Abelian varieties over finite fields with commutative endomorphism algebra: theory and algorithms

Jonas Bergström, Valentijn Karemaker, Stefano Marseglia

Abelian varieties over finite fields with commutative endomorphism algebra: theory and algorithms

Jonas Bergström, Valentijn Karemaker, and Stefano Marseglia

Abstract

We give a categorical description of all abelian varieties with commutative endomorphism ring over a finite field with $q = p^a$ elements in a fixed isogeny class in terms of pairs consisting of a fractional $\mathbb{Z}[\pi, q/\pi]$-ideal and a fractional $W \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\pi, q/\pi]$-ideal, with π the Frobenius endomorphism and W the ring of integers in an unramified extension of $\mathbb{Q}_p$ of degree a. The latter ideal should be compatible at p with the former and stable under the action of a semilinear Frobenius (and Verschiebung) operator; it will be the Dieudonné module of the corresponding abelian variety. Using this categorical description we create effective algorithms to compute isomorphism classes of these objects and we produce many new examples exhibiting exotic patterns.

1 Introduction

In order to classify abelian varieties over a finite field up to isomorphism one needs a way to represent them. However, representing abelian varieties over fields of positive characteristic is notoriously hard, since describing them with equations becomes impractical already in dimension two. As a first step, one can consider the classification and representation problem up to isogeny; an isogeny is a surjective homomorphism with finite kernel. Over finite fields, this problem has been completely solved by Honda-Tate theory in terms of the characteristic polynomial of the Frobenius endomorphism of the abelian variety. The isogeny classes can also be computed effectively, see e.g. [8]. In this article we consider the representation and classification problem up to isomorphism for any fixed isogeny class of abelian varieties over finite fields with commutative endomorphism algebra.

To state our results we now introduce some notation. Fix a prime power $q = p^a$ and let π be the Frobenius endomorphism of an abelian variety X with commutative endomorphism algebra, defined over the finite field $\mathbb{F}_q$. Note that the condition of the endomorphism algebra being commutative is equivalent to the condition that the characteristic polynomial of the Frobenius endomorphism is square-free. Let $\mathcal{A}_\pi$ be the category of abelian varieties isogenous to X. Morphisms in this category will be homomorphisms defined over $\mathbb{F}_q$.

Main contribution

Put $R := \mathbb{Z}[\pi, q/\pi] \subseteq E := \mathbb{Q}[\pi]$. For any rational prime ℓ, including $\ell = p$, set $E_\ell = E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ and $R_\ell = R \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. Let L be an unramified extension of $\mathbb{Q}_p$ of degree a, with W its maximal $\mathbb{Z}_p$-order, and put $W_R = W \otimes_{\mathbb{Z}_p} R_p \subseteq A = L \otimes_{\mathbb{Q}_p} E_p$. The algebra A comes with an action of σ, the Frobenius map of L over $\mathbb{Q}_p$, and an embedding $\Delta : E_p \to A$. For more details on these definitions see Section 4.1. Fix an additive map F such that $F\lambda = \lambda^\sigma F$ for all $\lambda \in L$ and such that $F^a = \Delta(\pi)$. Put $V = pF^{-1}$. With a $W_R\{F, V\}$-ideal we will mean a fractional W_R-ideal in A which is stable under the action of F and V. Finally, for each ℓ, let i_ℓ be the injection $E \to E_\ell$.

Now let $\mathcal{C}_\pi$ be the category whose objects are pairs (I, M), where I is a fractional R-ideal in E and M is a $W_R\{F, V\}$-ideal such that $\Delta^{-1}(M) = i_p(I)R_p$. The homomorphisms between objects (I, M) and (J, N) in $\mathcal{C}_\pi$ are the elements $\alpha \in E$ such that $\alpha I \subseteq J$ and $\Delta(i_p(\alpha))M \subseteq N$.

Our first main result can now be stated as follows.

Theorem 5.2. There is an equivalence of categories $\Psi : \mathcal{C}_\pi \to \mathcal{A}_\pi$.

This result is closely related to [34, Theorem 2.1] and is based on Tate's theorem (see [31, Main theorem]). The idea goes back (at least) to Waterhouse [33, Theorem 5.1] and can loosely be stated as

follows (cf. [34, Theorem 2.1]): in a pair (I, M), the ideal M determines the Dieudonné module (which is equivalent to the p-divisible group) of the abelian variety. The ideal I encodes the Tate modules of the abelian variety for all $\ell \neq p$, partial information about the Dieudonné module, as well as "global information" which is determined by an element of the class group of the endomorphism ring of the abelian variety. Indeed, the endomorphism ring of the corresponding abelian variety is $\Delta^{-1}(\{x \in A : xM \subseteq M\})$ locally at p and $\{x \in E : xI \subseteq I\}$ locally at every other prime.

Comparison with previous results

There are several equivalence of categories in the literature that are similar to ours, some of which consider very large subcategories of the category of abelian varieties over a finite field $\mathbb{F}_q$. To more easily compare our results to these ones, in the rest of this section we will only discuss previous results on isogeny classes with commutative endomorphism algebra.

Recall that each Dieudonné module of an abelian variety over a finite field splits into three parts: the étale part, its 'dual' the multiplicative part, and the local-local part. The difficulty in realizing categorical equivalences can be measured by the exponent a of $q = p^a$ and the complexity of the local-local part. The p-rank of an abelian variety measures how large each of these parts is. For example, the p-rank is maximal (that is, it equals the dimension g of the variety) if the local-local part is trivial.

In [7], Deligne uses canonical liftings to represent *ordinary* (meaning of p-rank g) abelian varieties over a finite field in terms of fractional R-ideals. So in this case we have a close relation between abelian varieties over finite fields and CM-abelian varieties over the complex numbers (the canonical liftings).

In [3], this is extended by Centeleghe and Stix, in line with the techniques of Waterhouse rather than using canonical liftings, to represent all abelian varieties over a finite *prime* field (meaning of cardinality $q = p$) in terms of fractional R-ideals. The change of technique is connected to the fact that canonical liftings do not exist in general if the abelian variety is not ordinary nor almost ordinary (meaning of p-rank $g - 1$).

In the case of ordinary abelian varieties as well as the case of abelian varieties over prime fields, the Dieudonné module plays no special role and behaves in the same way as the Tate modules for $\ell \neq p$. We show, see Proposition 4.16, that the same always holds for the étale-local and local-étale parts of the Dieudonné module. The local-local part will behave quite differently as soon as we leave these realms.

An almost-ordinary abelian variety has a Dieudonné module with nonzero local-local part, whose endomorphism ring is maximal, see [24, Proposition 2.1]. If the place of E_p of slope $1/2$ (called the supersingular part) in an isogeny class of almost-ordinary abelian varieties is unramified, then there are two isomorphism classes of Dieudonné modules; in the ramified case there is one. In the ramified case, Oswal and Shankar in [24] use a canonical lifting to give a categorical equivalence between almost-ordinary abelian varieties and fractional S-ideals, where S is the minimal overorder of R that has maximal endomorphism ring at the supersingular part. In the unramified case, they use canonical liftings of different CM-types to distinguish between the two isomorphism classes of Dieudonné modules; this gives rise to two disjoint equivalences of such abelian varieties with fractional S-ideals.

In [2], Bhatnagar and Fu use the techniques of [24] to give a similar description for abelian varieties over finite fields with maximal real multiplication and such that p is split in the ring of integers of the maximal real extension. As in the almost-ordinary case, the endomorphism ring of the local-local part of the Dieudonné module of these abelian varieties is necessarily maximal, and [2, Theorem 1.3] can be compared with [33, Theorem 5.3].

Theorem 5.2 subsumes all of the above equivalences for the isogeny classes with commutative endomorphism algebra. In the almost-ordinary case, Theorem 5.2 also gives a description of morphisms between abelian varieties with non-isomorphic supersingular parts, which is not present in [24]. Moreover, Theorem 5.2 also works for almost-ordinary abelian varieties in characteristic 2, while the results in [24] do not.

In [4], Centeleghe and Stix give a categorical description of *all* abelian varieties over a finite field. Fix any abelian variety X that is isogenous to a square-free product of simple abelian varieties. Then there is a ring S_X such that the category of abelian varieties which are isogenous to a power of X is equivalent to the category of S_X-modules that are free and finite rank over $\mathbb{Z}$, cf. [4, Theorem 1.1]. The immediate issue if one would like to make an effective algorithm based on this equivalence – which is one of the main aims of this article – is that the ring S_X will in general be non-commutative. This is shown to be the case as soon as X is not ordinary nor defined over a prime field.

Finally, let us mention that there are other categorical descriptions of abelian varieties in the literature, such as [13], [14], [16] and [36].

Effectiveness of our result

The description given in Theorem 5.2 is amenable to concrete computations and the second main result of this article is that we have created effective algorithms to compute isomorphism classes of abelian varieties over a finite field with commutative endomorphism algebra. Our most important contribution here is Algorithm 3, which computes isomorphism classes of Dieudonné modules even when the endomorphism ring of the local-local part is not maximal. To our knowledge, this is the first algorithm that can compute isomorphism classes of Dieudonne modules with non-maximal endomorphism ring. To do so, we leverage the fact that the local-local parts of Dieudonné modules with maximal endomorphism ring have been classified by Waterhouse, see [33, Theorem 5.1]. Interestingly, in *all* isogeny classes of abelian varieties whose isomorphism classes we have computed, which are not defined over a prime field, nor ordinary, nor almost ordinary, it turns out that there are examples of isomorphism classes of abelian varieties with Dieudonné modules whose local-local part has a non-maximal endomorphism ring. The implementation of the code is available at https://github.com/stmar89/IsomClAbVarFqCommEndAlg[1].

The examples we compute in Section 8 show that the endomorphism rings that appear in a given isogeny class of abelian varieties (which are not defined over a prime field, nor ordinary, nor almost ordinary) behave quite wildly. To make this concrete, let $\mathcal{S}$ be the set of overorders of $R = \mathbb{Z}[\pi, q/\pi]$ and let $\mathcal{E}$ be the subset of $\mathcal{S}$ consisting of orders T such that there exists an abelian variety $X \in \mathcal{A}_\pi$ with $\mathrm{End}(X) = T$, and consider the following three statements which are true in the ordinary and almost-ordinary case, as well as over a prime field:

1. For every $S \in \mathcal{E}$ and $T \in \mathcal{S}$, if $S \subseteq T$ then $T \in \mathcal{E}$.
2. The order $S = \cap_{T \in \mathcal{E}} T$ is in $\mathcal{E}$.
3. For every S in $\mathcal{E}$, $n(\mathcal{O}_E)$ divides $n(S)$, where $n(S)$ (resp. $n(\mathcal{O}_E)$) is the number of isomorphism classes of abelian varieties in $\mathcal{A}_\pi$ with endomorphism ring S (resp. $\mathcal{O}_E$).

In Section 8, among other things, we give examples that violate all three of these statements. Our explicit knowledge of the Dieudonné modules also allows us to compute the a-numbers of the abelian varieties and study their distribution in the isogeny class.

Outline of the paper

In Section 2 we describe the isomorphism classes of abelian varieties over finite fields in a fixed isogeny class in terms of isomorphism classes of Tate and Dieudonné modules together with the class groups of the endomorphism ring they determine. From here on, we only consider abelian varieties with a commutative endomorphism ring.

The Tate modules of our abelian varieties can then be viewed as fractional R_ℓ-ideals for primes $\ell \neq p$. Even though these are local objects, we show in Section 3 how they can be described in terms of fractional ideals of some overorders of R (see Theorem 3.12), which are global objects. There are well-established algorithms to compute isomorphism classes of these types of ideals (see Algorithm 4).

Inspired by Waterhouse [33, Section 5], we show in Subsections 4.1 and 4.2 how to realize the Dieduonné modules of our abelian varieties as fractional $W_R\{F, V\}$-ideals. In Subsection 4.3 we then show a series of results about the structure of $W_R\{F, V\}$-ideals corresponding to the connected-étale sequence of Dieudonné modules. In particular, there is an étale part $R_p^{\{0\}}$ (resp. multiplicative part $R_p^{\{1\}}$) of R, and we show in Corollary 4.18 that the étale (resp. multiplicative) part of $W_R\{F, V\}$-ideals can be described as fractional $R_p^{\{0\}}$-ideals (respectively $R_p^{\{1\}}$-ideals).

The descriptions of Tate modules and Dieudonné modules in Sections 2–4 are put together in Section 5 to give a categorical equivalence between pairs of a fractional R-ideal and a fractional $W_R\{F, V\}$-ideal and abelian varieties in our fixed isogeny class, see Theorem 5.2, also stated above. In Proposition 5.7 and Corollary 5.8, we show some consequences of this equivalence for the possible endomorphism rings of our abelian varieties.

[1] The examples in this paper where computed using the code at commit c25be473adfeb1dba9932d47961e54649889fa78

In Section 6 we show how to create algorithms to compute isomorphism classes of $W_R\{F,V\}$-ideals. To avoid precision issues, we globalize our objects like in Section 3, considering fractional ideals in étale $\mathbb{Q}$-algebras rather than in étale $\mathbb{Q}_p$-algebras. Since Subsection 4.3.3 deals with the étale and multiplicative parts of the Dieudonné modules, we focus our attention on the local-local part. We extend Waterhouse's classification of isomorphism classes of $W_R\{F,V\}$-ideals with maximal endomorphism ring ([33, Theorem 5.1]) by describing the fibers of the extension map from (the local-local part of) W_R-ideals to ideals of the maximal order. Finally, we show that checking whether our ideals are stable under F and V can be done up to a power of the prime p, i.e., in a finite quotient; see Algorithm 3.

In Section 7 we use the categorical equivalence of Theorem 5.2 together with the results of the previous sections to create Algorithm 7, which computes isomorphism classes of abelian varieties in our fixed isogeny class. The representative we compute for each isomorphism class contains complete information about the Tate modules of the corresponding abelian variety for each $\ell \neq p$. Moreover, we get an approximation of F and V acting on the Dieudonné module modulo some power of p, which is sufficiently large to detect stability. This approximation can in principle be made arbitrarily accurate.

