subspaces of dimension 2 that are $\mathbb{F}_\ell[\epsilon]$-stable. The subspace $\epsilon R = \mathbb{F}_\ell\epsilon f_1 \oplus \mathbb{F}_\ell\epsilon f_2$ is isotropic because

$$\langle \epsilon f_1, \epsilon f_2 \rangle_\ell = \langle f_1, \epsilon^2 f_2 \rangle_\ell = 0.$$

Together with Lemma 6.9, we conclude that all $\ell^2 + \ell + 1$ of these $\mathbb{F}_\ell[\epsilon]$-stable subspaces are maximal isotropic. From Lemma 6.1, R contains a total of $\ell^3 + \ell^2 + \ell + 1$ maximal isotropic subspaces. Thus, the (ℓ, ℓ)-neighbors corresponding to the remaining ℓ^3 subspaces are not stable for the action of $\mathfrak{o}_n$. They are however stable for the action of $\mathfrak{o}_{n+1}$, so those are $\mathfrak{o}_{n+1}$-lattices.

It remains to prove that among the $\ell^2 + \ell + 1$ neighbors that are $\mathfrak{o}_n$-stable, only the lattice $\ell\mathfrak{o}_{n-1}\Lambda$ (which corresponds to the subspace ϵR) is $\mathfrak{o}_{n-1}$-stable, and that it is not $\mathfrak{o}_{n-2}$-stable. This would prove that $\ell\mathfrak{o}_{n-1}\Lambda$ is an $\mathfrak{o}_{n-1}$-lattice, and the $\ell^2 + \ell$ other lattices have order $\mathfrak{o}_n$.

Write $\Gamma = \ell\mathfrak{o}_{n-1}\Lambda$. Then $\pi(\Gamma) = \epsilon R$ is maximal isotropic and $\mathbb{F}_\ell[\epsilon]$-stable. Suppose by contradiction that we have $\mathfrak{o}_{n-2}\Gamma \subset \Gamma$. Then, $\ell\mathfrak{o}_{n-2}\Lambda \subset \mathfrak{o}_{n-2}\Gamma \subset \Gamma \subset \Lambda$, so $\ell\mathfrak{o}_{n-2}\Lambda \subset \Lambda$. But $\ell\mathfrak{o}_{n-2} \not\subset \mathfrak{o}_n$, which contradicts the fact that Λ is an $\mathfrak{o}_n$-lattice. Therefore Γ is an $\mathfrak{o}_{n-1}$-lattice.

Let $H \subset R$ be another maximal isotropic subspace, and suppose that $\pi^{-1}(H)$ is $\mathfrak{o}_{n-1}$-stable. Let $\lambda = e_1(a + \ell^n x) + e_2(b + \ell^n y) \in \pi^{-1}(H)$, with $a, b \in \mathbb{Z}_\ell$ and $x, y \in \mathfrak{o}_0$, and let $z \in \mathfrak{o}_{n-1}$. A simple computation yields

$$\Lambda = z\lambda + \Lambda = zae_1 + zbe_2 + \Lambda.$$

Therefore, both za and zb must be in $\mathfrak{o}_n$ for any $z \in \mathfrak{o}_{n-1}$. It follows that a and b must be in $\ell\mathbb{Z}_\ell$, whence $\lambda \in \Gamma$. So $\pi^{-1}(H) \subset \Gamma$, and we conclude that $H = \epsilon R$ from the fact that both are maximal isotropic. This proves that no (ℓ, ℓ)-neighbor other that Γ is $\mathfrak{o}_{n-1}$-stable. □

6.3. **Changing the real multiplication with (ℓ, ℓ)-isogenies.** The results for lattices are now ready to be applied to analyze how (ℓ, ℓ)-isogenies can change the real multiplication. Fix a principally polarizable absolutely simple ordinary abelian surface $\mathscr{A}$ over $\mathbb{F}_q$. As usual, K is its endomorphism algebra, and K_0 the maximal real subfield of K. The local real order $\mathfrak{o}_0(\mathscr{A})$ of $\mathscr{A}$ is of the form $\mathfrak{o}_n = \mathbb{Z}_\ell + \ell^n\mathfrak{o}_0$ for some non-negative integer n.

Definition 6.10. *Let $\varphi : \mathscr{A} \to \mathscr{B}$ be an isogeny. If $\mathfrak{o}_0(\mathscr{A}) \subset \mathfrak{o}_0(\mathscr{B})$, we say that φ is an* RM-ascending *isogeny, if $\mathfrak{o}_0(\mathscr{B}) \subset \mathfrak{o}_0(\mathscr{A})$ we say it is* RM-descending, *otherwise $\mathfrak{o}_0(\mathscr{A}) = \mathfrak{o}_0(\mathscr{B})$ and it is* RM-horizontal.

Proof of Theorem 3. Theorem 3 follows from Proposition 6.6 together with Remark 6.5, and the observation that the $\mathfrak{o}_{n-1}$-lattice $\ell\mathfrak{o}_{n-1}\Lambda$ has order $\mathfrak{o}_{n-1}\cdot\mathfrak{o}(\Lambda)$. □

In the following, we show that some structure of the graphs of horizontal isogenies at any level can be inferred from the structure at the maximal level: indeed, there is a graph homomorphism from any non-maximal level to the level above.

Definition 6.11 (RM-predecessor)**.** *Suppose $\mathfrak{o}_0(\mathscr{A}) = \mathfrak{o}_n$ with $n > 0$. Note that the kernel κ of the unique RM-ascending isogeny of Proposition 3 is given by $(\mathfrak{o}_{n-1}T_\ell\mathscr{A})/T_\ell\mathscr{A}$ (via Proposition 3.1) and does not depend on the polarization. The* RM-predecessor *of $\mathscr{A}$ is the variety $\mathrm{pr}(\mathscr{A}) = \mathscr{A}/\kappa$, and we denote by $\mathrm{up}_{\mathscr{A}} : \mathscr{A} \to \mathscr{A}/\kappa$ the canonical projection. If ξ is a principal polarization on $\mathscr{A}$, let $\mathrm{pr}(\xi)$ be the unique principal polarization induced by ξ via $\mathrm{up}_{\mathscr{A}}$.*

Proposition 6.12. *Suppose $n > 0$. For any principal polarization ξ on $\mathscr{A}$, and any RM-horizontal (ℓ,ℓ)-isogeny $\varphi : \mathscr{A} \to \mathscr{B}$ with respect to ξ, there is an (ℓ,ℓ)-isogeny $\tilde{\varphi} : \mathrm{pr}(\mathscr{A}) \to \mathrm{pr}(\mathscr{B})$ with respect to $\mathrm{pr}(\xi)$ such that the following diagram commutes:*

$$\begin{tikzcd}
\mathrm{pr}(\mathscr{A}) \arrow[r, "\tilde{\varphi}"] & \mathrm{pr}(\mathscr{B}) \\
\mathscr{A} \arrow[u, "\mathrm{up}_{\mathscr{A}}"] \arrow[r, "\varphi"] & \mathscr{B}. \arrow[u, "\mathrm{up}_{\mathscr{B}}"']
\end{tikzcd}$$

Proof. This follows from the fact that if Λ is an $\mathfrak{o}_n$-lattice, and $\Gamma \in \mathscr{L}(\Lambda)$ is an (ℓ,ℓ)-neighbor of Λ, then $\ell\mathfrak{o}_{n-1}\Gamma \in \mathscr{L}(\ell\mathfrak{o}_{n-1}\Lambda)$. □

7. (ℓ,ℓ)-ISOGENIES PRESERVING THE REAL MULTIPLICATION

7.1. **(ℓ,ℓ)-neighbors and $\mathfrak{l}$-neighbors.** Let $\mathscr{L}_0(\Lambda)$ be the set of (ℓ,ℓ)-neighbors of the lattice Λ with maximal real multiplication. These neighbors will be analysed through $\mathfrak{l}$-neighbors, for $\mathfrak{l}$ a prime ideal in $\mathfrak{o}_0$. This will allow us to account for the possible splitting behaviors of ℓ. The relation between the set $\mathscr{L}_0(\Lambda)$ and the sets $\mathscr{L}_\mathfrak{l}(\Lambda)$ is given by the following proposition proved case-by-case in the following three sections, as Propositions 7.2, 7.6 and 7.8:

Proposition 7.1. *Let Λ be a lattice with maximal real multiplication. The set of (ℓ,ℓ)-neighbors with maximal real multiplication is*

$$\mathscr{L}_0(\Lambda) = \begin{cases} \mathscr{L}_{\ell\mathfrak{o}_0}(\Lambda) & \text{if } \ell \text{ is inert in } K_0, \\ \mathscr{L}_{\mathfrak{l}_1}[\mathscr{L}_{\mathfrak{l}_2}(\Lambda)] = \mathscr{L}_{\mathfrak{l}_2}[\mathscr{L}_{\mathfrak{l}_1}(\Lambda)] & \text{if } \ell \text{ splits as } \mathfrak{l}_1\mathfrak{l}_2 \text{ in } K_0, \\ \mathscr{L}_\mathfrak{l}[\mathscr{L}_\mathfrak{l}(\Lambda)] & \text{if } \ell \text{ ramifies as } \mathfrak{l}^2 \text{ in } K_0. \end{cases}$$

7.1.1. *The inert case.* Suppose that ℓ is inert in K_0. Then, $\ell\mathcal{O}_{K_0}$ is the unique prime ideal of K_0 above ℓ. The orders in K_ℓ with maximal real multiplication are exactly the orders $\mathfrak{o}_{\ell^n\mathfrak{o}_0} = \mathfrak{o}_0 + \ell^n\mathfrak{o}_K$.