Finally, in Section 8, we give examples of computations of isomorphism classes of abelian varieties using our algorithms. In particular, we study the behavior of the endomorphism rings that appear for g-dimensional abelian varieties of p-rank $< g-1$, which shows patterns very different from abelian varieties with higher p-rank (that is, ordinary and almost-ordinary abelian varieties, as referred to above), see Examples 8.3, 8.4, 8.5, 8.6, 8.7 and 8.10.

At the end of the paper we collect a list of the notation used.

Contents

2 Tate and Dieudonné modules

Let X be an abelian variety over a finite field $\mathbb{F}_q$ of characteristic p. In this section we discuss a general description of the isogeny class of X over $\mathbb{F}_q$, as also contained in [34] (cf. [35]). Since we will focus on abelian varieties with commutative endomorphism algebra in this article, we will restrict to this case at the end of this section.

By Poincaré reducibility, the abelian variety X admits an isogeny decomposition $X \sim X_1^{k_1} \times \ldots \times X_r^{k_r}$ over $\mathbb{F}_q$ into simple abelian varieties X_i with respective multiplicities k_i. By Honda-Tate theory, the isogeny class of X is determined by the characteristic polynomial $h(x)$ of its Frobenius endomorphism. The isogeny decomposition of X implies that $h(x) = h_1(x)^{k_1} \cdot \ldots \cdot h_r(x)^{k_r} \in \mathbb{Z}[x]$, where each $h_i(x)$ is the characteristic polynomial of the Frobenius endomorphism π_i of X_i. Write $m(x) = m_1(x) \cdot \ldots \cdot m_r(x)$ and let $R = \mathbb{Z}[\pi, q/\pi]$ denote the $\mathbb{Z}$-order in the étale algebra $E = \mathbb{Q}[x]/(m(x))$ with $\pi := x \bmod m(x)$.

Set $\underline{k} = (k_1, \ldots, k_r)$. We denote by $\mathcal{A}_{\pi,\underline{k}}$ the category whose objects are the abelian varieties $\mathbb{F}_q$-isogenous to X together with $\mathbb{F}_q$-homomorphisms. We write $\mathcal{A}_{\pi,\underline{k}}^{\mathrm{isom}}$ for the set of $\mathbb{F}_q$-isomorphism classes in $\mathcal{A}_{\pi,\underline{k}}$. If $\underline{k} = (1, \ldots, 1)$, then the subscript $\underline{k}$ will be omitted from the notation.

All homomorphisms will be assumed to be defined over $\mathbb{F}_q$. Recall that the endomorphism ring $\mathrm{End}(X)$ is an order in the endomorphism algebra

$$\mathrm{End}^0(X) := \mathrm{End}(X) \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \mathrm{Mat}_{k_1}(\mathrm{End}_k^0(X_1)) \times \ldots \times \mathrm{Mat}_{k_r}(\mathrm{End}_k^0(X_r)). \tag{1}$$

Consider the group scheme G_X over $\mathbb{Z}$ such that

$$G_X(R_0) = (\mathrm{End}(X) \otimes_{\mathbb{Z}} R_0)^\times \tag{2}$$

for any commutative ring R_0 with unit.

For a rational prime $\ell \neq p$, let $T_\ell(X)$ be the ℓ-adic Tate module of X and set $V_\ell(X) = T_\ell(X) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. Let $M(X)$ be the covariant Dieudonné module of X (which is categorically equivalent to its p-divisible group). Put $R_\ell := R \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ for any prime ℓ, including $\ell = p$.

Definition 2.1. Out of the Tate and Dieudonné modules of X, we build

$$\begin{aligned}
\widetilde{\mathfrak{X}}_{\pi,\underline{k},\ell} &:= \{\text{left } R_\ell\text{-lattices in } V_\ell(X) \text{ of full rank}\} \text{ for all } \ell \neq p;\\
\prod_{\ell\neq p}{}' \widetilde{\mathfrak{X}}_{\pi,\underline{k},\ell} &:= \{(T_\ell)_{\ell\neq p} \in \prod_{\ell\neq p} \widetilde{\mathfrak{X}}_{\pi,\underline{k},\ell} : T_\ell = T_\ell(X) \text{ for all but finitely many } \ell \neq p\};\\
\widetilde{\mathfrak{X}}_{\pi,\underline{k},p} &:= \{\text{Dieudonné submodules in } M(X) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \text{ of full rank}\};\\
\widetilde{\mathfrak{X}}_{\pi,\underline{k}} &= \widetilde{\mathfrak{X}}_{\pi,\underline{k},p} \times \prod_{\ell\neq p}{}' \widetilde{\mathfrak{X}}_{\pi,\underline{k},\ell}.
\end{aligned}$$

As before, if $\underline{k} = (1, \ldots, 1)$ then it will be omitted from the notation.

By Tate's theorem, $\widetilde{\mathfrak{X}}_{\pi,\underline{k}}$ is in bijection with

$$\widetilde{\mathcal{A}}_{\pi,\underline{k}} := \{ \text{ quasi-isogenies } \varphi : X' \to X, \text{ up to isomorphism } \} \tag{3}$$

by mapping $(\varphi : X' \to X) \mapsto (\varphi_*(M(X')), (\varphi_*(T_\ell(X')))_{\ell\neq p})$; a quasi-isogeny $\varphi : X' \to X$ is an element of $\mathrm{Hom}(X', X) \otimes_{\mathbb{Z}} \mathbb{Q}$ such that there exists an integer N for which $N\varphi$ is an isogeny. This map $\widetilde{\mathcal{A}}_{\pi,\underline{k}} \to \widetilde{\mathfrak{X}}_{\pi,\underline{k}}$ is $G_X(\mathbb{A}_f)$-equivariant by construction, where $\mathbb{A}_f$ denotes the finite adele ring of $\mathbb{Q}$.

Further, we may project $\widetilde{\mathcal{A}}_{\pi,\underline{k}} \twoheadrightarrow \mathcal{A}_{\pi,\underline{k}}^{\mathrm{isom}}$ by mapping $(\varphi : X' \to X)$ to the isomorphism class of X'. Since two quasi-isogenies $\varphi_1 : X' \to X$ and $\varphi_2 : X'' \to X$ are considered isomorphic if there is an isomorphism $\alpha : X' \to X''$ such that $\varphi_2 \circ \alpha = \varphi_1$, this surjection can be viewed as taking the $G_X(\mathbb{Q})$-orbits of $\widetilde{\mathcal{A}}_{\pi,\underline{k}}$.

Definition 2.2. Starting with the objects in Definition 2.1, we let

$$\begin{aligned}
\mathfrak{X}_{\pi,\underline{k},\ell} &:= \widetilde{\mathfrak{X}}_{\pi,\underline{k},\ell} \text{ up to isomorphism of } R_\ell\text{-modules};\\
\mathfrak{X}_{\pi,\underline{k},p} &:= \widetilde{\mathfrak{X}}_{\pi,\underline{k},p} \text{ up to isomorphism of Dieudonné modules};\\
\mathfrak{X}_{\pi,\underline{k}} &:= \mathfrak{X}_{\pi,\underline{k},p} \times \prod_{\ell\neq p} \mathfrak{X}_{\pi,\underline{k},\ell}.
\end{aligned}$$

Thus we obtain a projection map $\widetilde{\mathfrak{X}}_{\pi,\underline{k}} \to \mathfrak{X}_{\pi,\underline{k}}$. Consider the fiber $\widetilde{\mathcal{A}}_{\pi,\underline{k},Y}$ in $\widetilde{\mathcal{A}}_{\pi,\underline{k}} \simeq \widetilde{\mathfrak{X}}_{\pi,\underline{k}}$ above an element $Y = (M/\simeq, (T_\ell)_{\ell\neq p}/\simeq)$ in $\mathfrak{X}_{\pi,\underline{k}}$. By definition, it consists of all isomorphism classes of quasi-isogenies $\varphi : X' \to X$ such that the Dieudonné and Tate modules of the source abelian varieties X' satisfy $M(X') \simeq M$ and $T_\ell(X') \simeq T_\ell$ for each $\ell \neq p$.

The group $G_X(\mathbb{A}_f)$ acts transitively on the set of quasi-isogenies on each fiber $\widetilde{\mathcal{A}}_{\pi,\underline{k},Y}$. The stabilizer of any given $\varphi : X' \to X$ in $\widetilde{\mathcal{A}}_{\pi,\underline{k},Y}$ under this action is the open compact subgroup

$$U_Y := \mathrm{Aut}(M) \times \prod_{\ell\neq p} \mathrm{Aut}_{R_\ell}(T_\ell) \tag{4}$$

of $G_X(\mathbb{A}_f)$. Hence, the fiber can be described as

$$\widetilde{\mathcal{A}}_{\pi,\underline{k},Y} \simeq G_X(\mathbb{A}_f)/U_Y. \tag{5}$$

For all $X' \in \mathcal{A}_{\pi,\underline{k}}$, we have that $\mathrm{End}(X)$ and $\mathrm{End}(X')$ are locally equal at all but finitely many rational primes. It follows that $G_{X'}(\mathbb{Q}) \simeq G_X(\mathbb{Q})$ and $G_{X'}(\mathbb{A}_f) \simeq G_X(\mathbb{A}_f)$ for all $X' \in \mathcal{A}_{\pi,\underline{k}}$, where $G_{X'}(R_0) = (\mathrm{End}(X') \otimes_{\mathbb{Z}} R_0)^\times$, cf. (2). In particular, we have

$$G_X(\mathbb{Q}) \simeq G_{X_1^{k_1}}(\mathbb{Q}) \times \ldots \times G_{X_r^{k_r}}(\mathbb{Q})$$

and

$$G_X(\mathbb{A}_f) \simeq G_{X_1^{k_1}}(\mathbb{A}_f) \times \ldots \times G_{X_r^{k_r}}(\mathbb{A}_f).$$

By contrast, in general, the same splitting does not apply to U_Y, since it is an integral object.

Finally, and similarly to $\widetilde{\mathcal{A}}_{\pi,\underline{k}} \to \widetilde{\mathfrak{X}}_{\pi,\underline{k}}$, we obtain a surjective map $\Phi : \mathcal{A}^{\mathrm{isom}}_{\pi,\underline{k}} \twoheadrightarrow \mathfrak{X}_{\pi,\underline{k}}$ by associating to an abelian variety the isomorphism classes of its Dieudonné and Tate modules. Recall that $\widetilde{\mathcal{A}}_{\pi,\underline{k}} \twoheadrightarrow \mathcal{A}^{\mathrm{isom}}_{\pi,\underline{k}}$ arises from taking $G_X(\mathbb{Q})$-orbits. It then follows from (5) and the commutative diagram

$$\begin{array}{ccc} \widetilde{\mathcal{A}}_{\pi,\underline{k}} & \xrightarrow{\sim} & \widetilde{\mathfrak{X}}_{\pi,\underline{k}} \\ \downarrow & & \downarrow \\ \mathcal{A}^{\mathrm{isom}}_{\pi,\underline{k}} & \xrightarrow{\Phi} & \mathfrak{X}_{\pi,\underline{k}} \end{array}$$

that the fiber $\mathcal{A}^{\mathrm{isom}}_{\pi,\underline{k},Y}$ above $Y \in \mathfrak{X}_\pi$ in $\mathcal{A}^{\mathrm{isom}}_{\pi,\underline{k}}$ satisfies

$$\mathcal{A}^{\mathrm{isom}}_{\pi,\underline{k},Y} \simeq G_X(\mathbb{Q})\backslash G_X(\mathbb{A}_f)/U_Y. \tag{6}$$

By construction, this fiber consists exactly of all isomorphism classes of abelian varieties in $\mathcal{A}^{\mathrm{isom}}_{\pi,\underline{k}}$ that are everywhere locally isomorphic, with Dieudonné and Tate modules given by the vector Y. Ranging over all local isomorphism types Y, we obtain the following result.

Proposition 2.3. (cf. [34, Theorem 2.1]) *The set of isomorphism classes $\mathcal{A}^{\mathrm{isom}}_{\pi,\underline{k}}$ of X can be described algebraically as*

$$\mathcal{A}^{\mathrm{isom}}_{\pi,\underline{k}} \simeq \bigsqcup_{Y\in\mathfrak{X}_{\pi,\underline{k}}} G_X(\mathbb{Q})\backslash G_X(\mathbb{A}_f)/U_Y; \tag{7}$$

here, the isomorphism class of X is sent to the neutral element.

Corollary 2.4. *The number of isomorphism classes of abelian varieties in $\mathcal{A}_{\pi,\underline{k}}$ equals*

$$|\mathcal{A}^{\mathrm{isom}}_{\pi,\underline{k}}| = \sum_{M\in\mathfrak{X}_{\pi,\underline{k},p}} \sum_{N\in\prod_{\ell\neq p}\mathfrak{X}_{\pi,\underline{k},\ell}} |G_X(\mathbb{Q})\backslash G_X(\mathbb{A}_f)/U_{M\times N}|,$$

where the sums run over the local isomorphism types $Y = M \times N \in \mathfrak{X}_{\pi,\underline{k},p} \times \prod_{\ell\neq p}\mathfrak{X}_{\pi,\underline{k},\ell} = \mathfrak{X}_{\pi,\underline{k}}$.

As mentioned above, in this article we will restrict our attention to abelian varieties with commutative endomorphism algebra. By [31, Theorem 2.(c)], this is equivalent to requiring h to be *square-free*, i.e. $k_i = 1$ for all i. From now on, we will therefore omit the multiplicities from the notation and simply

write $\mathcal{A}_\pi$, $\mathcal{A}_\pi^{\mathrm{isom}}$, $\mathfrak{X}_\pi$, $\mathfrak{X}_{\pi,p}$ and $\mathfrak{X}_{\pi,\ell}$. In particular, Equation (1) then reads $\mathrm{End}^0(X) \simeq \mathrm{End}^0(X_1) \times \ldots \times \mathrm{End}^0(X_r)$. Furthermore, the fiber above $Y = M \times N$, given as in (6), then equals the (usual) class group $\mathrm{Cl}(\mathcal{O}_Y)$, where

$$\mathcal{O}_Y = \mathrm{End}^0(X) \cap \left(\mathrm{End}(M) \times \prod_{\ell \neq p} \mathrm{End}_{R_\ell}(T_\ell) \right); \tag{8}$$

this intersection takes place in $\mathrm{End}^0(X) \otimes_{\mathbb{Q}} \mathbb{A}_f$. This also implies that its cardinality is the (usual) class number $h(\mathcal{O}_Y)$. We summarize this discussion in the following corollary.