Proposition 7.2. *Let Λ be a lattice with maximal real multiplication. If ℓ is inert in K_0, the set of (ℓ,ℓ)-neighbors with maximal real multiplication is*

$$\mathscr{L}_0(\Lambda) = \mathscr{L}_{\ell\mathfrak{o}_0}(\Lambda).$$

Proof. Since $\mathfrak{o}_0/\ell\mathfrak{o}_0 \cong \mathbb{F}_{\ell^2}$, $\Lambda/\ell\Lambda$ is a free $\mathfrak{o}(\Lambda)/\ell\mathfrak{o}(\Lambda)$-module of rank 1. In particular, it is a vector space over $\mathbb{F}_{\ell^2}$ of dimension 2, and thereby the $\mathfrak{o}_0$-stable maximal isotropic subspaces of $\Lambda/\ell\Lambda$ are $\mathbb{F}_{\ell^2}$-lines. Since any $\mathbb{F}_{\ell^2}$-line is isotropic, $\mathscr{L}_{\ell\mathfrak{o}_0}(\Lambda)$ is precisely the set of (ℓ,ℓ)-neighbors preserving the maximal real multiplication. □

Remark 7.3. The structure of $\mathscr{L}_0(\Lambda)$ is then fully described by Proposition 4.5, with $\mathfrak{l} = \ell\mathfrak{o}_0$, and $N\mathfrak{l} = \ell^2$. In particular, $\mathscr{L}(\Lambda)$ consists of ℓ^2+1 neighbors with maximal real multiplication, and $\ell^3+\ell$ with real multiplication by $\mathfrak{o}_1$.

7.1.2. *The split case.* Suppose that ℓ splits in K_0 as $\ell\mathcal{O}_{K_0} = \mathfrak{l}_1\mathfrak{l}_2$. The orders in K_ℓ with maximal real multiplication are exactly the orders $\mathfrak{o}_{\mathfrak{f}} = \mathfrak{o}_0 + \mathfrak{f}\mathfrak{o}_K$, where $\mathfrak{f} = \mathfrak{l}_1^m\mathfrak{l}_2^n$ for any non-negative integers m and n.

Lemma 7.4. *Suppose Λ has maximal real multiplication. Then, we have the orthogonal decomposition $\Lambda/\ell\Lambda = (\mathfrak{l}_1\Lambda/\ell\Lambda) \perp (\mathfrak{l}_2\Lambda/\ell\Lambda)$.*

Proof. Let $\mathfrak{o} = \mathfrak{o}(\Lambda)$. Since $\mathfrak{l}_1$ and $\mathfrak{l}_2$ are coprime and $\mathfrak{l}_1\mathfrak{l}_2 = \ell\mathfrak{o}_0$, the quotient $\mathfrak{o}/\ell\mathfrak{o}$ splits as $\mathfrak{l}_1\mathfrak{o}/\ell\mathfrak{o} \oplus \mathfrak{l}_2\mathfrak{o}/\ell\mathfrak{o}$. It follows that $\Lambda/\ell\Lambda = (\mathfrak{l}_1\Lambda/\ell\Lambda) \oplus (\mathfrak{l}_2\Lambda/\ell\Lambda)$. Furthermore, $\langle \mathfrak{l}_1\Lambda, \mathfrak{l}_2\Lambda\rangle = \langle \Lambda, \mathfrak{l}_1\mathfrak{l}_2\Lambda\rangle = \langle \Lambda, \ell\Lambda\rangle \subset \ell\mathbb{Z}_\ell$, so $\mathfrak{l}_1\Lambda/\ell\Lambda \subset (\mathfrak{l}_2\Lambda/\ell\Lambda)^\perp$. The last inclusion is also an equality because both $\mathfrak{l}_1\Lambda/\ell\Lambda$ and $\mathfrak{l}_2\Lambda/\ell\Lambda$ have dimension 2. □

Lemma 7.5. *Suppose Λ has maximal real multiplication. An (ℓ,ℓ)-neighbor $\Gamma \in \mathscr{L}(\Lambda)$ has maximal real multiplication if and only if there exist $\Gamma_1 \in \mathscr{L}_{\mathfrak{l}_1}(\Lambda)$ and $\Gamma_2 \in \mathscr{L}_{\mathfrak{l}_2}(\Lambda)$ such that $\Gamma = \mathfrak{l}_2\Gamma_1 + \mathfrak{l}_1\Gamma_2$.*

Proof. First, let $\Gamma \in \mathscr{L}(\Lambda)$ be an (ℓ,ℓ)-neighbor with maximal real multiplication. Defining $\Gamma_i = \Gamma + \mathfrak{l}_i\Lambda$, we then have

$$\mathfrak{l}_2\Gamma_1 + \mathfrak{l}_1\Gamma_2 = (\mathfrak{l}_1 + \mathfrak{l}_2)\Gamma + \ell\Lambda = \mathfrak{o}_0\Gamma + \ell\Lambda = \Gamma.$$

By contradiction, suppose $\Gamma_i \notin \mathscr{L}_i(\Lambda)$. Then, Γ_i is either Λ or $\mathfrak{l}_i\Lambda$. Suppose first that $\Gamma_i = \Lambda$. Then $\Gamma \subset \mathfrak{l}_i\Lambda$, and even $\Gamma = \mathfrak{l}_i\Lambda$ since $[\Lambda : \Gamma] = [\Lambda : \mathfrak{l}_i\Lambda] = \ell^2$. But the orthogonal decomposition of Lemma 7.4 implies that $\mathfrak{l}_i\Lambda/\Lambda$ is not isotropic, contradicting the fact that $\Gamma \in \mathscr{L}(\Lambda)$.

For the converse, suppose $\Gamma = \mathfrak{l}_2\Gamma_1 + \mathfrak{l}_1\Gamma_2$ for some $\Gamma_1 \in \mathscr{L}_{\mathfrak{l}_1}(\Lambda)$ and $\Gamma_2 \in \mathscr{L}_{\mathfrak{l}_2}(\Lambda)$. Then $\Gamma/\ell\Lambda$ is of dimension 2, so it suffices to prove that it is isotropic. Each summand $\mathfrak{l}_i\Gamma_j$ is isotropic, because it is of dimension 1, and Lemma 7.4 implies that $\mathfrak{l}_2\Gamma_1$ and $\mathfrak{l}_1\Gamma_2$ are orthogonal, so their sum Γ is isotropic. □

Proposition 7.6. *Suppose Λ has maximal real multiplication. If ℓ splits in K_0 as $\ell\mathfrak{o}_0 = \mathfrak{l}_1\mathfrak{l}_2$, the set of (ℓ,ℓ)-neighbors of Λ with maximal real multiplication is*

$$\mathscr{L}_0(\Lambda) = \mathscr{L}_{\mathfrak{l}_1}[\mathscr{L}_{\mathfrak{l}_2}(\Lambda)] = \mathscr{L}_{\mathfrak{l}_2}[\mathscr{L}_{\mathfrak{l}_1}(\Lambda)].$$

Proof. For any $\Gamma_1 \in \mathscr{L}_{\mathfrak{l}_1}(\Lambda)$ and $\Gamma_2 \in \mathscr{L}_{\mathfrak{l}_2}(\Lambda)$, we have that $\mathfrak{l}_2\Gamma_1 + \mathfrak{l}_1\Gamma_2 \in \mathscr{L}_{\mathfrak{l}_2}(\Gamma_1)$ and $\mathfrak{l}_2\Gamma_1 + \mathfrak{l}_1\Gamma_2 \in \mathscr{L}_{\mathfrak{l}_1}(\Gamma_2)$. This proposition is thus a consequence of Lemma 7.5. □

Remark 7.7. When ℓ splits in K_0, $\mathscr{L}_0(\Lambda)$ is then of size $\ell^2+2\ell+1$, and the $\ell^3-\ell$ other (ℓ,ℓ)-neighbors have real order $\mathfrak{o}_1$.

7.1.3. *The ramified case.* Suppose that ℓ ramifies in K_0 as $\ell\mathcal{O}_{K_0} = \mathfrak{l}^2$. Then, $\mathfrak{o}_0/\ell\mathfrak{o}_0$ is isomorphic to $\mathbb{F}_\ell[\epsilon]$ with $\epsilon^2 = 0$. The orders in K_ℓ with maximal real multiplication are exactly the orders $\mathfrak{o}_{\mathfrak{l}^n} = \mathfrak{o}_0 + \mathfrak{l}^n\mathfrak{o}_K$.

Proposition 7.8. *Suppose Λ has maximal real multiplication. If ℓ splits in K_0 as $\ell\mathfrak{o}_0 = \mathfrak{l}^2$, the set of (ℓ,ℓ)-neighbors of Λ with maximal real multiplication is*

$$\mathscr{L}_0(\Lambda) = \mathscr{L}_{\mathfrak{l}}[\mathscr{L}_{\mathfrak{l}}(\Lambda)].$$

Proof. Let $\Gamma \in \mathscr{L}_0(\Lambda)$. First, if $\Gamma = \mathfrak{l}\Lambda$, observe that for any $\Pi \in \mathscr{L}_{\mathfrak{l}}(\Lambda)$, we have $\mathfrak{l}\Lambda \in \mathscr{L}_{\mathfrak{l}}(\Lambda)$, and therefore $\Gamma \in \mathscr{L}_{\mathfrak{l}}[\mathscr{L}_{\mathfrak{l}}(\Lambda)]$. We can now safely suppose $\Gamma \neq \mathfrak{l}\Lambda$. Let $\Pi = \Gamma + \mathfrak{l}\Lambda$. We have the sequence of inclusions

$$\ell\Lambda \subset \mathfrak{l}\Pi \subset \Gamma \subsetneq \Pi \subset \Lambda.$$

By contradiction, suppose $\Pi = \Lambda$. Then, $\Gamma \cap \mathfrak{l}\Lambda = \ell\Lambda$. Since $\mathfrak{l}\Gamma \subset \Gamma \cap \mathfrak{l}\Lambda = \ell\Lambda$, it follows that $\mathfrak{l}\Lambda = \mathfrak{l}\Pi = \mathfrak{l}\Gamma + \ell\Lambda \subset \ell\Lambda$, a contradiction. Therefore $\Gamma \subsetneq \Pi \subsetneq \Lambda$, and each inclusion must be of index ℓ. Then, $\Gamma \in \mathscr{L}_{\mathfrak{l}}(\Pi) \subset \mathscr{L}_{\mathfrak{l}}[\mathscr{L}_{\mathfrak{l}}(\Lambda)]$.

Let us now prove that $\mathscr{L}_{\mathfrak{l}}[\mathscr{L}_{\mathfrak{l}}(\Lambda)] \subset \mathscr{L}_0(\Lambda)$. Let $\Pi \in \mathscr{L}_{\mathfrak{l}}(\Lambda)$ and $\Gamma \in \mathscr{L}_{\mathfrak{l}}(\Pi)$. We have the sequence of inclusions

$$\ell\Lambda = \mathfrak{l}(\mathfrak{l}\Lambda) \subset_\ell \mathfrak{l}\Pi \subset_\ell \Gamma \subset_\ell \Pi \subset_\ell \Lambda,$$

where $\subset_\ell$ means that the first lattice is of index ℓ in the second. Therefore $\ell\Lambda \subset \Gamma \subset \Lambda$, and $\Gamma/\ell\Lambda$ is of dimension 2 over $\mathbb{F}_\ell$. Since $\Gamma/\mathfrak{l}\Lambda$ is a line, there is an element $\pi \in \Pi$ such that $\Pi = \mathbb{Z}_\ell\pi + \mathfrak{l}\Lambda$. Similarly, $\Pi/\mathfrak{l}\Gamma$ is a line, so there is an element $\gamma \in \Gamma$ such that $\Gamma = \mathbb{Z}_\ell\gamma + \mathfrak{l}\pi + \ell\Lambda$. Therefore, writing $x = \gamma + \ell\Lambda$ and $y = \pi + \ell\Lambda$, $\Gamma/\ell\Lambda$ is generated as an $\mathbb{F}_\ell$-vector space by x and ϵy. Since $\gamma \in \Gamma \subset \Pi = \mathbb{Z}_\ell\pi + \mathfrak{l}\Lambda$, there exist $a \in \mathbb{Z}_\ell$ and $z \in \Lambda/\ell\Lambda$ such that $x = ay + \epsilon z$. Then,

$$\langle x, \epsilon y\rangle_\ell = \langle ay, \epsilon y\rangle_\ell + \langle \epsilon z, \epsilon y\rangle_\ell = a\langle y, \epsilon y\rangle_\ell + \langle z, \epsilon^2 y\rangle_\ell = 0,$$

where the last equality uses Lemma 6.9, and the fact that $\epsilon^2 = 0$. So $\Gamma/\ell\Lambda$ is maximal isotropic, and $\Gamma \in \mathscr{L}(\Lambda)$. Furthermore $\epsilon x = a\epsilon y$, and $\epsilon y = 0$ are both in $\Gamma/\ell\Lambda$, so the latter is $\mathbb{F}_\ell[\epsilon]$-stable, so Γ is $\mathfrak{o}_0$-stable. This proves that $\Gamma \in \mathscr{L}_0(\Lambda)$. □

Remark 7.9. We can deduce from Lemma 6.8 that $|\mathscr{L}_0(\Lambda)| = \ell^2 + \ell + 1$. In fact, for any two distinct lattices $\Pi_1, \Pi_2 \in \mathscr{L}_{\mathfrak{l}}(\Lambda)$, we have $\mathscr{L}_{\mathfrak{l}}(\Pi_1) \cap \mathscr{L}_{\mathfrak{l}}(\Pi_2) = \{\mathfrak{l}\Lambda\}$.

7.2. Locally maximal real multiplication and (ℓ,ℓ)-isogenies.

Fix again a principally polarizable absolutely simple ordinary abelian surface $\mathscr{A}$ over $\mathbb{F}_q$, with endomorphism algebra K, and K_0 the maximal real subfield of K. Now suppose that $\mathscr{A}$ has locally maximal real multiplication at ℓ. Recall from Theorem 4 that any such locally maximal real order is of the form $\mathfrak{o}_{\mathfrak{f}} = \mathfrak{o}_0 + \mathfrak{f}\mathfrak{o}_K$, for some $\mathfrak{o}_0$-ideal $\mathfrak{f}$. The structure of $\mathfrak{l}$-isogeny graphs as described by Theorem 1 can be used to describe graphs of (ℓ,ℓ)-isogenies preserving the real multiplication, via Theorem 2.

Proof of Theorem 2. This theorem is a direct consequence of Proposition 7.1 translated to the world of isogenies via Remark 6.5. □

Remark 7.10. Note that in particular, Theorem 2 implies that the kernels of the (ℓ,ℓ)-isogenies $\mathscr{A} \to \mathscr{B}$ preserving the real multiplication do not depend on the choice of a polarization ξ on $\mathscr{A}$.

7.2.1. *The inert and ramified cases.* Combining Theorem 1 and Theorem 2 allows us to describe the graph of (ℓ,ℓ)-isogenies with maximal local real multiplication at ℓ. For purpose of exposition, we assume from now on that the primitive quartic CM-field K is different from $\mathbb{Q}(\zeta_5)$, but the structure for $\mathbb{Q}(\zeta_5)$ can be deduced in the same way (bearing in mind that in that case, $\mathcal{O}_{K_0}^\times$ is of index 5 in $\mathcal{O}_K^\times$). Let $\mathscr{A}$ be any principally polarizable abelian variety with order $\mathcal{O}$, with maximal real

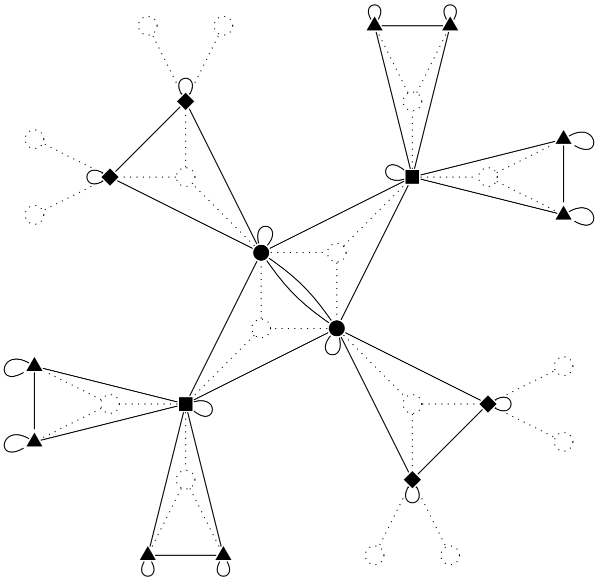

FIGURE 4. An example of (ℓ,ℓ)-isogeny graph, when ℓ ramifies in K_0.

multiplication locally at ℓ. When ℓ is inert in K_0, the connected component of $\mathscr{A}$ in the (ℓ,ℓ)-isogeny graph (again, for maximal local real multiplication) is exactly the volcano $\mathscr{V}_{\mathfrak{l}}(\mathcal{O})$ (see Notation 4.16). When ℓ ramifies as $\mathfrak{l}^2$ in K_0, the connected component of $\mathscr{A}$ in the graph of $\mathfrak{l}$-isogenies is isomorphic to the graph $\mathscr{V}_{\mathfrak{l}}(\mathcal{O})$, and the graph of (ℓ,ℓ)-isogenies can be constructed from it as follows: on the same set of vertices, add an edge in the (ℓ,ℓ)-graph between $\mathscr{B}$ and $\mathscr{C}$ for each path of length 2 between $\mathscr{B}$ and $\mathscr{C}$ in the $\mathfrak{l}$-volcano; each vertex $\mathscr{B}$ has now $\ell^2+2\ell+1$ outgoing edges, while there are only $\ell^2+\ell+1$ possible kernels of RM-preserving (ℓ,ℓ)-isogenies (see Remark 7.9). This is because the edge corresponding to the canonical projection $\mathscr{B}\to\mathscr{B}/\mathscr{B}[\mathfrak{l}]$ has been accounted for $\ell+1$ times. Remove ℓ of these copies, and the result is exactly the graph of (ℓ,ℓ)-isogenies.