Corollary 2.5. *The number of isomorphism classes of abelian varieties with commutative endomorphism algebra in $\mathcal{A}_\pi$ equals*

$$|\mathcal{A}_\pi^{\mathrm{isom}}| = \sum_{M \in \mathfrak{X}_{\pi,p}} \sum_{N \in \prod_{\ell \neq p} \mathfrak{X}_{\pi,\ell}} h(\mathcal{O}_{M \times N}).$$

3 Global representatives of Tate modules

In Section 2 we realized the Tate modules of abelian varieties as R_ℓ-ideals. In this section we will find global representatives of these local fractional ideals, namely, as certain fractional R-ideals, see Theorem 3.12. In Section 7, this will provide an effective method to compute (recalling Definition 2.2) representatives of $\prod_{\ell \neq p} \mathfrak{X}_{\pi,\ell}$, see Algorithm 4. Even though $\prod_{\ell \neq p} \mathfrak{X}_{\pi,\ell}$ is local in nature, Algorithm 4 only uses exact techniques which are not affected by precision issues. We will also use the results of this section to compute isomorphism classes of fractional ideals of a $\mathbb{Z}_p$-order; see Subsection 6.2.

3.1 Isomorphism classes of fractional ideals

Let Z be either $\mathbb{Z}$ or $\mathbb{Z}_p$, and let Q be the field of fractions of Z. Let S be a Z-order in an étale Q-algebra E with maximal order $\mathcal{O}$. For a fractional S-ideal I, the multiplicator ring $(I : I)$ is an order. For a maximal ideal ℓ in Z, set $E_\ell = E \otimes_Q Q_\ell$, $S_\ell = S \otimes_Z Z_\ell$, and $I_\ell = I \otimes_Z Z_\ell$. Let $\mathfrak{l}$ be a maximal ideal of S. Denote by $S_\mathfrak{l}$ the completion of S at $\mathfrak{l}$. Set $I_\mathfrak{l} = I \otimes_S S_\mathfrak{l}$.

Definition 3.1. Let $\mathcal{S}$ be a (possibly infinite) set of maximal ideals ℓ of Z, and $\mathcal{T}$ be a (possibly infinite) set of maximal ideals $\mathfrak{l}$ of S. We define the following objects:

$$\begin{aligned}
\mathcal{W}_\ell(S) &= \frac{\{\text{fractional } S\text{-ideals}\}}{\{I_\ell \simeq J_\ell \text{ as } S_\ell\text{-modules}\}},\\
\mathcal{W}_\mathfrak{l}(S) &= \frac{\{\text{fractional } S\text{-ideals}\}}{\{I_\mathfrak{l} \simeq J_\mathfrak{l} \text{ as } S_\mathfrak{l}\text{-modules}\}},\\
\mathcal{W}(S) &= \frac{\{\text{fractional } S\text{-ideals}\}}{\{I_\ell \simeq J_\ell \text{ as } S_\ell\text{-modules, for every } \ell\}},\\
\mathcal{W}_\mathcal{S}(S) &= \frac{\{\text{fractional } S\text{-ideals}\}}{\{I_\ell \simeq J_\ell \text{ as } S_\ell\text{-modules, for every } \ell \in \mathcal{S}\}},\\
\mathcal{W}_\mathcal{T}(S) &= \frac{\{\text{fractional } S\text{-ideals}\}}{\{I_\mathfrak{l} \simeq J_\mathfrak{l} \text{ as } S_\mathfrak{l}\text{-modules, for every } \mathfrak{l} \in \mathcal{T}\}}.
\end{aligned}$$

We denote the class of a fractional S-ideal I in $\mathcal{W}_\ell(S)$ (resp. $\mathcal{W}_\mathfrak{l}(S)$, $\mathcal{W}(S)$, $\mathcal{W}_\mathcal{S}(S)$, $\mathcal{W}_\mathcal{T}(S)$) by $[I]_\ell$ (resp. $[I]_\mathfrak{l}$, $[I]$, $[I]_\mathcal{S}$, $[I]_\mathcal{T}$).

This subsection will be devoted to studying the relations between the objects defined in Definition 3.1, which are local in nature, and to giving a concrete description of them by means of global representatives.

Remark 3.2. If $Z = \mathbb{Z}_p$ then $\mathcal{W}(S)$ coincides with the set of S-linear isomorphism classes of fractional S-ideals.

Remark 3.3. Ideal multiplication endows each set defined in Definition 3.1 with a commutative monoid structure, whose unit is given by the class of the order S. This structure will not be used in this article. The class $[I]$ of I in $\mathcal{W}(S)$ is often called the genus of I. There is a vast literature studying genera of

fractional ideals and more generally of finitely generated modules. See for example [27], [26], [10], [11] and [25]. Moreover, two fractional S-ideals I and J are in the same genus if and only if they are weakly equivalent, that is, their localizations at every maximal ideal of S are isomorphic, see [18, Section 5]. The definition of weak equivalence was originally given in [6]. Results to compute and classify weak equivalence classes are given in [20], [22] and [23].

Lemma 3.4. *Let I and J be two fractional S-ideals and fix a maximal ideal ℓ of Z. Then the following statements are equivalent:*

(i) $[I]_\ell = [J]_\ell$.

(ii) $I_\mathfrak{l} \simeq J_\mathfrak{l}$ *as* $S_\mathfrak{l}$*-modules for every maximal ideal* $\mathfrak{l}$ *of* S *above* ℓ.

Proof. Denote by $\mathfrak{l}_1, \ldots, \mathfrak{l}_n$ the maximal ideals of S above ℓ. Since S_ℓ is a complete semilocal ring, we have a canonical isomorphism

$$S_\ell \simeq S_{\mathfrak{l}_1} \times \ldots \times S_{\mathfrak{l}_n}.$$

Tensoring with I and J, we obtain the equivalence of (i) and (ii). □

Lemma 3.5. *Let $\mathfrak{l}$ be a maximal ideal of S above the maximal ideal ℓ of Z.*

(i) For every fractional S_ℓ-ideal I there exists a fractional S-ideal $\widetilde{I}$ such that $\widetilde{I} \otimes_Z Z_\ell = I$. The class $[\widetilde{I}]_\ell$ in $\mathcal{W}_\ell(S)$ is uniquely determined by the class $[I]_\ell$ in $\mathcal{W}(S_\ell)$. Hence, we have a canonical bijection $\mathcal{W}_\ell(S) \longleftrightarrow \mathcal{W}(S_\ell)$.

(ii) Similarly, we have a canonical bijection $\mathcal{W}_\mathfrak{l}(S) \longleftrightarrow \mathcal{W}(S_\mathfrak{l})$.

Proof. Identify E with its image in E_ℓ. Then $\widetilde{I} = I \cap E$ satisfies $\widetilde{I} \otimes_Z Z_\ell = I$. Morever, we see that if J is a second fractional S_ℓ-ideal, then $[I] = [J]$ if and only if $[\widetilde{I}]_\ell = [\widetilde{J}]_\ell$. This completes the proof of (i). For (ii), assume that $\mathfrak{l} = \mathfrak{l}_1, \ldots, \mathfrak{l}_n$ are the maximal ideals of S above ℓ and that we are given a fractional $S_\mathfrak{l}$-ideal I. Consider the fractional S_ℓ-ideal $I' = I \times S_{\mathfrak{l}_2} \times \ldots S_{\mathfrak{l}_n}$ and the fractional S-ideal $\widetilde{I}$ such that $\widetilde{I} \otimes_Z Z_\ell = I'$. We get that $(\widetilde{I})_\mathfrak{l} = I$ and that the class of $\widetilde{I}$ in $\mathcal{W}_\mathfrak{l}(S)$ is uniquely determined by the class of I in $\mathcal{W}(S_\mathfrak{l})$. □

Given a set $\mathcal{S}$ as above, denote by $\mathcal{S}_0$ the finite subset of $\mathcal{S}$ consisting of maximal ideals of Z dividing the index $[\mathcal{O} : S]$. Define $\mathcal{W}_{\mathcal{S}_0}(S)$ and $[I]_{\mathcal{S}_0}$ analogously to $\mathcal{W}_\mathcal{S}(S)$ and $[I]_\mathcal{S}$. Similarly, given a set $\mathcal{T}$ as above, denote by $\mathcal{T}_0$ the finite subset of $\mathcal{T}$ consisting of maximal ideals of S containing the conductor $\mathfrak{f} = (S : \mathcal{O})$ of S. Define $\mathcal{W}_{\mathcal{T}_0}(S)$ and $[I]_{\mathcal{T}_0}$ analogously.

Proposition 3.6. *Consider the natural surjections*

$$\mathcal{W}(S) \xrightarrow{i_1} \mathcal{W}_\mathcal{S}(S) \xrightarrow{i_2} \mathcal{W}_{\mathcal{S}_0}(S)$$

and

$$\mathcal{W}(S) \xrightarrow{j_1} \mathcal{W}_\mathcal{T}(S) \xrightarrow{j_2} \mathcal{W}_{\mathcal{T}_0}(S).$$

Then i_2 and j_2 are bijections. Moreover, i_1 is a bijection if and only if $\mathcal{S}$ contains all maximal ideals above the index $[\mathcal{O} : S]$, and j_1 is a bijection if and only if $\mathcal{T}$ contains all maximal ideals above the conductor $\mathfrak{f}$ of S.

Proof. A maximal ideal ℓ does not divide the index $[\mathcal{O} : S]$ if and only if $S_\ell = \mathcal{O}_\ell$. For such a prime ℓ, every fractional S-ideal I satisfies $I_\ell \simeq \mathcal{O}_\ell$, since $\mathcal{O}_\ell$ is a principal ideal ring. This immediately implies the statements about i_1 and i_2. The statements about j_1 and j_2 follow analogously from the observation that a maximal ideal $\mathfrak{l}$ of S does not divide the conductor $\mathfrak{f}$ of S if and only if $S_\mathfrak{l} = \mathcal{O}_\mathfrak{l}$. □

The construction described in the following lemma will also be used in Algorithms 1 and 5.

Lemma 3.7. *Let $\mathfrak{l}_1, \ldots, \mathfrak{l}_n$ be maximal ideals of S. Consider a vector of fractional S-ideals $(I_1, \ldots, I_n)$ such that each I_i is contained in S. For each i, let k_i be a nonnegative integer such that $\mathfrak{l}_i^{k_i} S_{\mathfrak{l}_i} \subseteq (I_i)_{\mathfrak{l}_i}$. Set*

$$J = \sum_{i=1}^{n} \left((I_i + \mathfrak{l}_i^{k_i}) \prod_{j \neq i} \mathfrak{l}_j^{k_j} \right).$$

Then $J_{\mathfrak{l}_i} = (I_i)_{\mathfrak{l}_i}$ for each i, and $J_\mathfrak{l} = S_\mathfrak{l}$ for every other maximal ideal $\mathfrak{l}$ of S.

Proof. See the proof of [23, Theorem 4.4]. □

Proposition 3.8. *The natural maps*

$$\mathcal{W}_{\mathcal{S}_0}(S) \longrightarrow \prod_{\ell \in \mathcal{S}_0} \mathcal{W}_\ell(S)$$

and

$$\mathcal{W}_{\mathcal{T}_0}(S) \longrightarrow \prod_{\mathfrak{l} \in \mathcal{T}_0} \mathcal{W}_\mathfrak{l}(S),$$

are bijections.

Proof. The maps are injective by construction. Surjectivity follows from Lemma 3.7. □

Proposition 3.9. *Let ℓ be a maximal ideal of Z and let $\mathfrak{l}_1, \ldots, \mathfrak{l}_n$ be the maximal ideals of S above ℓ and above the conductor $\mathfrak{f} = (S : \mathcal{O})$. We have a natural bijection*

$$\varphi : \mathcal{W}_\ell(S) \longrightarrow \prod_{i=1}^{n} \mathcal{W}_{\mathfrak{l}_i}(S).$$

Proof. As pointed out above, if $\mathfrak{l}$ is a maximal ideal of S which does not divide the conductor, then $S_\mathfrak{l} = \mathcal{O}_\mathfrak{l}$, which is a principal ideal ring. Hence, for every fractional S-ideal I, we have $I_\mathfrak{l} \simeq \mathcal{O}_\mathfrak{l}$, or equivalently, $\mathcal{W}_\mathfrak{l}(S)$ is trivial. Therefore φ is injective by Lemma 3.4. Surjectivity follows from Lemma 3.7. □

The next proposition is [23, Proposition 4.3].

Proposition 3.10. *Let $\mathfrak{l}$ be a maximal ideal of S. Let k be a nonnegative integer such that $(\mathfrak{l}^k\mathcal{O})_\mathfrak{l} \subseteq S_\mathfrak{l}$. Then the natural map*

$$\mathcal{W}(S + \mathfrak{l}^k\mathcal{O}) \longrightarrow \mathcal{W}_\mathfrak{l}(S)$$

is a bijection.

Remark 3.11. In the statement of Proposition 3.10, we can take $k = \mathrm{val}_\ell([\mathcal{O} : S])$ to achieve $(\mathfrak{l}^k\mathcal{O})_\mathfrak{l} \subseteq S_\mathfrak{l}$, where v_ℓ denotes the ℓ-adic valuation. Note also that if $(\mathfrak{l}^k\mathcal{O})_\mathfrak{l} \subseteq S_\mathfrak{l}$ and $k' > k$ then $S + \mathfrak{l}^k\mathcal{O} = S + \mathfrak{l}^{k'}\mathcal{O}$.

3.2 Determining $\prod_{\ell \neq p} \mathfrak{X}_{\pi,\ell}$

As in Section 2, we consider an isogeny class $\mathcal{A}_\pi$ of abelian varieties over $\mathbb{F}_q$, where $q = p^a$ for some prime p, with commutative endomorphism algebra $E = \mathbb{Q}[\pi]$. We now use the results of the previous subsection to give a concrete description of the set $\prod_{\ell \neq p} \mathfrak{X}_{\pi,\ell}$.

Theorem 3.12. *Set $R = \mathbb{Z}[\pi, q/\pi]$.*

(i) For each $\ell \neq p$, localization at ℓ induces a bijection

$$\mathcal{W}_\ell(R) \longrightarrow \mathfrak{X}_{\pi,\ell}.$$

(ii) Denote by $\mathfrak{l}_1, \ldots, \mathfrak{l}_n$ the maximal ideals of R which divide the conductor $(R : \mathcal{O})$ and do not contain p. For each i, let k_i be a nonnegative integer such that $(\mathfrak{l}_i^{k_i}\mathcal{O})_{\mathfrak{l}_i} \subseteq R_{\mathfrak{l}_i}$. Then we have a bijection

$$\prod_{i=1}^{n} \mathcal{W}(R + \mathfrak{l}_i^{k_i}\mathcal{O}) \longrightarrow \prod_{\ell \neq p} \mathfrak{X}_{\pi,\ell}.$$

Proof. Fix a prime $\ell \neq p$ and an abelian variety $X \in \mathcal{A}_\pi$. After identifying $V_\ell(X) = T_\ell(X) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ with $E_\ell = \mathbb{Q}[\pi]_\ell$ we see that

$$\mathfrak{X}_{\pi,\ell} = \{\text{fractional } R_\ell\text{-ideals in } E_\ell \text{ up to isomorphism as } R_\ell\text{-modules}\}.$$

Hence, localization at ℓ induces a natural injective map

$$\mathcal{W}_\ell(R) \longrightarrow \mathfrak{X}_{\pi,\ell}.$$

Surjectivity follows from the fact that every fractional R_ℓ-ideal J is of the form $J = I \otimes_R R_\ell$ for some fractional R-ideal I, cf. Lemma 3.5.(i). This completes the proof of (i).

Combining Propositions 3.6 (applied with $\mathcal{S}$ consisting of all rational primes $\ell \neq p$), 3.9, and 3.10, we see that there is a natural bijection from $\prod_{i=1}^{n} \mathcal{W}(R + \mathfrak{l}_i^{k_i}\mathcal{O})$ to $\prod_{\ell \neq p} \mathcal{W}_\ell(R)$. By applying (i) for each $\ell \neq p$, we obtain (ii). □

4 Dieudonné modules and where to find them

In Subsections 4.1 and 4.2 we will find representatives of Dieudonné modules as certain fractional $W_R(:= W \otimes_{\mathbb{Z}_p} R_p)$-ideals in $A = L \otimes_{\mathbb{Q}_p} E_p$, where W is the maximal order in an unramifed extension L of $\mathbb{Q}_p$ of degree a. These fractional ideals should be stable under operators $F : A \to A$ and $V = pF^{-1}$, where F has the Frobenius property, see Definition 4.1; they are called $W_R\{F, V\}$-ideals. Maps between $W_R\{F, V\}$-ideals will be given by elements from E_p via the diagonal embedding $\Delta : E_p \to A$, see Lemma 4.6. Theorem 4.9 gives a bijection between isomorphism classes of Dieudonné modules and Δ-isomorphism classes of $W_R\{F, V\}$-ideals.

In Subsection 4.3.1, we study an analogue for $W_R\{F, V\}$-ideals of the connected-étale sequence, which gives a decomposition of any $W_R\{F, V\}$-ideal into an étale part, a multiplicative part and a local-local part. The étale and multiplicative parts are studied in Subsection 4.3.3. A classification due to Waterhouse of all possible local-local parts with maximal endomorphism ring is given in Subsection 4.3.4.

Later, in Section 6 we will create an effective algorithm to find global representatives of Δ-isomorphism classes of $W_R\{F, V\}$-ideals.

4.1 The Frobenius property

Firstly, we introduce some notation, closely following that of Waterhouse [33, Section 5]. Let $q = p^a$ again be a power of a prime p. We consider an isogeny class $\mathcal{A}_\pi$ of abelian varieties over $\mathbb{F}_q$ with commutative endomorphism algebra $E = \mathbb{Q}[\pi]$, or equivalently, of abelian varieties such that the characteristic polynomial of their Frobenius endomorphism π is square-free. Let R be the order of E generated by the Frobenius and Verschiebung endomorphisms, that is, $R = \mathbb{Z}[\pi, q/\pi]$.

We are interested in the completions $E_p = E \otimes_{\mathbb{Q}} \mathbb{Q}_p$ of E, and $R_p = R \otimes_{\mathbb{Z}} \mathbb{Z}_p \subseteq E_p$ of R, at the rational prime p. For each place ν of E_p, let e_ν denote the ramification index and f_ν the inertia degree of E_ν over $\mathbb{Q}_p$. Also let $n_\nu = e_\nu f_\nu = [E_\nu : \mathbb{Q}_p]$ and denote by π_ν the image of π in E_ν. Note that $E_p = \prod_{\nu|p} E_\nu$.

Let L be the totally unramified extension of $\mathbb{Q}_p$ of degree a and let $W = \mathcal{O}_L$ be the maximal $\mathbb{Z}_p$-order of L. We know that $L = \mathbb{Q}_p(\zeta_{q-1})$ and $W = \mathbb{Z}_p[\zeta_{q-1}]$, where ζ_{q-1} is a primitive $(q-1)$-st root of unity.

Observe that $L \otimes_{\mathbb{Q}_p} E_p$ is an etalé $\mathbb{Q}_p$-algebra, that is, it is isomorphic to a direct sum of finitely many finite extensions of $\mathbb{Q}_p$. Indeed,

$$L \otimes_{\mathbb{Q}_p} E_p \simeq \prod_{\nu|p} \left(\underbrace{LE_\nu \times \ldots \times LE_\nu}_{g_\nu \text{ copies}} \right) =: A, \tag{9}$$

where $g_\nu = \gcd(a, f_\nu)$. Denote the ν-component of A by A_ν. For an element $b = (b_\nu)_{\nu|p}$ of $A = \prod_\nu A_\nu$ we denote by $b_{\nu,i}$ the i-th component of b_ν in $A_\nu = \prod_{j=1}^{g_\nu} LE_\nu$. Wee see E_ν embeds diagonally into A_ν for each ν. Hence we have an induced embedding

$$\Delta : E_p \hookrightarrow A,$$

which endows A with an E_p-algebra structure.

The isomorphism in Equation (9) restricted to a component A_ν is given on simple tensors $\omega \otimes \beta \in L \otimes_{\mathbb{Q}_p} E_p$ by

$$\omega \otimes \beta \mapsto (\omega\beta_\nu, \omega^\sigma \beta_\nu, \ldots, \omega^{\sigma^{g_\nu - 1}} \beta_\nu), \tag{10}$$

where σ is the Frobenius of L over $\mathbb{Q}_p$. This means that A has an L-algebra structure, and the image of $\lambda \in L$ in each A_ν equals

$$(\lambda, \lambda^\sigma, \ldots, \lambda^{\sigma^{g_\nu - 1}}).$$

We also have an action of σ on A_ν via

$$(\omega\beta_\nu, \omega^\sigma \beta_\nu, \ldots, \omega^{\sigma^{g_\nu - 1}} \beta_\nu) \mapsto (\omega^\sigma \beta_\nu, \omega^{\sigma^2} \beta_\nu, \ldots, \omega^{\sigma^{g_\nu}} \beta_\nu). \tag{11}$$

Since $\omega^{\sigma^{g_\nu}} \beta_\nu = (\omega\beta_\nu)^{\tau_\nu}$, where τ_ν is the Frobenius of LE_ν over E_ν, we see that σ acts on each A_ν as a cyclic permutation followed by τ_ν in the last component. By slight abuse of notation, we will denote the maps induced by σ on A_ν and A also by σ.

Definition 4.1. A map $F_\nu : A_\nu \to A_\nu$ will be said to have the *Frobenius property* if it is additive and satisfies $F_\nu \lambda = \lambda^\sigma F_\nu$ for all $\lambda \in L$ and $F_\nu^a = \Delta|_{E_\nu}(\pi_\nu) \in A_\nu$.

Given a set $\mathcal{S}$ of places ν of E_p, a map $F : \prod_{\nu\in\mathcal{S}} A_\nu \to A_\nu$ will be said to have the Frobenius property if $F|_{A_\nu}$ has the Frobenius property for all places ν of E_p.

Lemma 4.2. *For every $\alpha_\nu = (\alpha_{\nu,1}, \dots, \alpha_{\nu,g_\nu}) \in A_\nu$ we have*

$$\alpha_\nu \cdot \alpha_\nu^\sigma \cdots \alpha_\nu^{\sigma^{a-1}} = (\beta_\nu, \dots, \beta_\nu) \in A_\nu,$$

where

$$\beta_\nu = N_{LE_\nu/E_\nu}(\alpha_{\nu,1} \cdots \alpha_{\nu,g_\nu}) \in E_\nu.$$

Proof. For ease of notation, set $g = g_\nu$ and $N = N_{LE_\nu/E_\nu}$, and write $\tau = \tau_\nu$ for the Frobenius of LE_ν over E_ν. As above, we see τ has order a/g and satisfies $\sigma^g(\alpha) = (\tau(\alpha_1), \dots, \tau(\alpha_g))$. For each $0 \le k \le a/g - 1$ and each $0 \le i \le g-1$, we have

$$\sigma^{kg+i}(\alpha) = (\tau^k(\alpha_{i+1}), \dots, \tau^k(\alpha_g), \tau^{k+1}(\alpha_1), \dots, \tau^{k+1}(\alpha_i)).$$

Hence

$$\begin{aligned}
\alpha \cdot \sigma(\alpha) \cdots \sigma^{a-1}(\alpha) &= \prod_{k=0}^{\frac{a}{g}-1} \prod_{i=0}^{g-1} \sigma^{kg+i}(\alpha) \\
&= \prod_{i=0}^{g-1} \left(\prod_{k=0}^{\frac{a}{g}-1} \tau^k(\alpha_{i+1}), \dots, \prod_{k=0}^{\frac{a}{g}-1} \tau^k(\alpha_g), \prod_{k=0}^{\frac{a}{g}-1} \tau^{k+1}(\alpha_1), \dots, \prod_{k=0}^{\frac{a}{g}-1} \tau^{k+1}(\alpha_i) \right) \\
&= \prod_{i=0}^{g-1} (N(\alpha_{i+1}), \dots, N(\alpha_g), N(\alpha_1), \dots, N(\alpha_i)) \\
&= (N(\alpha_1 \cdots \alpha_g), \dots, N(\alpha_1 \cdots \alpha_g)),
\end{aligned}$$

as required. □

Lemma 4.3. *Let $\alpha_\nu \in A_\nu$ be such that*

$$\alpha_\nu \cdot \alpha_\nu^\sigma \cdots \alpha_\nu^{\sigma^{a-1}} = (\pi_\nu, \dots, \pi_\nu) \in A_\nu. \qquad (*)$$

For $z \in A_\nu$, define $F_\nu(z) = \alpha_\nu \cdot z^\sigma$, i.e. $F_\nu = \alpha_\nu \circ \sigma$, and extend this component-wise to obtain a map F on A. Then F has the Frobenius property.

Proof. It is enough to check the desired properties on each component A_ν. Rather than doing so using the isomorphism given by Equation (10), we use a different presentation of A_ν. Namely, let $h_\nu(x)$ be the minimal polynomial of π_ν over $\mathbb{Q}_p$ and write

$$h_\nu(x) = f_1(x) \cdots f_r(x)$$

for its factorization into irreducible factors over $L[x]$. Then we have an L-algebra isomorphism

$$\varphi : A_\nu \xrightarrow{\sim} \prod_{i=1}^{r} \frac{L[x]}{f_i(x)}.$$

The action of σ on A_ν in this presentation is induced by the automorphism of $L[x]$ sending $s(x) = \sum_k a_k x^k$ to $s(x)^\sigma = \sum_k a_i^\sigma x^k$.

For $z \in A_\nu$, we have $\varphi(z) = ([s_{z,1}(x)], \dots, [s_{z,r}(x)])$ for some $s_{z,i}(x) \in L[x]$, where $[s_{z,i}(x)]$ denotes the class of $s_{z,i}(x)$ in the quotient $L[x]/f_i(x)$. For any $\lambda \in L$,

$$\varphi(F_\nu(\lambda z)) = ([s_{\alpha_\nu,i}(x) s_{(\lambda z)^\sigma,i}(x)], \dots) = ([\lambda^\sigma s_{\alpha_\nu,i}(x) s_{z,i}(x)^\sigma], \dots) = \varphi(\lambda^\sigma F_\nu(z)),$$

which shows that $F_\nu \lambda = \lambda^\sigma F_\nu$, as required. Finally, we have by construction that

$$s_{\alpha_\nu,i}(x) \cdot s_{\alpha_\nu,i}(x)^\sigma \cdots s_{\alpha_\nu,i}(x)^{\sigma^{a-1}} s_{z,i}(x) - x \in (f_i(x)),$$

for $i = 1, \dots, r$. This shows that $\varphi(F_\nu^a) = \varphi(\pi_\nu)$, completing the proof. □

In [33, p. 544] there is the following construction of an element $\alpha_\nu \in A_\nu$ enjoying property $(*)$ of Lemma 4.3: Since the degree a/g_ν of the unramified extension LE_ν/E_ν divides the ν-adic valuation $\mathrm{val}_\nu(\pi_\nu)$, it follows that π_ν is the norm of an element $u_\nu \in LE_\nu$. We can then put $\alpha_\nu = (1, 1, \ldots, 1, u_\nu) \in A_\nu$. The following definition will reappear later in Proposition 4.19 and in Algorithm 3.

Definition 4.4. If $F_\nu : A_\nu \to A_\nu$ is a map with the Frobenius property defined by $F_\nu(z) = \alpha_\nu \cdot z^\sigma$ for an element $\alpha_\nu = (1, 1, \ldots, 1, u_\nu) \in A_\nu$ then we will say that F_ν is of *W-type*.

Given a set $\mathcal{S}$ of places ν of E_p, a map $F : \prod_{\nu\in\mathcal{S}} A_\nu \to A_\nu$ will be said to be of W-type if $F|_{A_\nu}$ is of W-type for all places ν of E_p.