Example 7.11. Suppose $\ell=2$ ramifies in K_0 as $\mathfrak{l}^2$, and $\mathfrak{l}$ is principal in $\mathcal{O}_{K_0}$. Suppose further that $\mathfrak{l}$ splits in K into two prime ideals of order 4 in $\mathrm{Cl}(\mathcal{O}_K)$. Then, the first four levels of any connected component of the (ℓ,ℓ)-isogeny graph for which the largest order is $\mathcal{O}_K$ are isomorphic to the graph of Figure 4. The underlying $\mathfrak{l}$-isogeny volcano is represented with dotted nodes and edges. Since $\mathfrak{l}$ is principal in $\mathcal{O}_{K_0}$, it is an undirected graph, and we represent it as such. The level 0, i.e., the surface of the volcano, is the dotted cycle of length 4 at the center. The circles have order $\mathcal{O}_K$, the squares have order $\mathcal{O}_{K_0}+\mathfrak{l}\mathcal{O}_K$, the diamonds $\mathcal{O}_{K_0}+\ell\mathcal{O}_K$, and the triangles $\mathcal{O}_{K_0}+\mathfrak{l}^3\mathcal{O}_K$.

7.2.2. *The split case.* For simplicity, suppose again that the primitive quartic CM-field K is a different from $\mathbb{Q}(\zeta_5)$. Let $\mathscr{A}$ be any principally polarizable abelian variety with order $\mathcal{O}$, with maximal real multiplication locally at ℓ. The situation when ℓ splits as $\mathfrak{l}_1\mathfrak{l}_2$ in K_0 (with $\mathfrak{l}_1$ and $\mathfrak{l}_2$ principal in $\mathcal{O}\cap K_0$) is a bit more delicate because the $\mathfrak{l}_1$ and $\mathfrak{l}_2$-isogeny graphs need to be carefully pasted together. Let

$\mathscr{G}_{\mathfrak{l}_1,\mathfrak{l}_2}(\mathscr{A})$ be the connected component of $\mathscr{A}$ in the labelled isogeny graphs whose edges are $\mathfrak{l}_1$-isogenies (labelled $\mathfrak{l}_1$) and $\mathfrak{l}_2$-isogenies (labelled $\mathfrak{l}_2$). The graph of (ℓ,ℓ)-isogenies is the graph on the same set of vertices, such that the number of edges between two vertices $\mathscr{B}$ and $\mathscr{C}$ is exactly the number of paths of length 2 from $\mathscr{B}$ to $\mathscr{C}$, whose first edge is labelled $\mathfrak{l}_1$ and second edge is labelled $\mathfrak{l}_2$. It remains to fully understand the structure of the graph $\mathscr{G}_{\mathfrak{l}_1,\mathfrak{l}_2}(\mathscr{A})$. Like for the cases where ℓ is inert or ramified in K_0, we would like a complete characterization of the structure of the isogeny graph, i.e., a description that is sufficient to construct an explicit model of the abstract graph.

Without loss of generality, suppose $\mathcal{O}$ is locally maximal at ℓ. Then, the endomorphism ring of any variety in $\mathscr{G}_{\mathfrak{l}_1,\mathfrak{l}_2}(\mathscr{A})$ is characterized by the conductor $\mathfrak{l}_1^m\mathfrak{l}_2^n$ at ℓ, and we denote by $\mathcal{O}_{m,n}$ the corresponding order. The graph $\mathscr{G}_{\mathfrak{l}_1,\mathfrak{l}_2}(\mathscr{A})$ only depends on the order, so we also denote it $\mathscr{G}_{\mathfrak{l}_1,\mathfrak{l}_2}(\mathcal{O})$. For simplicity of exposition, let us assume that $\mathfrak{l}_1$ and $\mathfrak{l}_2$ are principal in $\mathcal{O}\cap K_0$, so that the $\mathfrak{l}_i$-isogeny graphs are volcanoes.

Definition 7.12 (cyclic homomorphism). *Let $\mathscr{X}$ and $\mathscr{Y}$ be two graphs. A graph homomorphism $\psi : \mathscr{X} \to \mathscr{Y}$ is a* cyclic homomorphism *if each edge of $\mathscr{X}$ and $\mathscr{Y}$ can be directed in such a way that ψ becomes a homomorphism of directed graphs, and each undirected cycle in $\mathscr{X}$ becomes a directed cycle.*

Lemma 7.13. *Let $\mathscr{X}$, $\mathscr{Y}$ and $\mathscr{Y}'$ be connected, d-regular graphs, with $d \leq 2$, such that $\mathscr{Y}$ and $\mathscr{Y}'$ are isomorphic. If $\varphi : \mathscr{Y} \to \mathscr{X}$ and $\varphi' : \mathscr{Y}' \to \mathscr{X}$ are two cyclic homomorphisms, there is an isomorphism $\psi : \mathscr{Y} \to \mathscr{Y}'$ such that $\varphi = \varphi' \circ \psi$.*

Proof. The statement is trivial if d is 0 or 1. Suppose $d = 2$, i.e., $\mathscr{X}$, $\mathscr{Y}$ and $\mathscr{Y}'$ are cycles. Let $\mathscr{X}$ be the cycle $x_0 - x_1 - \cdots - x_m$, with $x_m = x_0$. Similarly, $\mathscr{Y}$ is the cycles $y_0 - y_1 - \cdots - y_n$, with $y_n = y_0$. Without loss of generality, $\varphi(y_0) = x_0$ and $\varphi(y_1) = x_1$. There is a direction on the edges of $\mathscr{X}$ and $\mathscr{Y}$ such that φ becomes a homomorphism of directed graphs, and $\mathscr{Y}$ becomes a directed cycle. Without loss of generality, the direction of $\mathscr{Y}$ is given by $y_i \to y_{i+1}$. Since $y_0 \to y_1$, we have $\varphi(y_0) \to \varphi(y_1)$, hence $x_0 \to x_1$. Since $y_1 \to y_2$, we must also have $x_1 \to \varphi(y_2)$, so $\varphi(y_2) \neq x_0$ and therefore $\varphi(y_2) = x_2$, and as a consequence $x_1 \to x_2$. Repeating inductively, we obtain $x_i \to x_{i+1}$ for all $i \leq m$, and $\varphi(y_i) = x_{i \bmod m}$ for all $i \leq n$.

Similarly, any direction on $\mathscr{X}$ and $\mathscr{Y}'$ such that $\mathscr{Y}'$ is a directed cycle and φ' becomes a homomorphism of directed graphs turns $\mathscr{X}$ into a directed cycle. Without loss of generality, it is exactly the directed cycle $x_0 \to x_1 \to \cdots \to x_m$ (if it is the other direction, simply invert the directions of $\mathscr{Y}'$). There is then an enumeration $\{y_i'\}_{i=0}^n$ of $\mathscr{Y}'$ such that $\varphi'(y_i') = x_i$, and $y_i' \to y_{i+1}'$ for each i. The isomorphism ψ is then simply given by $\psi(y_i) = y_i'$. □

Proposition 7.14. *The graph $\mathscr{G}_{\mathfrak{l}_1,\mathfrak{l}_2}(\mathcal{O})$, with edges labelled by $\mathfrak{l}_1$ and $\mathfrak{l}_2$, and bi-levelled by $(v_{\mathfrak{l}_1}, v_{\mathfrak{l}_2})$, is isomorphic to the unique (up to isomorphism) graph $\mathscr{G}$ with edges labelled by $\mathfrak{l}_1$ and $\mathfrak{l}_2$, and bi-levelled by a pair (v_1, v_2), satisfying:*

(i) For $i = 1, 2$, the subgraph of $\mathscr{G}$ containing only the edges labelled by $\mathfrak{l}_i$ is a disjoint union of ℓ-volcanoes, levelled by v_i,

(ii) For $i \neq j$, if u and v are connected by an $\mathfrak{l}_i$-edge, then $v_j(u) = v_j(v)$,

(iii) For any non-negative integers m, and n, let $\mathscr{G}_{m,n}$ be the subgraph containing the vertices v such that $(v_1(v), v_2(v)) = (m, n)$. Then,