4.2 Determining $\mathfrak{X}_{\pi,p}$

In this section we describe $\mathfrak{X}_{\pi,p}$ in terms of isomorphism classes of $W_R\{F, V\}$-ideals, see Theorem 4.9.

Definition 4.5. Put $W_R = W \otimes_{\mathbb{Z}_p} R_p$ which is a $\mathbb{Z}_p$-order inside A. Let $\alpha \in A$ be an element such that $F = \alpha \circ \sigma$ has the Frobenius property; this implies that F is bijective on A. Put $V = pF^{-1}$. By $W_R\{F, V\}$-ideals, we will mean fractional W_R-ideals inside A which are stable by the action of F and V. Given two objects J_1, J_2, let:

- $\mathrm{Hom}_{W_R\{F,V\}}(J_1, J_2)$ consist of the W_R-linear morphisms from J_1 to J_2 that commute with the action of F and V.
- $\mathrm{Hom}_\Delta(J_1, J_2) := \{x \in E_p : \Delta(x)J_1 \subseteq J_2\}$.

Note that W_R does not in general respect the splitting of A given by Equation (9), that is, it cannot be written as a direct sum of components, each lying inside one A_ν. On the other hand, the maximal order $\mathcal{O}_A$ of A, which is the image of $W \otimes \mathcal{O}_{E_p}$ under (9), does respect the splitting.

The following lemma can be seen as a version of Tate's isogeny theorem (see [5, Theorem A.1.1.1]) in this setting.

Lemma 4.6. *Let J_1 and J_2 be any two fractional W_R-ideals. Then Δ induces a bijection*

$$\mathrm{Hom}_{W_R\{F,V\}}(J_1, J_2) \longleftrightarrow \mathrm{Hom}_\Delta(J_1, J_2),$$

which is in fact an isomorphism of R_p-modules.

Proof. The map Δ gives an injection of $\mathrm{Hom}_\Delta(J_1, J_2)$ into $\mathrm{Hom}_{W_R\{F,V\}}(J_1, J_2)$. We now show that this map is also surjective.

Since every W_R-linear morphism φ determines a unique A-linear endomorphism of A, we get that φ is actually multiplication by some element $y \in A$, that is, $\varphi(x) = yx$ for every $x \in A$.

We restrict ourselves to the component A_ν of A. We want to show that since $y_\nu \in A_\nu$ commutes with F_ν, it belongs to $\Delta(E_\nu)$. Put $J_{1,\nu} = J_1 \cap A_\nu$. Commuting with F_ν means that for every $z \in J_{1,\nu}$ we have

$$F_\nu(y_\nu z) = y_\nu F_\nu(z).$$

Since $J_{1,\nu}$ and $\mathcal{O}_{A_\nu}$ are $\mathbb{Z}_p$-lattices of the same rank, the quotient $(J_{1,\nu} + \mathcal{O}_{A_\nu})/J_{1,\nu}$ is a finite abelian group, say of exponent n. Then $\Delta_{|_{E_\nu}}(n)(J_{1,\nu} + \mathcal{O}_{A_\nu}) \subseteq J_{1,\nu}$, which implies that $\Delta_{|_{E_\nu}}(n) \in J_{1,\nu}$ since $1 \in J_{1,\nu} + \mathcal{O}_{A_\nu}$. We have

$$F(y_\nu \Delta_{|_{E_\nu}}(n)) = \alpha\left(y_{\nu,2}, y_{\nu,3}, \ldots, y_{\nu,g_\nu}, \tau(y_1)\right)\Delta_{|_{E_\nu}}(n)$$

and

$$y_\nu F(\Delta_{|_{E_\nu}}(n)) = \alpha\left(y_{\nu,1}, y_{\nu,2}, \ldots, y_{\nu,g_\nu-1}, y_{\nu,g_\nu}\right)\Delta_{|_{E_\nu}}(n)$$

with $\alpha \neq 0$, which shows that $y_{\nu,1} = \ldots = y_{\nu,g_\nu}$ and $y_{\nu,g_\nu} = \tau(y_{\nu,1})$ so $y_\nu \in \Delta_{|_{E_\nu}}(E_\nu)$. □

Definition 4.7. Two fractional W_R-ideals will be called *Δ-isomorphic* if they are isomorphic as R_p-modules via multiplication by an invertible element of $\Delta(E_p)$.

Corollary 4.8. *Two fractional $W_R\{F, V\}$-ideals are isomorphic precisely if they are Δ-isomorphic. Moreover, being stable under F and V is a well-defined notion on Δ-isomorphism classes.*

Proof. The first statement is a direct application of Lemma 4.6. The second statement follows from the fact that F and V act trivially on the elements of $\Delta(E_p)$. □

From now on, we will use Lemma 4.6 to identify $\mathrm{Hom}_{W_R\{F,V\}}(J_1, J_2)$ with the corresponding subset of E_p.

Theorem 4.9. *There is a bijection between $\mathfrak{X}_{\pi,p}$ and the Δ-isomorphism classes of $W_R\{F,V\}$-ideals.*

Proof. A Dieudonné module is a $W_R\{F,V\}$-module, with F having the Frobenius property (cf. Definition 4.1 and $V = pF^{-1}$, that is free over W of rank $2g$, cf. [33, Chapter 1]. Morphisms between them are W_R-linear morphisms that commute with the action of F and V. Every W_R-module that is free over W of rank $2g$ is W_R-linearly isomorphic to a fractional ideal in A (which are all free over W of rank $2g$). The result then follows from Lemma 4.6. □

4.3 Isomorphism classes of $W_R\{F,V\}$-ideals

4.3.1 The connected-étale sequence

For a place ν of E_p put $s(\nu) = \mathrm{val}_\nu(\pi)/(ae_\nu)$. This will be rational number between 0 and 1 (which is equal to i_ν/n_ν in the notation of [33, p. 527]) called the *slope* of ν. Let $\mathfrak{p}_{E_\nu}$ denote the maximal ideal of $\mathcal{O}_{E_p}$ corresponding to ν.

The splitting $\mathcal{O}_{E_p} = \prod_{\nu|p} \mathcal{O}_{E_\nu}$ does not necessarily descend to R_p. However, R_p is complete and semilocal, so it can be identified with the direct sum of the completions at its maximal ideals. The maximal ideals of R_p are exactly equal to $\mathfrak{p}_{E_\nu} \cap R_p = \{x \in R_p : \mathrm{val}_\nu(x) > 0\}$, which might coincide for different ν. We denote the set of maximal ideals of R_p by $\mathcal{P}_{R_p}$.

Lemma 4.10. *Let $*$ denote one of $\{0\}$, $\{1\}$ or the open interval $(0,1)$. Let ν and μ be two places of E. Assume that $s(\nu) \in *$. If $\mathfrak{p}_{E_\nu} \cap R_p = \mathfrak{p}_{E_\mu} \cap R_p$ then $s(\mu) \in *$, as well.*

Proof. We have $R_p = \mathbb{Z}_p[\pi, q/\pi]$. Say that $s(\nu) = 0$ and $s(\mu) > 0$, then $\pi \in \mathfrak{p}_{E_\mu} \cap R_p$ but $\pi \notin \mathfrak{p}_{E_\nu} \cap R_p$, contradiction. Say that $s(\nu) = 1$ and $s(\mu) < 1$, then $q/\pi \in \mathfrak{p}_{E_\mu} \cap R_p$ but $q/\pi \notin \mathfrak{p}_{E_\nu} \cap R_p$, contradiction. □

Notation 4.11. We partition $\mathcal{P}_{R_p} = \mathcal{P}_{R_p}^{\{0\}} \sqcup \mathcal{P}_{R_p}^{(0,1)} \sqcup \mathcal{P}_{R_p}^{\{1\}}$ according to Lemma 4.10. That is, for each $* \in \{\{0\}, \{1\}, (0,1)\}$, let $\mathcal{P}_{R_p}^*$ denote the maximal ideals $\mathfrak{p}_{E_\nu} \cap R_p$ of R_p for which $s(\nu) \in *$. We decompose

$$R_p = R_p^{\{0\}} \times R_p^{(0,1)} \times R_p^{\{1\}},$$

where

$$R_p^* := \prod_{\mathfrak{p} \in \mathcal{P}_{R_p}^*} R_\mathfrak{p}.$$

In this product we put $R_p^* = 0$ if $\mathcal{P}_{R_p}^* = \emptyset$. For ease of notation, we will write $R_p' = R_p^{(0,1)}$ from now on. The decomposition of R_p induces a corresponding decomposition of E_p, of A, of W_R, of any fractional $W_R\{F,V\}$-ideal, and of their endomorphism rings. All these decompositions will be denoted analogously to that of R_p. In particular, we will write E', W_R', A', Δ', F' and V'. In the same vein, by a Δ^*-*morphism* we will mean a morphism given by multiplication by an invertible element of $\Delta(E_p^*)$ and F^* will denote the restriction of F to A^*.

The decomposition of the endomorphism rings can be deduced from the connected-étale sequence, see [5, Example 3.1.6]. The three parts corresponding to $\{0\}$, $(0,1)$ and $\{1\}$ will be called the *étale part*, the *local-local part*, and the *multiplicative part*, respectively.

Proposition 4.12. *There is a bijection between $\mathcal{P}_{R_p}^{\{0\}}$ (resp. $\mathcal{P}_{R_p}^{\{1\}}$) and the maximal ideals of $\mathbb{Z}_p[\pi]$ that do not contain π (resp. of $\mathbb{Z}_p[q/\pi]$ that do not contain q/π).*

Proof. Note that $\mathcal{P}_{R_p}^{\{0\}}$ consists of the maximal ideals of R_p not containing π. Let $\mathfrak{p}$ be a maximal ideal of $\mathbb{Z}_p[\pi]$ that does not contain π. Then $q/\pi \in (\mathbb{Z}_p[\pi])_\mathfrak{p}$ and hence $R_\mathfrak{p} = (\mathbb{Z}_p[\pi])_\mathfrak{p}$. Since R_p is isomorphic to the direct product of the completions of R at the maximal ideals above $\mathfrak{p}$, and $(\mathbb{Z}_p[\pi])_\mathfrak{p}$ is local, we get that there is only one maximal ideal of R above $\mathfrak{p}$, proving bijectivity. The proof for $\mathcal{P}_{R_p}^{\{1\}}$ is analogous. □

Corollary 4.13. *There is a bijection between the maximal ideals not containing π (resp. q/π) of R_p and the irreducible factors $f(x) \neq x$ modulo p of the minimal polynomial of π.*

Proof. There is a bijection between the maximal ideals of $\mathbb{Z}_p[\pi]$ and the irreducible factors modulo p of the minimal polynomial of π, see [30, Theorem 8.2]. An irreducible factor $f(x)$ corresponds to the maximal ideal $p\mathbb{Z}_p[\pi] + f(\pi)\mathbb{Z}_p[\pi]$. The maximal ideals that do not contain π therefore correspond to the irreducible factors different from x. The result now follows from Proposition 4.12. □

Proposition 4.14. *The set $\mathcal{P}'_{R_p}$ is non-empty if and only if the isogeny class $\mathcal{A}_\pi$ is non-ordinary. If so, then $\mathcal{P}'_{R_p}$ consists of one element, the maximal ideal $\mathfrak{p} = (p, \pi, q/\pi)$ of R_p, which has residue field $\mathbb{F}_p$. If $q = p^a$ is not prime, that is, $a > 1$, then $\mathfrak{p}$ is singular and R_p is not the maximal order of E_p.*

Proof. The first statement is clear. Assume for the rest of the proof that the isogeny class is non-ordinary. If we set $\mathfrak{p} = (p, \pi, q/\pi)$ then

$$\frac{R_p}{\mathfrak{p}} = \frac{\mathbb{Z}_p[\pi, q/\pi]}{(p, \pi, q/\pi)} \simeq \mathbb{F}_p. \tag{12}$$

Hence $\mathfrak{p}$ is a maximal ideal of R_p with residue field $\mathbb{F}_p$. Let $\mathfrak{p}_{E_\nu}$ be any maximal ideal of $\mathcal{O}_{E_p}$ associated to a place of slope in the interval $(0, 1)$. Since both π and q/π belong to $\mathfrak{p}_{E_\nu}$, we have that $\mathfrak{p}_{E_\nu} \cap R_p = \mathfrak{p}$. So $\mathfrak{p}$ is the unique element of $\mathcal{P}'_{R_p}$.

Assume that $a > 1$. We now show the last statement by contradiction: assume that $\mathfrak{p}$ is regular, that is, $R_\mathfrak{p}$ is a DVR, with valuation $\mathrm{val}_\mathfrak{p}$. Let $s = \mathrm{val}_\mathfrak{p}(\pi)/ae_\mathfrak{p}$ be the slope of the place associated with $\mathfrak{p}$. If $0 < s < 1/2$ then there must a place of slope $1 - s$, contradicting the fact that $\mathcal{P}'_{R_p}$ consists of one element. Hence $s = 1/2$. By Equation (12), we have

$$e_\mathfrak{p} = e_\mathfrak{p} f_\mathfrak{p} = [E_\mathfrak{p} : \mathbb{Q}_p] > 1,$$

where the inequality follows from the fact that the endomorphism ring is commutative and so

$$f_\mathfrak{p} \mathrm{val}_\mathfrak{p}(\pi)/a = s[E_\mathfrak{p} : \mathbb{Q}_p] = \frac{1}{2}[E_\mathfrak{p} : \mathbb{Q}_p] \in \mathbb{Z},$$

see [33, p. 527]. Hence $e_\mathfrak{p} \geq 2$ which implies that $p \in \mathfrak{p}^2$. Since $\mathfrak{p}$ is fixed by the automorphism of E_p sending π to q/π, we get that

$$\mathrm{val}_\mathfrak{p}(\pi) = \mathrm{val}_\mathfrak{p}(q/\pi) = sae_\mathfrak{p} = \frac{1}{2}ae_\mathfrak{p} \geq a > 1.$$

This implies that $\pi, q/\pi \in \mathfrak{p}^2$ as well. It follows that $\mathfrak{p} = \mathfrak{p}^2$ which is impossible. Therefore, $\mathfrak{p}$ is a singular maximal ideal and, hence, R_p is not the maximal order of E_p. □

Conversely, it is not true that if $\mathfrak{p}$ is singular, then q is not a prime; see Example 8.10.

4.3.2 Duality

The CM involution $\pi \mapsto \bar{\pi} = q/\pi$ induces an involution $\phi : E_p \to E_p$ by $\phi(\sum_{i,j} a_{i,j}\pi^i\bar{\pi}^j) = \sum_{i,j} a_{i,j}\pi^j\bar{\pi}^i$ with $a_{i,j} \in \mathbb{Q}_p$. If ν is a place of E_p then $\bar{\nu} = \nu \circ \phi$ is also a place of E_p with $s(\bar{\nu}) = 1 - s(\nu)$. We also define $\phi : A \to A$ by $\phi(\sum_{i,j} a_{i,j,k}\zeta_{q-1}^k\pi^i\bar{\pi}^j) = \sum_{i,j} a_{i,j,k}\zeta_{q-1}^k\pi^j\bar{\pi}^i$. The proof of the following lemma is omitted.

Lemma 4.15. *Choose any $F_\nu = \alpha \circ \sigma$ with the Frobenius property. Then $F_{\bar{\nu}} = \phi(\alpha) \circ \sigma$ will have the Frobenius property, and ϕ induces a bijection, taking $W_{R_\nu}\{F_\nu, V_\nu\}$-ideals I to $W_{R_{\bar{\nu}}}\{F_{\bar{\nu}}, V_{\bar{\nu}}\}$-ideals $\phi(I)$.*

4.3.3 The étale and multiplicative parts

By Theorem 4.9, Dieudonné modules in $\mathfrak{X}_{\pi,p}$ are in bijection with $W_R\{F, V\}$-ideals. In this section, we show that we can describe the étale and multiplicative part of the Dieudonné module, that is when $* = \{0\}$ or $* = \{1\}$, in terms of R_p^*-ideals in E_p^* rather than $W_R^*\{F^*, V^*\}$-ideals in A^*.

Proposition 4.16. *If $*$ is either $\{0\}$ or $\{1\}$ then one can choose F^* with the Frobenius property such that the following hold.*

(i) If I is an R_p^*-ideal then $W \otimes_{\mathbb{Z}_p} I$ is a $W_R^*\{F^*, V^*\}$-ideal.

(ii) If J is a $W_R^*\{F^*, V^*\}$-ideal then $J = W \otimes_{\mathbb{Z}_p} (\Delta^*)^{-1}(J \cap \Delta^*(E_p^*))$.

(iii) For any $W_R^*\{F^*, V^*\}$-ideals J_1, J_2 there is a bijection

$$\mathrm{Hom}_{\Delta^*}(J_1 \cap \Delta^*(E_p^*), J_2 \cap \Delta^*(E_p^*)) \longleftrightarrow \mathrm{Hom}_{W_R^*\{F^*,V^*\}}(J_1, J_2).$$

Remark 4.17. Note that F^* chosen in Proposition 4.16, and in Corollary 4.18 below, is not necessarily of W-type.

Proof.

(i) We first prove the case $* = \{0\}$. Arguing as in the proof of [33, Theorem 7.4], we can find an invertible element α of $W_R^{\{0\}}$ such that $F^{\{0\}} = \alpha \circ \sigma$ has the Frobenius property. Since $\sigma(W \otimes I) \subseteq W \otimes I$ it follows that $F^{\{0\}}(W \otimes I) \subseteq W \otimes I$. Furthermore, $p\alpha^{-1}$ is in $W_R^{\{0\}}$ since α is a unit, and hence $V^{\{0\}}(W \otimes I) \subseteq W \otimes I$, as well.

Now consider $* = \{1\}$. Since π/q is a unit in $R_p^{\{1\}}$, [33, Theorem 7.4] can be used in the same way to find an invertible element u of $W_R^{\{1\}}$ such that $F^{\{1\}} = (pu) \circ \sigma$ has the Frobenius property. It then follows in the same way as above that $W \otimes I$ will be stable under $F^{\{1\}}$ and $V^{\{1\}}$.

In the rest of this proof we use terminology and results of [9, Chapter 0] to carry out a descent argument.

(ii) Let G be the Galois group of $L = \mathbb{Q}_p(\zeta_{q-1})$ over $\mathbb{Q}_p$. We have that $G = \{\sigma_j\}_{j=1,\dots,a}$ with $\sigma_j(\zeta_{q-1}) = \zeta_{q-1}^{p^j}$. The group G acts on $W = \mathbb{Z}_p[\zeta_{q-1}]$ and therefore has an induced action on $W \otimes_{\mathbb{Z}_p} R_p^*$. Moreover, $R_p^* = (W \otimes_{\mathbb{Z}_p} R_p^*)^G$ because $W^G = \mathbb{Z}_p$.

For any $i = 1, \dots, p^a - 1$, let $x_i = (p^a - 1)^{-1}\zeta_{q-1}^{-i} \in W$ and $y_i = \zeta_{q-1}^i \in W$. Any (not necessarily primitive) $(p^a - 1)$-st root of unity except 1 is a root of $x^{p^a-2} + x^{p^a-3} + \ldots + 1$ and hence,

$$\sum_{i=1}^{p^a-1} x_i \sigma_j(y_i) = \frac{1}{p^a - 1} \sum_{i=1}^{p^a-1} (\zeta_{q-1}^{p^j-1})^i = \begin{cases} 1 \text{ if } j = a, \\ 0 \text{ if } j = 1, \dots, a-1. \end{cases}$$

Let J be any $W_R^*\{F^*, V^*\}$-ideal. It follows from [9, Theorem 1.6.(ii')] that $W \otimes_{\mathbb{Z}_p} R_p^*$ over R_p^* is a G-Galois-extension of commutative rings. Moreover, J is stable under G, in fact $J^G = J \cap \Delta(E_p^*)$. Consider the descent datum on J defined by $\Phi_{\sigma_j} = \sigma_j$ for all $j = 1, \dots, a$. From [9, Theorem 7.1] it follows that $J = W \otimes (\Delta^*)^{-1}(J \cap \Delta^*(E_p^*))$.

(iii) The set $\mathrm{Hom}_{\Delta^*}(J_1 \cap \Delta^*(E_p^*), J_2 \cap \Delta^*(E_p^*))$ can be identified with the set of $x \in E_p^*$ such that $x(J_1 \cap \Delta^*(E_p^*)) \subseteq J_2 \cap \Delta^*(E_p^*)$. By Lemma 4.6 we may identify $\mathrm{Hom}_{W_R^*\{F^*,V^*\}}(J_1, J_2)$ with the set of $x \in E_p^*$ such that $\Delta^*(x)J_1 \subseteq J_2$. Since $\Phi_{\sigma_j}\Delta^*(x) = \Delta^*(x)\Phi_{\sigma_j}$ for any j, we conclude from [9, Theorem 7.2] that the map $x \mapsto \Delta^*(x)$ induces a bijection.

□

Corollary 4.18. *If $*$ is either $\{0\}$ or $\{1\}$ then one can choose F^* with the Frobenius property such that the map $\psi : [I]_{R_p^*} \mapsto [I \otimes W]_{\Delta^*}$ is a bijection from isomorphism classes of R_p^*-ideals to Δ^*-isomorphism classes of $W_R^*\{F^*, V^*\}$-ideals.*

Proof. It follows from Proposition 4.16.(i) and (iii) that the map ψ is well defined and injective, since the bijection in Proposition 4.16.(iii) restricts to a bijection on the subsets of Hom_{Δ^*} resp. $\mathrm{Hom}_{W_R^*}$ consisting of isomorphisms. Surjectivity follows from Proposition 4.16.(ii). □

4.3.4 The local-local part in the maximal endomorphism ring case

In [33, proof of Theorem 5.1], Waterhouse gave an explicit description of isomorphism classes of fractional $\mathcal{O}_{A'}$-ideals which are stable by the action of F' and V'. We paraphrase it in (i) of Proposition 4.19 below, adding a formula for their number in (ii).

Each fractional $\mathcal{O}_{A'}$-ideal is a direct sum of fractional $\mathcal{O}_{A_\nu}$-ideals. Moreover, the action of F' and V' preserves ν-components. Hence it is enough to focus our attention on a single ν-component A_ν of A'. Let t_ν be a uniformizer of E_ν. Then t_ν is also a uniformizer of LE_ν and every fractional $\mathcal{O}_{A_\nu}$-ideal is uniquely determined by its generator, which has the form $(t_\nu^{\varepsilon_1}, \ldots, t_\nu^{\varepsilon_{g_\nu}})$ for some nonnegative integers $\epsilon_1, \ldots, \epsilon_{g_\nu}$.

Proposition 4.19. *For each place ν of E with $s(\nu) \in (0,1)$ consider the set χ_ν all ordered g_ν-tuples*

$$0 \leq n_1, \ldots, n_{g_\nu} \leq e_\nu$$

such that

$$\sum_{i=1}^{g_\nu} n_i = \frac{g_\nu \mathrm{val}_\nu(\pi_\nu)}{a}.$$

For each such tuple, set $\varepsilon_1 = 0$ and $\varepsilon_i = \varepsilon_{i-1} + n_{i-1}$, for $i = 2, \ldots, g_\nu$.

Fix any F' of W-type (see Definition 4.4). Then:

(i) The map υ_ν given by $(\varepsilon_1, \ldots, \varepsilon_{g_\nu}) \mapsto (t_\nu^{\varepsilon_1}, \ldots, t_\nu^{\varepsilon_{g_\nu}})$ induces a bijection between $\chi' = \prod_{s(\nu)\in(0,1)} \chi_\nu$ and the set of Δ'-isomorphism classes of fractional $W_R'\{F', V'\}$-ideals with multiplicator ring $\mathcal{O}_{A'}$;

(ii) We have

$$|\chi_\nu| = \sum_{i=0}^{d} (-1)^i \binom{g_\nu}{i} \binom{g_\nu \mathrm{val}_\nu(\pi_\nu)/a - i(e_\nu+1) + g_\nu - 1}{g_\nu - 1}, \tag{13}$$

with $d = \min(g_\nu, \lfloor g_\nu \mathrm{val}_\nu(\pi_\nu)/(a(g_\nu+1)) \rfloor)$.

Proof. The set χ_ν is defined as in [33, Theorem 5.1]. In the proof of *loc. cit.*, it is shown that υ_ν can be found in the wanted form, and that an ideal determined by g_ν-tuples of the form $(t_\nu^{\varepsilon_1}, \ldots, t_\nu^{\varepsilon_{g_\nu}})$ is a $W_R'\{F', V'\}$-ideal if and only if, for all ν, the number ε_1 is any integer and ε_i for $i = 2, \ldots, g_\nu$ are as in the statement. Since we are working up to Δ'-isomorphism, we can scale and hence assume that $\varepsilon_1 = 0$.

The cardinality $|\chi_\nu|$ is equal to the number of ways of writing $m = g_\nu \mathrm{val}_\nu(\pi_\nu)/a$ as a sum of positive integers (i.e., weak compositions) with each positive integer bounded by e_ν. The formula (13) can be found by noticing that it is also equal to the coefficient of x^m in the polynomial

$$(1 + x + \ldots + x^{e_\nu})^{g_\nu} = \frac{(1 - x^{e_\nu+1})^{g_\nu}}{(x-1)^{g_\nu}};$$

the coefficient of $x^{i(e_\nu+1)}$ in the numerator of the rational expression equals $(-1)^i \binom{g_\nu}{i}$, and the coefficient x^j for $j \geq 0$ in the expansion of the denominator equals $\binom{j+g_\nu-1}{g_\nu-1}$. One then considers all choices of i, j such that $i(e_\nu+1) + j = m$. For a reference, see for instance [1, Equation (4.0)]. □

Definition 4.20. Using the notation from Proposition 4.19, put

$$\Upsilon := \{ \prod_{s(\nu)\in(0,1)} \upsilon_\nu(\epsilon_1, \ldots, \epsilon_{g_\nu}) : (\epsilon_1, \ldots, \epsilon_{g_\nu}) \in \chi_\nu \text{ for all } s(\nu) \in (0,1)\}.$$

5 Equivalences of categories

In this section we will extend the results of Section 2 to give a categorical equivalence in Theorem 5.2 between the isogeny class $\mathcal{A}_\pi$ and a category $\mathcal{C}_\pi$ of pairs of ideals, see Definition 5.1. The pairs of ideals will respectively give representatives of the Tate modules and the Dieudonné module of the corresponding abelian variety.

Definition 5.1. For each ℓ, let i_ℓ be the injection $E \to E_\ell$. Let $\mathcal{C}_\pi$ be the category whose objects are pairs (I, M), where I is a fractional R-ideal in E, and M is a $W_R\{F, V\}$-ideal such that $\Delta^{-1}(M) = i_p(I)R_p$. The homomorphisms between objects (I, M) and (J, N) in $\mathcal{C}_\pi$ are the elements $\alpha \in E$ such that $\alpha I \subseteq J$ and $\Delta(i_p(\alpha))M \subseteq N$.

Theorem 5.2. *There is an equivalence of categories $\Psi : \mathcal{C}_\pi \to \mathcal{A}_\pi$.*

Proof. Recall that we have fixed an abelian variety X in $\mathcal{A}_\pi$. For each object (I, M) in $\mathcal{C}_\pi$, we fix positive integers k, n_p, and n_ℓ for all $\ell \neq p$, such that

$$\ell^{n_\ell} T_\ell(X) \subseteq k \cdot i_\ell(I) \subseteq T_\ell(X) \quad \text{and} \quad p^{n_p} M(X) \subseteq k \cdot M \subseteq M(X).$$

For all $\ell \neq p$, let $K_\ell(I)$ be the subgroup of $X(\overline{\mathbb{F}}_p)[\ell^{n_\ell}] = T_\ell(X)/\ell^{n_\ell} T_\ell(X)$ equal to $k \cdot i_\ell(I)/\ell^{n_\ell} T_\ell(X)$. Define $K_p(I)$ analogously. This is possible by the results of Section 2 together with Theorem 3.12(i) and Theorem 4.9. Let K be the subgroup of X generated by all $K_\ell(I)$ together with $K_p(I)$.