(i) *$\mathscr{G}_{0,0}$ is isomorphic to the Cayley graph $\mathscr{C}_{0,0}$ of the subgroup of* $\mathrm{Pic}(\mathcal{O})$ *with generators the invertible ideals of the order $\mathcal{O}$ above ℓ, naturally labelled by $\mathfrak{l}_1$ and $\mathfrak{l}_2$,*

(ii) *each connected component of $\mathscr{G}_{m,n}$ is isomorphic to the Cayley graph $\mathscr{C}_{m,n}$ of the subgroup of* $\mathrm{Pic}(\mathcal{O}_{m,n})$ *with generators the invertible ideals of the order $\mathcal{O}_{m,n}$ above ℓ, naturally labelled by $\mathfrak{l}_1$ and $\mathfrak{l}_2$,*

(iv) *For any two vertices u and v in $\mathscr{G}$, there is a path of the form $u -_{\mathfrak{l}_1} w -_{\mathfrak{l}_2} v$ if and only if there is a path of the form $u -_{\mathfrak{l}_2} w' -_{\mathfrak{l}_1} v$ (where $-_{\mathfrak{l}_i}$ denotes an edge labelled by $\mathfrak{l}_i$).*

Proof. First, it is not hard to see that $\mathscr{G}_{\mathfrak{l}_1,\mathfrak{l}_2}(\mathcal{O})$ satisfies all these properties. Properties (i) and (ii) follow from Proposition 4.7 and Theorem 1. Property (iii) follows from the free CM-action of $\mathrm{Pic}(\mathcal{O}_{m,n})$ on the corresponding isomorphism classes. Property (iv) follows from the fact that $\mathscr{A}[\mathfrak{l}_1] \oplus \mathscr{A}[\mathfrak{l}_2]$ is a direct sum.

Let $\mathscr{G}$ and $\mathscr{G}'$ be two graphs with these properties. For $i = 1, 2$, let pr_i (respectively, pr'_i) be the predecessor map induced by the volcano structure of the $\mathfrak{l}_i$-edges on $\mathscr{G}$ (respectively, on $\mathscr{G}'$). We will construct an isomorphism $\Psi : \mathscr{G} \to \mathscr{G}'$ by starting with the isomorphism between $\mathscr{G}_{0,0}$ and $\mathscr{G}'_{0,0}$ and extending it on the blocks $\mathscr{G}_{m,n}$ and $\mathscr{G}'_{m,n}$ one at a time. Let $n > 0$, and suppose, by induction, that Ψ has been defined exactly on the blocks $\mathscr{G}_{i,j}$ for $i + j < n$. Let us extend Ψ to the blocks $\mathscr{G}_{m,n-m}$ for $m = 0, \ldots, n$ in order.

Both $\mathscr{G}_{0,n}$ and $\mathscr{G}'_{0,n}$ have the same number of vertices, and their connected components are all isomorphic $\mathscr{C}_{0,n}$, which are of degree d at most 2. We have the graph homomorphism $\mathrm{pr}_2 : \mathscr{G}_{0,n} \to \mathscr{G}_{0,n-1}$. Let S be the set of connected components of $\mathscr{G}_{0,n}$. Define the equivalence relation on S

$$A \sim B \Longleftrightarrow \mathrm{pr}_2(A) = \mathrm{pr}_2(B).$$

Similarly define the equivalence relation $\sim'$ on the set S' of connected components of $\mathscr{G}'_{0,n}$. Observe that each equivalence class for either $\sim$ or $\sim'$ has same cardinality, so one can choose a bijection $\Theta : S \to S'$ such that for any $A \in S$, we have $\Psi(\mathrm{pr}_2(A)) = \mathrm{pr}'_2(\Theta(A))$. It is not hard to check that pr_2 and pr'_2 are cyclic homomorphisms, using Property (iv). From Lemma 7.13, for each $A \in S$, there is a graph isomorphism $\psi_A : A \to \Theta(A)$ such that for any $x \in A$, $\mathrm{pr}'_2(\psi_A(x)) = \Psi(\mathrm{pr}_2(x))$. Let $\hat{\Psi}$ be the map extending Ψ by sending any $x \in \mathscr{G}_{0,n}$ to $\psi_A(x)$, where A is the connected component of x in $\mathscr{G}_{0,n}$. We need to show that it is a graph isomorphism. Write $\mathscr{D}$ and $\mathscr{D}'$ the domain and codomain of Ψ. The map $\hat{\Psi}$, restricted and corestricted to $\mathscr{D}$ and $\mathscr{D}'$ is exactly Ψ so is an isomorphism. Also, the restriction and corestriction to $\mathscr{G}_{0,n}$ and $\mathscr{G}'_{0,n}$ is an isomorphism, by construction. Only the edges between $\mathscr{G}_{0,n}$ and $\mathscr{D}$ (respectively $\mathscr{G}'_{0,n}$ and $\mathscr{D}'$) might cause trouble. The only edges between $\mathscr{G}_{0,n}$ and $\mathscr{D}$ are actually between $\mathscr{G}_{0,n}$ and $\mathscr{G}_{0,n-1}$, and are of the form $(x, \mathrm{pr}_2(x))$. But Ψ was precisely constructed so that $\Psi(\mathrm{pr}_2(x)) = \mathrm{pr}'_2(\Psi(x))$, so $\hat{\Psi}$ is indeed an isomorphism.

Now, let $0 < m < n$ and suppose that Ψ has been extended to the components $\mathscr{G}_{i,n-i}$ for each $i < m$. Let us extend it to $\mathscr{G}_{m,n-m}$. Since $m > 0$ and $n - m > 0$, the graph $\mathscr{C}_{m,n-m}$ is a single point, with no edge. Let us now prove that for any pair (x_1, x_2), where x_1 is a vertex in $\mathscr{G}_{m-1,n-m}$ and x_2 in $\mathscr{G}_{m,n-m-1}$ such that $\mathrm{pr}_2(x_1) = \mathrm{pr}_1(x_2)$, there is a unique vertex x in $\mathscr{G}_{m,n-m}$ such that $(x_1, x_2) = (\mathrm{pr}_1(x), \mathrm{pr}_2(x))$. First, we show that for any vertex $x \in \mathscr{G}_{m,n-m}$, we have

$$\mathrm{pr}_1^{-1}(\mathrm{pr}_1(x)) \cap \mathrm{pr}_2^{-1}(\mathrm{pr}_2(x)) = \{x\}.$$

Let $z = \mathrm{pr}_1(\mathrm{pr}_2(x))$. Let $X = \mathrm{pr}_1^{-1}(\mathrm{pr}_1(x))$ and $Y = \mathrm{pr}_1^{-1}(z)$. From Property (ii), z and $\mathrm{pr}_1(x)$ are at the same v_1-level, so from Property (i), we have $|X| = |Y|$. For any $y \in Y$, we have $\mathrm{pr}_1(x) -_{\mathfrak{l}_2} z -_{\mathfrak{l}_1} y$, so there is a vertex x' such that $\mathrm{pr}_1(x) -_{\mathfrak{l}_1} x' -_{\mathfrak{l}_2} y$. Then, $v_1(x') = v_1(y) = v_1(\mathrm{pr}_1(x)) - 1$, and therefore $x' \in X$. This implies that pr_2 induces a surjection $\tilde{\mathrm{pr}}_2 : X \to Y$, which is a bijection since $|X| = |Y|$. So

$$X \cap \mathrm{pr}_2^{-1}(\mathrm{pr}_2(x)) = X \cap \tilde{\mathrm{pr}}_2^{-1}(\mathrm{pr}_2(x)) = \{x\}.$$

Now, an elementary counting argument shows that $x \mapsto (\mathrm{pr}_1(x), \mathrm{pr}_2(x))$ is a bijection between the vertices of $\mathscr{G}_{m,n-m}$ and the pairs (x_1, x_2), where x_1 is a vertex in $\mathscr{G}_{m-1,n-m}$ and x_2 in $\mathscr{G}_{m,n-m-1}$ such that $\mathrm{pr}_2(x_1) = \mathrm{pr}_1(x_2)$. This property also holds in $\mathscr{G}'$, and we can thereby define $\psi : \mathscr{G}_{m,n-m} \to \mathscr{G}'_{m,n-m}$ as the bijection sending any vertex x in $\mathscr{G}_{m,n-m}$ to the unique vertex x' in $\mathscr{G}'_{m,n-m}$ such that

$$(\mathrm{pr}'_1(x'), \mathrm{pr}'_2(x')) = (\Psi(\mathrm{pr}_1(x)), \Psi(\mathrm{pr}_2(x))).$$

It is then easy to check that the extension of Ψ induced by ψ is an isomorphism. The final step, extending on $\mathscr{G}_{n,0}$, is similar to the case of $\mathscr{G}_{0,n}$. This concludes the induction, and proves that $\mathscr{G}$ and $\mathscr{G}'$ are isomorphic. □

8. Applications to "going up" algorithms

8.1. **Largest reachable orders.** The results from Section 6.3 and Section 7.2 on the structure of the graph of (ℓ, ℓ)-isogenies allow us to determine exactly when there exists a sequence of (ℓ, ℓ)-isogenies leading to a surface with maximal local order at ℓ. When there is no such path, one can still determine the largest reachable orders.