Define the abelian variety $X_{(I,M)} = X/K$ in $\mathcal{A}_\pi$. By Tate's theorem, there exists an isogeny $\varphi : X_{(I,M)} \to X$ such that $\varphi_*(T_\ell(X_{(I,M)})) = k \cdot i_\ell(I) \subseteq T_\ell(X)$ and $\varphi_*(M(X_{(I,M)})) = k \cdot M \subseteq M(X)$. Finally, define the quasi-isogeny $\varphi_{(I,M)} = \varphi/k : X_{(I,M)} \to X$ and put $\Psi((I, M)) = X_{(I,M)}$.

Let $\alpha : (I, M) \to (J, N)$ be a homomorphism between objects of $\mathcal{C}_\pi$. We will first only consider $\alpha \in E^\times$, which will correspond via Ψ to isogenies in $\mathcal{A}_\pi$. The pair $(\alpha I, i_p(\alpha)M)$, which belongs to $\mathcal{C}_\pi$ since $\alpha \in E^\times$, gives rise (by Tate's theorem, as above) to a quasi-isogeny $\varphi_\alpha : X_{(\alpha I, i_p(\alpha)M)} \to X$. Multiplication with $\alpha \in E^\times$ is then the same as an isomorphism $\epsilon_\alpha : X_{(I,M)} \to X_{(\alpha I, i_p(\alpha)M)}$ such that $\varphi_{(I,M)} = \varphi_\alpha \circ \epsilon_\alpha$. Again by Tate's theorem, the inclusion $(\alpha I, i_p(\alpha)M) \subseteq (J, N)$ gives rise to an isogeny $\epsilon : X_{(\alpha I, i_p(\alpha)M)} \to X_{(J,N)}$ such that $\varphi_{(I,M)} = \varphi_{(J,N)} \circ \epsilon \circ \epsilon_\alpha$. We put $\Psi(\alpha : (I, M) \to (J, N)) = \epsilon \circ \epsilon_\alpha$.

Since Ψ respects composition and the identity, it is a functor. It also follows directly that the functor Ψ is essentially surjective.

Each isogeny $X_{(I,M)} \to X_{(J,N)}$ is equal to $\varphi_{(J,N)}^{-1} \circ \alpha \circ \varphi_{(I,M)}$ for some $\alpha \in E^\times$, viewed as a quasi-isogeny of X, and necessarily $\alpha I \subseteq J$ and $\Delta(i_p(\alpha))M \subseteq N$. Moreover, if $\alpha \neq \beta \in E$ we see directly that $\Psi(\alpha : (I, M) \to (J, N)) \neq \Psi(\beta : (I, M) \to (J, N))$. This shows that Ψ is both full and faithful when restricted to homomorphisms of $\mathcal{C}_\pi$ in $E^\times$ and isogenies in $\mathcal{A}_\pi$.

Let us now consider any $\alpha \in E$. The isogeny decomposition $X \sim X_1 \times \ldots \times X_r$ gives a corresponding decomposition $E = E_1 \times \ldots \times E_r$. An element $\alpha = (\alpha_1, \ldots, \alpha_r) \in E$ is in $E^\times$ precisely if $\alpha_i \neq 0$ for all $i = 1, \ldots, r$. Moreover any morphism between simple factors X_i and X_j is either an isogeny (and then necessarily $i = j$), or the zero morphism. It is now immediate that Ψ is both full and faithful on all homomorphisms. □

Definition 5.3. For any overorder $S \supseteq R$ in E, let $\mathcal{D}_\pi(S)$ denote the category of fractional S-ideals with homomorphisms between two S-ideals I, J being $\alpha \in E$ such that $\alpha I \subseteq J$.

The following corollary reproves the second part of [21, Corollary 4.4], which builds upon [3] and [7].

Corollary 5.4. *Assume that (at least) one of the following conditions holds:*

(i) The number $q = p$ is a prime;

(ii) The category $\mathcal{A}_\pi$ consists of ordinary abelian varieties,

then there is an equivalence of categories between $\mathcal{D}_\pi(R)$ and $\mathcal{A}_\pi$, inducing a bijection between $\mathrm{ICM}(R)$ *and $\mathcal{A}_\pi^{\mathrm{isom}}$.*

Proof. If either of the conditions holds, define a functor $\Xi : \mathcal{D}_\pi(R) \to \mathcal{A}_\pi$ by letting $\Xi(I) = \Psi(I, W \otimes I)$ and $\Xi(\alpha : I \to J) = \Psi(\alpha : I \to J)$.

If $q = p$ is a prime, then $W = \mathbb{Z}_p$ and $W_R\{F, V\}$-ideals are nothing but R_p-ideals. Theorem 5.2 then shows that Ξ is an equivalence.

Say now that $\mathcal{A}_\pi$ consists of ordinary abelian varieties. Proposition 4.16 shows that all $W_R\{F, V\}$-ideals are of the form $W \otimes I$, with I a fractional R-ideal. Theorem 5.2 then shows that also in this case Ξ is an equivalence. □

In the next result we restrict ourselves to abelian varieties such that the local-local part of their Dieudonné module has maximal endomorphism ring. This gives an equivalence that is similar in spirit to, for instance, [33, Theorems 5.1 and 5.3], [24, Theorems 1.1 and 4.5] (see further in Example 5.6) and [2, Theorem 1.3].

Corollary 5.5. *Let S denote the smallest order in $\mathcal{O}_E$ containing R and such that S_p contains $\mathcal{O}_{E'_p}$. Let r be the number of Δ'-isomorphism classes of $W'_R\{F', V'\}$-ideals whose endomorphism ring contains $\mathcal{O}_{E'_p}$. Then there are full and faithful functors $\Psi_i : \mathcal{D}_\pi(S) \to \mathcal{A}_\pi$ for $i = 1, .., r$ that induce a bijection between the isomorphism classes of abelian varieties Z in $\mathcal{A}_\pi$ with $\mathcal{O}_{E'_p} \subseteq \mathrm{End}(Z)_p$ and the disjoint union of r copies of* $\mathrm{ICM}(S)$.

Proof. Let $M'_1, \dots, M'_r$ be representatives of each Δ'-isomorphism class of $W'_R\{F', V'\}$-ideals whose endomorphism ring contains $\mathcal{O}_{E'_p}$. Choose $F^{\{0\}}$ and $F^{\{1\}}$ as in Proposition 4.16 so that, for each $i = 1, \dots, r$,

$$M_i = W_R^{\{0\}} \oplus M'_i \oplus W_R^{\{1\}},$$

is a $W_R\{F, V\} = W_R^{\{0\}}\{F^{\{0\}}, V^{\{0\}}\} \times W'_R\{F', V'\} \times W_R^{\{1\}}\{F^{\{1\}}, V^{\{1\}}\}$-ideal. Since $\Delta^{-1}(M_i) = R_p^{\{0\}} \times \mathcal{O}_{E'_p} \times R_p^{\{0\}}$, for any fractional S-ideal I it follows that $\Delta^{-1}(\Delta(i_p(I))M_i) = i_p(I)\,\Delta^{-1}(M_i) = i_p(I)(R_p^{\{0\}} \times \mathcal{O}_{E'_p} \times R_p^{\{0\}})$ and hence $(I, \Delta(i_p(I))M_i)$ will be an object in $\mathcal{C}_\pi$.

For each $i = 1, \dots, r$, define a functor $\Psi_i : \mathcal{D}_\pi(S) \to \mathcal{A}_\pi$ by putting $\Psi_i(I) = \Psi((I, \Delta(i_p(I))M_i))$ and $\Psi_i(\alpha : I \to J) = \Psi(\alpha : (I, \Delta(i_p(I))M_i) \to (J, \Delta(i_p(J))M_i))$. That these functors are full and faithful follows from the corresponding facts for Ψ.

Finally, take any abelian variety Z in $\mathcal{A}_\pi$ with $\mathcal{O}_{E'_p} \subseteq \mathrm{End}(Z)_p$. Then there is an object (I, M) in $\mathcal{C}_\pi$ such that $\Psi((I, M))$ is isomorphic to Z. Write $I'_p = i_{p|_{E'_p}}(I)R'_p$. Since I'_p is a principal $\mathcal{O}_{E'_p}$-ideal, there is a $\beta \in E$ such that $\Delta'(\beta)M' = \Delta'(I'_p)M'_j$ for some $j \in \{1, \dots, r\}$. Then

$$\beta I'_p = \beta\Delta'^{-1}(M') = I'_p\Delta'^{-1}(M'_j) = I'_p\mathcal{O}_{E'_p} = I'_p. \tag{14}$$

By the strong approximation theorem we can find a new element $\beta \in E$ such that (14) still holds, and moreover $\beta_\ell \in R_\ell^\times$, for any $\ell \neq p$, and $\beta_p^* \in (R_p^*)^\times$ for $* \in \{\{0\}, \{1\}\}$. Then put $\gamma = \beta\gamma'$ for any $\gamma' \in (I : I)^\times$. It follows that $\Delta'(\gamma)M' = I'_pM'_j$ and that $\gamma I = I$. By Proposition 4.16 we get that if N_1 and N_2 are any $W_R^{\{0\}}\{F^{\{0\}}, V^{\{0\}}\}$-ideals such that $(\Delta^{\{0\}})^{-1}(N_1) = (\Delta^{\{0\}})^{-1}(N_2)$ then $N_1 = N_2$. The corresponding statement also holds for $W_R^{\{1\}}\{F^{\{1\}}, V^{\{1\}}\}$-ideals. It follows that $\gamma M = \Delta(i_p(I))M_j$. Hence, $\Psi_j(I)$ is isomorphic to $\Psi((I, M)) \simeq Z$ in $\mathcal{A}_\pi$, via $\gamma \in E$. □

Example 5.6. If $\mathcal{A}_\pi$ consists of almost-ordinary abelian varieties, then there is a unique place ν above p with slope $s(\nu) \in (0, 1)$ and it will have slope $1/2$. It follows from [24, Proposition 2.1] that the endomorphism ring of all $W'_R\{F', V'\}$-ideals contains $\mathcal{O}_{E'_p}$. Corollary 5.5 can then be compared with [24, Theorem 4.5.(3)]. Equation (13) shows that if ν is the place above p with $s(\nu) = 1/2$, then the number r of Δ'-isomorphism classes of $W'_R\{F', V'\}$-ideals whose endomorphism ring contains $\mathcal{O}_{E'_p}$ equals $r = 2$ if $e_\nu = 1$, and equals $r = 1$ if $e_\nu = 2$. Note that Corollary 5.5 holds also for even q, while [24, Theorem 4.5.(3)] does not.

In the case when $e_\nu = 1$, we can use Theorem 5.2 to describe isogenies between two abelian varieties $X_1 = \Psi_1(I)$ and $X_2 = \Psi_2(J)$. Say that M'_1 is generated as a $\mathcal{O}_{A_\nu}$-ideal by $(1, 1) \in A_\nu = LE_\nu \oplus LE_\nu$, and M'_2 by $(1, t_\nu) \in A_\nu$, where t_ν is a uniformizer of $E_\nu \subseteq LE_\nu$ (compare with Proposition 4.19). We see that every $\alpha \in (J : I) \cap E^\times$ induces an isogeny $X_1 \to X_2$, but $\beta \in (I : J) \cap E^\times$ induces an isogeny $X_2 \to X_1$ if and only if $\mathrm{val}_\nu(\beta) > 0$. These types of isogenies are not described in [24].

Note finally that if q is not prime, then R'_p is singular by Proposition 4.14. So, in this case R cannot be an endomorphism ring of an almost-ordinary abelian variety.

In the following two results we will draw some consequences from Theorem 5.2 on the endomorphism rings of abelian varieties in $\mathcal{A}_\pi$.

Proposition 5.7. *Say that there is a $W'_R\{F', V'\}$-ideal M' with endomorphism ring $T' \subseteq E'_p$ such that $\Delta'^{-1}(M')$ is invertible in T'. Let S be any overorder of R such that S'_p contains T'. Then there is an abelian variety in $\mathcal{A}_\pi$ with endomorphism ring S.*

Proof. Choose $F^{\{0\}}$ and $F^{\{1\}}$ as in Proposition 4.16 and let M be the $W_R\{F, V\} = W_R^{\{0\}}\{F^{\{0\}}, V^{\{0\}}\} \times W'_R\{F', V'\} \times W_R^{\{1\}}\{F^{\{1\}}, V^{\{1\}}\}$-ideal $(W_R^{\{0\}} \otimes R_p^{\{0\}}) \oplus M' \oplus (W_R^{\{1\}} \otimes R_p^{\{1\}})$. Fix the fractional R-ideal I such that $i_\ell(I)R_\ell = R_\ell$ and such that $i_p(I)R_p = \Delta^{-1}(M)$, whose existence is guaranteed by [32, Theorem 9.4.9, Lemma 9.5.3]. Since $\Delta^{-1}(\Delta(i_p(S))M) = i_p(S)\Delta^{-1}(M) = i_p(SI)R_p$ we have that $(SI, \Delta(i_p(S))M) \in \mathcal{C}_\pi$, and since I is locally principal for all ℓ (including p), we have that $(SI : SI) = (S : S) = S$. The abelian variety $\Psi((SI, \Delta(i_p(S))M))$ then has endomorphism ring S. □

Corollary 5.8. *Let S be any overorder of R. There exists an abelian variety in the isogeny class whose endomorphism ring T satisfies $S_\ell \simeq T_\ell$ for every $\ell \neq p$ and $S_p^* \simeq T_p^*$ for $*$ equal to $\{0\}$ or $\{1\}$.*

Proof. It follows from [33, Theorem 5.1] that there is a $W_R'\{F', V'\}$-ideal M' with maximal endomorphism ring. The abelian variety $\Psi((SI, \Delta(i_p(S))M))$ constructed as in the proof of Proposition 5.7 then has an endomorphism ring with the wanted properties. □

6 Computing fractional $W_R\{F, V\}$-ideals

The goal of this section is to provide an effective method to compute representatives of the Δ-isomorphism classes of $W_R\{F, V\}$-ideals.