Proposition 8.1. *Suppose $\mathscr{A}$ has maximal local real order, and $\mathfrak{o}(\mathscr{A}) = \mathfrak{o}_{\mathfrak{f}}$.*

(i) If ℓ divides $\mathfrak{f}$, there is a unique (ℓ, ℓ)-isogeny to a surface with order $\mathfrak{o}_{\ell^{-1}\mathfrak{f}}$.

(ii) If ℓ ramifies in K_0 as $\mathfrak{l}^2$ and $\mathfrak{f} = \mathfrak{l}$, then there exists an (ℓ, ℓ)-isogeny to a surface with maximal local order if and only if $\mathfrak{l}$ is not inert in K. It is unique if $\mathfrak{l}$ is ramified, and there are two if it splits.

(iii) If ℓ splits in K_0 as $\mathfrak{l}_1\mathfrak{l}_2$, and $\mathfrak{f} = \mathfrak{l}_1^i$ for some $i > 0$, then there exists an (ℓ, ℓ)-isogeny to a surface with local order $\mathfrak{o}_{\mathfrak{l}_1^{i-1}}$ if and only if $\mathfrak{l}_2$ is not inert in K. It is unique if $\mathfrak{l}_2$ is ramified, and there are two if it splits. Also, there always exist an (ℓ, ℓ)-isogeny to a surface with local order $\mathfrak{o}_{\mathfrak{l}_1^{i-1}\mathfrak{l}_2}$.

Proof. This is a straightforward case-by-case analysis of Propositions 4.7 and Theorem 2. □

Definition 8.2 (parity of $\mathscr{A}$). *Suppose $\mathscr{A}$ has real order $\mathfrak{o}_n = \mathbb{Z}_\ell + \ell^n\mathfrak{o}_0$. Construct $\mathscr{B}$ by the RM-predecessor of $\mathcal{A}$ n times, i.e., $\mathscr{B} = \mathrm{pr}(\mathrm{pr}(\ldots \mathrm{pr}(\mathscr{A}) \ldots))$ is the (iterated) RM-predecessor of $\mathscr{A}$ that has maximal real local order. Let $\mathfrak{f}$ be the conductor of $\mathfrak{o}(\mathscr{B})$. The* parity *of $\mathscr{A}$ is 0 if $N(\mathfrak{f} \cap \mathfrak{o}_0)$ is a square, and 1 otherwise.*

Remark 8.3. The parity is always 0 if ℓ is inert in K_0.

Theorem 6. *For any $\mathscr{A}$, there exists a sequence of (ℓ, ℓ)-isogenies starting from $\mathscr{A}$ and ending at a variety with maximal local order, except in the following two cases:*

(i) $\mathscr{A}$ has parity 1, ℓ splits in K_0 as $\mathfrak{l}_1\mathfrak{l}_2$, and both $\mathfrak{l}_1$ and $\mathfrak{l}_2$ are inert in K, in which case the largest reachable local orders are $\mathfrak{o}_0 + \mathfrak{l}_1\mathfrak{o}_K$ and $\mathfrak{o}_0 + \mathfrak{l}_2\mathfrak{o}_K$;

(ii) $\mathscr{A}$ *has parity 1,* ℓ *ramifies in* K_0 *as* $\mathfrak{l}^2$*, and* $\mathfrak{l}$ *is inert in* K*, in which case the largest reachable local order is* $\mathfrak{o}_0 + \mathfrak{l}\mathfrak{o}_K$.

Proof. First, from Propositon 6.12, there is a sequence of (ℓ,ℓ)-isogenies starting from $\mathscr{A}$ and ending at a variety with maximal local order if and only if there is such a path that starts by a sequence of isogenies up to $\mathscr{B} = \mathrm{pr}(\mathrm{pr}(\dots\mathrm{pr}(\mathscr{A})\dots))$, and then only consists of (ℓ,ℓ)-isogenies preserving the maximality of the local real order. It is therefore sufficient to look at sequences of RM-preserving (ℓ,ℓ)-isogenies from $\mathscr{B}$, which has by construction the same parity s as $\mathscr{A}$.

From Proposition 8.1, there is a path from $\mathscr{B}$ to a surface $\mathscr{C}$ with local order $\mathfrak{o}(\mathscr{C}) = \mathfrak{o}_{\mathfrak{l}^s}$ where $\mathfrak{l}$ is a prime ideal of $\mathfrak{o}_0$ above ℓ, and s is the parity of $\mathscr{A}$. We are done if the parity is 0. Suppose the parity is 1. From Propositions 4.7 and Theorem 2, one can see that there exists a sequence of RM-preserving (ℓ,ℓ)-isogeny from $\mathscr{C}$ which changes the parity to 0 if and only if ℓ ramifies in K_0 as $\mathfrak{l}^2$ and $\mathfrak{l}$ is not inert in K, or ℓ splits in K_0 as $\mathfrak{l}_1\mathfrak{l}_2$ and either $\mathfrak{l}_1$ or $\mathfrak{l}_2$ is not inert in K. This concludes the proof. □

8.2. **A "going up" algorithm.** In many applications (in particular, the CM method in genus 2 based on the CRT) it is useful to find a chain of isogenies to a principally polarized abelian surface with maximal endomorphism ring starting from any curve whose Jacobian is in the given isogeny class. Lauter and Robert [LR12a, §5] propose a probabilistic algorithm to construct a principally polarized abelian variety whose endomorphism ring is maximal. That algorithm is heuristic, and the probability of failure is difficult to analyze. We now apply our structural results from Subsection 7.2 to some of their ideas to give a provable algorithm.

8.2.1. *Prior work of Lauter–Robert.* Given a prime ℓ for which we would like to find an isogenous abelian surface over $\mathbb{F}_q$ with maximal local endomorphism ring at ℓ, suppose that $\alpha = \ell^e\alpha'$ for some $\alpha' \in \mathcal{O}_K$ and some $e > 0$. To find a surface $\mathscr{A}'/\mathbb{F}_q$ for which $\alpha/\ell^e \in \mathrm{End}(\mathscr{A}')$, Lauter and Robert [LR12a, §5] use (ℓ,ℓ)-isogenies and a test for whether $\alpha/\ell^e \in \mathrm{End}(\mathscr{A}')$. In fact, $\alpha/\ell^e \in \mathrm{End}(\mathscr{A}')$ is equivalent to testing that $\alpha(\mathscr{A}'[\ell^e]) = 0$, i.e., α is trivial on the ℓ^e-torsion of $\mathscr{A}$. To guarantee that, one defines an "obstruction" $N_e = \#\alpha(\mathscr{A}[\ell^e])$ that measures the failure of α/ℓ^e to be an endomorphism of $\mathscr{A}'$. To construct an abelian surface that contains the element α/ℓ^e as endomorphism, one uses (ℓ,ℓ)-isogenies iteratively in order to decrease the associated obstruction N_e (this is in essence the idea of [LR12a, Alg.21]).

To reach an abelian surface with maximal local endomorphism ring at ℓ, Lauter and Robert look at the structure of $\mathrm{End}(\mathscr{A}) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ as a $\mathbb{Z}_\ell$-module and define an obstruction via a particular choice of a $\mathbb{Z}_\ell$-basis [LR12a, Alg.23].

8.2.2. *Refined obstructions and provable algorithm.* Theorem 6 above gives a provable "going up" algorithm that runs in three main steps: 1) it uses (ℓ,ℓ)-isogenies to reach a surface with maximal local real endomorphism ring at ℓ; 2) it reaches the largest possible order via (ℓ,ℓ)-isogenies as in Theorem 6; 3) if needed, it makes a last step to reach maximal local endomorphism ring via a cyclic isogeny. To implement 1) and 2), one uses refined obstructions, which we now describe in detail.

8.2.3. *"Going up" to maximal real multiplication.* Considering the local orders $\mathfrak{o}_0 = \mathcal{O}_{K_0} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ and $\mathbb{Z}_\ell[\pi + \pi^\dagger]$, choose a $\mathbb{Z}_\ell$-basis $\{1, \beta/\ell^e\}$ for $\mathfrak{o}_0$ such that $\beta \in \mathbb{Z}[\pi,\pi^\dagger]$ and we apply a "real-multiplication" modification of [LR12a, Alg.21] to β. Thus, given an abelian surface $\mathscr{A}$ with endomorphism algebra isomorphic to K, define the obstruction for $\mathscr{A}$ to have maximal real multiplication at ℓ as

$$N_0(\mathscr{A}) = e - \max\{\epsilon \colon \beta(\mathscr{A}[\ell^\epsilon]) = 0\}.$$

Clearly, $\mathscr{A}$ will have maximal real endomorphism ring at ℓ if and only if $N_0(\mathscr{A}) = 0$. The following simple lemma characterizes the obstruction:

Lemma 8.4. *The obstruction $N_0(\mathscr{A})$ is equal to the valuation at ℓ of the conductor of the real multiplication $\mathcal{O}_0(\mathscr{A}) \subset \mathcal{O}_{K_0}$.*

Proof. Using the definition of $N_0(\mathscr{A})$ and the fact that $\beta/\ell^\epsilon \in \mathcal{O}(\mathscr{A})$ if and only if $\beta(\mathscr{A}[\ell^\epsilon]) = 0$, it follows that

$$\mathbb{Z}_\ell + \beta/\ell^{e-N_0(\mathscr{A})}\mathbb{Z}_\ell \subseteq \mathfrak{o}_0(\mathscr{A}) \subsetneq \mathbb{Z}_\ell + \beta/\ell^{e-N_0(\mathscr{A})+1}\mathbb{Z}_\ell.$$

Since all orders of $\mathcal{O}_{K_0}$ are of the form $\mathbb{Z} + c\mathcal{O}_{K_0}$ for some $c \in \mathbb{Z}_{>0}$, by localization at ℓ one sees that

$$\mathfrak{o}_0(\mathscr{A}) = \mathbb{Z}_\ell + \beta/\ell^{e-N_0(\mathscr{A})}\mathbb{Z}_\ell = \mathbb{Z}_\ell + \ell^{N_0(\mathscr{A})}\mathfrak{o}_0,$$

i.e., the valuation at ℓ of the conductor of $\mathcal{O}_0(\mathscr{A})$ is $N_0(\mathscr{A})$. □

The lemma proves the following algorithm works (i.e., that there always exists a neighbor decreasing the obstruction N_0):

Algorithm 1 Surfacing to maximal real endomorphism ring

```
Require: An abelian surface $\mathscr{A}/\mathbb{F}_q$ with endomorphism algebra $K = \mathrm{End}(\mathscr{A}) \otimes \mathbb{Q}$,
    and a prime number $\ell$.
Ensure: An isogenous abelian surface $\mathscr{A}'/\mathbb{F}_q$ with $\mathfrak{o}_0(\mathscr{A}') = \mathfrak{o}_0$.
 1: $\beta \leftarrow$ an element $\beta \in \mathbb{Z}[\pi, \overline{\pi}]$ such that $\{1, \beta/\ell^e\}$ is a $\mathbb{Z}_\ell$-basis for $\mathfrak{o}_0$.
 2: Compute $N_0(\mathscr{A}) := e - \max\{\epsilon \colon \beta(\mathscr{A}[\ell^\epsilon]) = 0\}$
 3: if $N_0(\mathscr{A}) = 0$ then
 4:     return $\mathscr{A}$
 5: end if
 6: $\mathcal{L} \leftarrow$ list of maximal isotropic $\kappa \subset \mathscr{A}[\ell]$ with $\kappa \cap \beta(\mathscr{A}[\ell^{e-N_0(\mathscr{A})+1}]) \neq \emptyset$
 7: for $\kappa \in \mathcal{L}$ do
 8:     Compute $N_0(\mathscr{A}/\kappa) := e - \max\{\epsilon \colon \beta((A/\kappa)[\ell^\epsilon]) = 0\}$
 9:     if $N_0(\mathscr{A}/\kappa, \epsilon) < N_0(\mathscr{A}, \epsilon)$ then
10:         $\mathscr{A} \leftarrow \mathscr{A}/\kappa$ and go to Step 3
11:     end if
12: end for
```

8.2.4. *Almost maximal order with (ℓ, ℓ)-isogenies.* For each prime ℓ, use the going-up algorithm (Algorithm 1), until $\mathcal{O}_0(\mathscr{A}) = \mathcal{O}_{K_0}$. Let ℓ be any prime and let $\mathfrak{l} \subset \mathcal{O}_{K_0}$ be a prime ideal above ℓ. Let $\mathfrak{o}_{0,\mathfrak{l}} = \mathcal{O}_{K_0,\mathfrak{l}}$ be the completion at $\mathfrak{l}$ of $\mathcal{O}_{K_0}$. Let $\mathfrak{o}_\mathfrak{l}(\mathscr{A}) = \mathcal{O}(\mathscr{A}) \otimes_{\mathcal{O}_{K_0}} \mathfrak{o}_{0,\mathfrak{l}}$. Consider the suborder $\mathfrak{o}_{0,\mathfrak{l}}[\pi, \pi^\dagger]$ of the maximal local (at $\mathfrak{l}$) order $\mathfrak{o}_\mathfrak{l} = \mathcal{O}_K \otimes_{\mathcal{O}_{K_0}} \mathfrak{o}_{0,\mathfrak{l}}$. Now write

$$\mathfrak{o}_{0,\mathfrak{l}}[\pi, \pi^\dagger] = \mathfrak{o}_{0,\mathfrak{l}} + \gamma_\mathfrak{l}\mathfrak{o}_{0,\mathfrak{l}}, \qquad \text{and} \qquad \mathfrak{o}_\mathfrak{l} = \mathfrak{o}_{0,\mathfrak{l}} + \gamma_\mathfrak{l}/\varpi^{f_\mathfrak{l}}\mathfrak{o}_{0,\mathfrak{l}},$$

for some endomorphism γ. Here, ϖ is a uniformizer for the local order $\mathfrak{o}_{0,\mathfrak{l}}$ and $f_\mathfrak{l} \geq 0$ is some integer. To define a similar obstruction to $N_0(\mathscr{A}, \epsilon)$, but at $\mathfrak{l}$, let

$$N_\mathfrak{l}(\mathscr{A}) = f_\mathfrak{l} - \max\{\delta \colon \gamma(\mathscr{A}[\mathfrak{l}^\delta]) = 0\}.$$

To compute these obstructions, we compute γ on the $\mathfrak{l}$-power torsion of $\mathscr{A}$. The idea is similar to Algorithm 1, except that in the split case, one must test the obstructions $N_{\mathfrak{l}}(\mathscr{A}, \epsilon)$ for both prime ideals $\mathfrak{l} \subset \mathcal{O}_{K_0}$ above ℓ at the same time. We now show that one can reach the maximal possible "reachable" (in the sense of Theorem 6) local order at ℓ starting from $\mathscr{A}$ and using only (ℓ, ℓ)-isogenies. When ℓ is either inert or ramified in K_0, there is only one obstruction $N_{\mathfrak{l}}(\mathscr{A})$, and one can ensure that it decreases at each step via the obvious modification of Algorithm 1.

Suppose now that $\ell\mathcal{O}_{K_0} = \mathfrak{l}_1\mathfrak{l}_2$ is split. Let $\mathfrak{f} = \mathfrak{l}_1^{i_1}\mathfrak{l}_2^{i_2}$ be the conductor of $\mathscr{A}$ and suppose, without loss of generality, that $i_1 \geq i_2$. To first ensure that one can reach an abelian surface $\mathscr{A}$ for which $0 \leq i_1 - i_2 \leq 1$, we relate the conductor $\mathfrak{f}$ to the two obstructions at $\mathfrak{l}_1$ and $\mathfrak{l}_2$.

Lemma 8.5. *Let $\mathscr{A}$ be an abelian surface with maximal local real endomorphism ring at ℓ and let $\mathfrak{o}(\mathscr{A}) = \mathfrak{o}_0 + \mathfrak{f}\mathfrak{o}_K$ where $\mathfrak{f}$ is the conductor. Then*

$$v_{\mathfrak{l}_1}(\mathfrak{f}) = N_{\mathfrak{l}_1}(\mathscr{A}) \qquad \textit{and} \qquad v_{\mathfrak{l}_2}(\mathfrak{f}) = N_{\mathfrak{l}_2}(\mathscr{A}).$$

Proof. The proof is the same as the one of Lemma 8.4. □

Using the lemma, and assuming $N_{\mathfrak{l}_1}(\mathscr{A}) - N_{\mathfrak{l}_2}(\mathscr{A}) > 1$, one repeatedly looks for an (ℓ, ℓ)-isogeny at each step that will decrease $N_{\mathfrak{l}_1}(\mathscr{A})$ by 1 and increase $N_{\mathfrak{l}_2}(\mathscr{A})$ by 1. Such an isogeny exists by Proposition 8.1(iii). One repeats this process until

$$0 \leq N_{\mathfrak{l}_1}(\mathscr{A}) - N_{\mathfrak{l}_2}(\mathscr{A}) \leq 1.$$

If at this stage $N_{\mathfrak{l}_2}(\mathscr{A}) > 0$, this means that $\ell \mid \mathfrak{f}$ and hence, by Proposition 8.1(i), there exists a unique (ℓ, ℓ)-isogeny decreasing both obstructions. One searches for that (ℓ, ℓ)-isogeny by testing whether the two obstructions decrease simultaneously, and repeats until $N_{\mathfrak{l}_2}(\mathscr{A}) = 0$.

If $N_{\mathfrak{l}_1}(\mathscr{A}) = 0$, then the maximal local order at ℓ has been reached. If $N_{\mathfrak{l}_1}(\mathscr{A}) = 1$ then Proposition 8.1(iii) implies that, if $\mathfrak{l}_2$ is not inert in K, then there exists an (ℓ, ℓ)-isogeny that decreases $N_{\mathfrak{l}_1}(\mathscr{A})$ to 0 and keeps $N_{\mathfrak{l}_2}(\mathscr{A})$ at zero.

8.2.5. *Final step via a cyclic isogeny.* In the exceptional cases of Theorem 6, it may happen that one needs to do an extra step via a cyclic isogeny to reach maximal local endomorphism ring at ℓ.

Whenever this cyclic $\mathfrak{l}$-isogeny is computable via the algorithm of [DJR16], one can always reach maximal local endomorphism ring at ℓ. But $\mathfrak{l}$-isogenies are computable if and only if $\mathfrak{l}$ is trivial in the narrow class group of K_0. We thus distinguish the following two cases:

(1) If $\mathfrak{l}$-isogenies are computable by [DJR16] then one can always reach maximal local endomorphism ring at ℓ.
(2) If $\mathfrak{l}$-isogenies are not computable by [DJR16], one can only use (ℓ, ℓ)-isogenies, so Theorem 6 tells us what the largest order that we can reach is.

Acknowledgements

The first and second authors were supported by the Swiss National Science Foundation. The third author was supported by the Swiss National Science Foundation under grant number 200021-156420.

References

[Bas63] H. Bass, *On the ubiquity of Gorenstein rings*, Mathematische Zeitschrift **82** (1963), no. 1, 8–28.

[BGL11] R. Bröker, D. Gruenewald, and K. Lauter, *Explicit CM theory for level 2-structures on abelian surfaces*, Algebra Number Theory **5** (2011), no. 4, 495–528.

[Bis15] G. Bisson, *Computing endomorphism rings of abelian varieties of dimension two*, Math. Comp. **84** (2015), no. 294, 1977–1989.

[BL94] J. Buchmann and H. W. Lenstra, *Approximating rings of integers in number fields*, J. Théor. Nombres Bordeaux **6** (1994), no. 2, 221–260. MR 1360644

[BL04] C. Birkenhake and H. Lange, *Complex abelian varieties*, Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen, Springer, 2004.

[BLS12] R. Bröker, K. Lauter, and A. Sutherland, *Modular polynomials via isogeny volcanoes*, Math. Comp. **81** (2012), no. 278, 1201–1231.

[CKL08] R. Carls, D. Kohel, and D. Lubicz, *Higher-dimensional 3-adic CM construction*, J. Algebra **319** (2008), no. 3, 971–1006.

[CL09] R. Carls and D. Lubicz, *A p-adic quasi-quadratic time point counting algorithm*, Int. Math. Res. Not. IMRN (2009), no. 4, 698–735.

[CQ05] G. Cardona and J. Quer, *Field of moduli and field of definition for curves of genus 2*, Computational aspects of algebraic curves, Lecture Notes Ser. Comput., vol. 13, World Sci. Publ., Hackensack, NJ, 2005, pp. 71–83.

[CR15] R. Cosset and D. Robert, *Computing (ℓ, ℓ)-isogenies in polynomial time on Jacobians of genus* 2 *curves*, Math. Comp. **84** (2015), no. 294, 1953–1975.

[CV04] C. Cornut and V. Vatsal, *Nontriviality of Rankin-Selberg L-functions and CM points*, Tech. report, 2004.

[DJR16] A. Dudeanu, D. Jetchev, and D. Robert, *Cyclic isogenies for abelian varieties with real multiplication*, preprint (2016).

[EL10] K. Eisenträger and K. Lauter, *A CRT algorithm for constructing genus 2 curves over finite fields*, Arithmetics, geometry, and coding theory (AGCT 2005), Sémin. Congr., vol. 21, Soc. Math. France, Paris, 2010, pp. 161–176.

[ES10] A. Enge and A. Sutherland, *Class invariants by the CRT method*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 6197, Springer, Berlin, 2010, pp. 142–156.

[FL08] D. Freeman and K. Lauter, *Computing endomorphism rings of Jacobians of genus 2 curves over finite fields*, Algebraic geometry and its applications, Ser. Number Theory Appl., vol. 5, World Sci. Publ., Hackensack, NJ, 2008, pp. 29–66.

[FM02] M. Fouquet and F. Morain, *Isogeny volcanoes and the SEA algorithm*, Algorithmic number theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 276–291.

[Gel75] Stephen S. Gelbart, *Automorphic forms on adèle groups*, Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1975, Annals of Mathematics Studies, No. 83. MR 0379375

[GHK$^+$06] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng, *The 2-adic CM method for genus 2 curves with application to cryptography*, Advances in cryptology—ASIACRYPT 2006, Lecture Notes in Comput. Sci., vol. 4284, Springer, Berlin, 2006, pp. 114–129.

[GL09] E. Goren and K. Lauter, *The distance between superspecial abelian varieties with real multiplication*, Journal of Number Theory **129** (2009), no. 6, 1562 – 1578.

[IT14] S. Ionica and E. Thomé, *Isogeny graphs with maximal real multiplication*, `https://arxiv.org/pdf/1407.6672v1.pdf` (accessed in Sept. 2016), 2014.

[JMV05] D. Jao, S. D. Miller, and R. Venkatesan, *Do all elliptic curves of the same order have the same difficulty of discrete log?*, Advances in cryptology—ASIACRYPT 2005, Lecture Notes in Comput. Sci., vol. 3788, Springer, Berlin, 2005, pp. 21–40.

[JMV09] ———, *Expander graphs based on GRH with an application to elliptic curve cryptography*, J. Number Theory **129** (2009), no. 6, 1491–1504.

[JW15] D. Jetchev and B. Wesolowski, *On graphs of isogenies of principally polarizable abelian surfaces and the discrete logarithm problem*, CoRR **abs/1506.00522** (2015).

[Koh96] D. Kohel, *Endomorphism rings of elliptic curves over finite fields*, ProQuest LLC, Ann Arbor, MI, 1996, Thesis (Ph.D.)–University of California, Berkeley.

[LR12a] K. Lauter and D. Robert, *Improved crt algorithm for class polynomials in genus 2*, IACR Cryptology ePrint Archive **2012** (2012), 443.

[LR12b] D. Lubicz and D. Robert, *Computing isogenies between abelian varieties*, Compos. Math. **148** (2012), no. 5, 1483–1515.

[Mes91] J.-F. Mestre, *Construction de courbes de genre* 2 *à partir de leurs modules*, Effective methods in algebraic geometry (Castiglioncello, 1990), Progr. Math., vol. 94, Birkhäuser Boston, Boston, MA, 1991, pp. 313–334.

[Mil86] J. S. Milne, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150. MR 861974

[Mum66] D. Mumford, *On the equations defining abelian varieties. I*, Invent. Math. **1** (1966), 287–354.

[NS99] J. Neukirch and N. Schappacher, *Algebraic number theory*, Grundlehren der mathematischen Wissenschaften, Springer, Berlin, New York, Barcelona, 1999.

[Rob10a] D. Robert, *Fonctions thêta et applications à la cryptologie*, PhD thesis, Université Henri Poincaré - Nancy I (2010).

[Rob10b] ———, *Theta functions and applications in cryptography*, Ph.D. thesis, Loria, Nancy, 2010.

[ST61] G. Shimura and Y. Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, Publications of the Mathematical Society of Japan, vol. 6, The Mathematical Society of Japan, Tokyo, 1961.

[Str10] Marco Streng, *Complex multiplication of abelian surfaces*, Ph.D. thesis, Universiteit Leiden, 2010.

[Sut11] A. Sutherland, *Computing Hilbert class polynomials with the Chinese remainder theorem*, Math. Comp. **80** (2011), no. 273, 501–538.

[Sut12] ———, *Accelerating the CM method*, LMS J. Comput. Math. **15** (2012), 172–204.

[Tat66] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Inventiones mathematicae **2** (1966), no. 2, 134–144.

[Vél71] J. Vélu, *Isogénies entre courbes elliptiques*, C. R. Acad. Sci. Paris Sér. A-B **273** (1971), A238–A241.

[vW99] P. van Wamelen, *Examples of genus two CM curves defined over the rationals*, Math. Comp. **68** (1999), no. 225, 307–320.

[Wat69] W. Waterhouse, *Abelian varieties over finite fields*, Annales scientifiques de l'École Normale Supérieure **2** (1969), no. 4, 521–560 (eng).

[Wen03] A. Weng, *Constructing hyperelliptic curves of genus 2 suitable for cryptography*, Math. Comp. **72** (2003), no. 241, 435–458 (electronic).

École Polytechnique Fédérale de Lausanne, EPFL SB MATHGEOM GR-JET, Switzerland
E-mail address: ernest.brooks@epfl.ch
E-mail address: dimitar.jetchev@epfl.ch

École Polytechnique Fédérale de Lausanne, EPFL IC LACAL, Switzerland
E-mail address: benjamin.wesolowski@epfl.ch