By the discussion after Notation 4.11, the decomposition $R_p = R_p^{\{0\}} \times R_p' \times R_p^{\{1\}}$ induces a decomposition of Δ-isomorphism classes of $W\{F, V\}$-ideals, which yields a natural bijection

$$\{\Delta\text{-isom. classes of } W_R\{F, V\}\text{-ideals}\} \longleftrightarrow \prod_{*\in\{\{0\},(0,1),\{1\}\}} \{\Delta^*\text{-isom. classes of } W_R^*\{F^*, V^*\}\text{-ideals}\}. \tag{15}$$

The next proposition states that for $* \in \{\{0\}, \{1\}\}$ the computation of the terms on the right hand side of (15) reduces to computations of known objects discussed in Section 3.

Proposition 6.1. *For $* \in \{\{0\}, \{1\}\}$ we have a natural bijection*

$$\{\Delta^*\textit{-isom. classes of } W_R^*\{F^*, V^*\}\textit{-ideals}\} \longleftrightarrow \prod_{\mathfrak{p}_\nu \in \mathcal{P}_{R_p}, s(\nu)\in *} \mathcal{W}_{\mathfrak{p}_\nu}(R), \tag{16}$$

where denotes $\mathfrak{p}_\nu$ the intersection with R_p of the maximal ideal inducing ν.

Proof. By Corollary 4.18, the left-hand side of (16) is in bijection with $\{\Delta^*$-isom. classes of R_p^*-ideals$\}$, which is just $\mathcal{W}(R_p^*)$ by Remark 3.2. Since R_p^* is the direct product of the rings $R_{\mathfrak{p}_\nu}$ for $\mathfrak{p}_\nu \in \mathcal{P}_R$ such that $s(\nu) \in *$, the latter set is in bijection with the right hand side of (16) by Proposition 3.9. □

In view of Proposition 6.1, we restrict our attention to computing the Δ'-isomorphism classes of $W_R'\{F', V'\}$-ideals. We can view E_p' as a subset of E_p and A' as a subset of A, so that $\Delta : E_p \to A$ restricted to E_p' is precisely Δ'. We say that two fractional W_R'-ideals I and J are Δ'-isomorphic if there exists a non-zero divisor $\gamma \in R_p'$ such that $\Delta'(\gamma)I = J$. Note that Δ'-isomorphism implies isomorphism as R_p'-modules, but that conversely two fractional W_R'-ideals can be isomorphic as R_p'-modules while not being Δ'-isomorphic.

The computation of Δ'-isomorphism classes is divided into three steps:

1. Compute W_R'-isomorphism classes of fractional W_R'-ideals.
2. Compute the partition of each W_R'-isomorphism class into Δ'-isomorphism classes of fractional W_R'-ideals.
3. Determine which Δ'-isomorphism classes of fractional W_R'-ideals are stable under the action of F and V, that is, which are $W_R'\{F', V'\}$-ideals.

The three steps will be discussed in Subsections 6.2, 6.3 and 6.4, respectively. In Section 7, we will summarize all steps in one algorithm.

Even though the rings R_p' and W_R' are $\mathbb{Z}_p$-orders, the method we describe will be exact, in the sense that every computation will be performed globally with fractional ideals of $\mathbb{Z}$-orders. To do so, we now introduce some further notation.

6.1 Global setting

Recall that L is an unramified extension of degree a of $\mathbb{Q}_p$. Let $c(x)$ be a lift to $\mathbb{Z}[x]$ of any irreducible factor of degree a of $x^{q-1}-1$ over $\mathbb{F}_p[x]$. We have $L \simeq \mathbb{Q}_p[x]/c(x)$. Set $\widetilde{L} = \mathbb{Q}[x]/c(x)$ and denote by ζ the class of x in $\widetilde{L}$. Note that $\widetilde{L} \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq L$. Moreover $\widetilde{L}$ has a unique place above p, which is unramified.

Let $g_1(x), \ldots, g_r(x)$ be the irreducible factors over $\widetilde{L}[x]$ of the characteristic polynomial $h(x)$ of π. Define

$$\widetilde{A} = \prod_{i=1}^{r} \frac{\widetilde{L}[x]}{g_i(x)} \quad \text{and} \quad \widetilde{W_R} = \prod_{i=1}^{r} \frac{\mathcal{O}_{\widetilde{L}}[x]}{g_i(x)}. \tag{17}$$

The association $\pi \mapsto (x + (g_i(x)))_{i=1,\ldots,r}$ induces an embedding $\widetilde{\Delta} : E \to \widetilde{A}$.

Remark 6.2.

(i) We have isomorphisms $\widetilde{A} \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq A$ and $\widetilde{W_R} \otimes_{\mathbb{Z}} \mathbb{Z}_p \simeq W_R$ giving inclusions $\widetilde{W_R} \subseteq \widetilde{A} \subseteq A$.

(ii) For every fractional W_R-ideal $I \subseteq A$, there is a unique fractional $\widetilde{W_R}$-ideal $\widetilde{I}$ such that $\widetilde{I} \otimes_{\mathbb{Z}} \mathbb{Z}_p = I$ and $\widetilde{I} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell = \mathcal{O}_{\widetilde{A}} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ for every prime $\ell \neq p$; see for example [32, Theorem 9.4.9, Lemma 9.5.3], as in Proposition 5.7. Note that the maximal order $\mathcal{O}_{\widetilde{A}}$ of $\widetilde{A}$ satisfies $\mathcal{O}_{\widetilde{A}} = \widetilde{\mathcal{O}}_A$. Also, if $I \subseteq J$ are fractional W_R-ideals then

$$\frac{\widetilde{J}}{\widetilde{I}} \simeq \frac{J}{I}$$

is a finite W_R-module annihilated by a power of p.

(iii) Let $\mathfrak{p}$ be a maximal ideal of W_R and $\widetilde{\mathfrak{p}}$ be as in (ii). Then $\widetilde{W}_{R,\widetilde{\mathfrak{P}}} \simeq W_{R,\mathfrak{P}}$.

(iv) Assume for a moment that $\widetilde{L}$ is a normal extension of $\mathbb{Q}$. Let $\widetilde{\sigma}_L$ be any generator of the decomposition group of the maximal ideal $p\mathcal{O}_{\widetilde{L}}$ of $\mathcal{O}_{\widetilde{L}}$. Then $\widetilde{\sigma}_L$ extends to the Frobenius σ of L. Let π_A denote the element $\widetilde{\Delta}(\pi)$. Since $h(x)$ is square-free, the elements $1_A, \pi_A, \ldots, \pi_A^{\deg(h)}$ form a $\widetilde{L}$-basis of $\widetilde{A}$. In other words, $\widetilde{A}$ can be described as

$$\widetilde{A} = 1_A \cdot \widetilde{L} \oplus \pi_A \cdot \widetilde{L} \oplus \ldots \oplus \pi_A^{\deg(h)} \cdot \widetilde{L}. \tag{18}$$

Using the presentation given in Equation 18, define $\widetilde{\sigma} : \widetilde{A} \to \widetilde{A}$ by fixing π_A and acting on the $\widetilde{L}$-coefficients as $\widetilde{\sigma}_L$. Observe that $\widetilde{\sigma}$ extends to the automorphism σ of A.

To simplify the exposition, we will assume that $\widetilde{L}$ is normal in the following algorithms. Nevertheless, we will always need only to compute the action of $\widetilde{\sigma}$ on finite quotients of $\mathcal{O}_{\widetilde{A}}$. We detail in Remarks 6.12 and 6.18 how to do this efficiently. Computing such finite approximations does not require us to compute the decomposition group of $p\mathcal{O}_{\widetilde{L}}$, and, in fact, it does not even require $\widetilde{L}$ to be normal.

(v) Let ν be a place of E_p. Then we have

$$\mathcal{O}_{A_\nu} = \underbrace{\mathcal{O}_{LE_\nu} \times \ldots \times \mathcal{O}_{LE_\nu}}_{g_\nu - \text{times}},$$

cf. Equation 9. The unique maximal ideal of $\mathcal{O}_{E_\nu}$ is denoted $\mathfrak{p}_{E_\nu}$. A maximal ideal of $\mathcal{O}_{A_\nu}$ is equal to the unique maximal ideal $\mathfrak{p}_{LE_\nu} = \mathfrak{p}_{E_\nu}\mathcal{O}_{LE_\nu}$ in exactly one of the g_ν factors, and to the ideal generated by 1 in all other factors. In particular, there are exactly g_ν maximal ideals $\mathfrak{P}_{\nu,1}, \ldots, \mathfrak{P}_{\nu,g_\nu}$ of $\mathcal{O}_{A_\nu}$ extending ν. Let $t_1, \ldots, t_{g_\nu}$ be some corresponding uniformizers. If $t_\nu \in E_p$ is a uniformizer for ν then its image in A_ν via the embedding induced by Δ is $(t_\nu, \ldots, t_\nu) = (v_1 t_1, \ldots, v_{g_\nu} t_{g_\nu})$ for units $v_i \in \mathcal{O}_{LE_\nu}^\times$. For each i, consider the maximal ideal $\widetilde{\mathfrak{P}}_{\nu,i}$ of $\mathcal{O}_{\widetilde{A}}$ built using (ii). Any lift of a basis element of the $\mathcal{O}_{\widetilde{A}}/\widetilde{\mathfrak{P}}_{\nu,i}$-vector space $\widetilde{\mathfrak{P}}_{\nu,i}/\widetilde{\mathfrak{P}}_{\nu,i}^2$ will map to a uniformizer of $\mathcal{O}_{\widetilde{A},\widetilde{\mathfrak{P}}_{\nu,i}} \simeq \mathcal{O}_{A,\mathfrak{P}_{\nu,i}}$. However, since $\mathcal{O}_A$ is generally not an integral domain, such a lift might not be a unit in the completions at the other maximal ideals above ν. For example, such a lift might be a zero-divisor. We address this issue in Lemma 6.3 below.

(vi) Let S' be an order in A', let I' be a fractional S'-ideal, and let $\mathfrak{p}'$ be a maximal ideal of S'. Consider the order in $A = A^{\{0\}} \times A' \times A^{\{1\}}$ given by $S = \mathcal{O}_{A^{\{0\}}} \times S' \times \mathcal{O}_{A^{\{1\}}}$ and its maximal ideal $\mathfrak{p} = \mathcal{O}_{A^{\{0\}}} \times \mathfrak{p}' \times \mathcal{O}_{A^{\{1\}}}$. Set $I = \mathcal{O}_{A^{\{0\}}} \times I' \times \mathcal{O}_{A^{\{1\}}}$. Define $\widetilde{S}$ as the order in $\widetilde{A}$ satisfying $\widetilde{S} \otimes_{\mathbb{Z}} \mathbb{Z}_p \simeq S$, and $\widetilde{\mathfrak{p}}$ as the prime of $\widetilde{S}$ such that $\widetilde{\mathfrak{p}} \otimes_{\mathbb{Z}} \mathbb{Z}_p \simeq \mathfrak{p}$, and $\widetilde{I}$ as the fractional $\widetilde{S}$-ideal such that $\widetilde{I} \otimes_{\mathbb{Z}} \mathbb{Z}_p \simeq I$, all using (ii). Then we have canonical isomorphisms

$$\widetilde{S}_{\widetilde{\mathfrak{p}}} \simeq S_{\mathfrak{p}} \simeq S'_{\mathfrak{p}'} \quad \text{and} \quad \widetilde{I}_{\widetilde{\mathfrak{p}}} \simeq I_{\mathfrak{p}} \simeq I'_{\mathfrak{p}'}.$$

With this convention we have $\widetilde{\mathcal{O}}_{A'} = \mathcal{O}_{\widetilde{A}}$.

Lemma 6.3. *Let $\widetilde{\mathfrak{P}}_{\nu,1}, \dots, \widetilde{\mathfrak{P}}_{\nu,g_\nu}$ be the maximal ideals of $\mathcal{O}_{\widetilde{A}}$ extending a place ν of E_p. Fix an index i and consider the natural surjective ring homomorphism*

$$\varphi : \mathcal{O}_{\widetilde{A}} \twoheadrightarrow \frac{\mathcal{O}_{\widetilde{A}}}{\widetilde{\mathfrak{P}}_{\nu,i}^2 \cdot \prod_{j \neq i} \widetilde{\mathfrak{P}}_{\nu,j}} \simeq \frac{\mathcal{O}_{\widetilde{A}}}{\widetilde{\mathfrak{P}}_{\nu,i}^2} \times \prod_{i \neq j} \frac{\mathcal{O}_{\widetilde{A}}}{\widetilde{\mathfrak{P}}_{\nu,j}}$$

Pick $b_i \in \widetilde{\mathfrak{P}}_{\nu,i} \setminus \widetilde{\mathfrak{P}}_{\nu,i}^2$ and let $t_{\nu,i}$ be an element of $\mathcal{O}_{\widetilde{A}}$ such that $\varphi(t_{\nu,i})$ equals the class of b_i in the i-th component and the class of 1 in every other component. Then the image of $t_{\nu,i}$ via the natural ring homomorphism $\mathcal{O}_{\widetilde{A}} \to \mathcal{O}_{\widetilde{A},\widetilde{\mathfrak{P}}_{\nu,j}} \simeq \mathcal{O}_{A,\mathfrak{P}_{\nu,j}}$ is a uniformizer if $j = i$ and a unit otherwise.

Proof. Omitted. □

6.2 Step 1: W'_R-isomorphism classes

Lemma 6.4. *Let $\mathcal{S}$ be the set of primes $\mathfrak{P}$ of W'_R. Then we have a natural bijection*

$$\mathcal{W}(W'_R) \longleftrightarrow \prod_{\mathfrak{P} \in \mathcal{S}} \mathcal{W}_{\widetilde{\mathfrak{P}}}(\widetilde{W}_R).$$

Proof. Note that W'_R is canonically isomorphic to the direct product of the completions $W_{R,\mathfrak{P}}$ where $\mathfrak{P}$ ranges over the set $\mathcal{S}$. The statement follows from the canonical isomorphism $\widetilde{W}_{R,\widetilde{\mathfrak{P}}} \simeq W_{R,\mathfrak{P}}$, see Remark 6.2.(ii), and from Remark 3.5. □

Building on the previous lemma, in the following algorithm we will compute the isomorphism classes of fractional W'_R-ideals, concluding the first step of the computation of isomorphism classes of $W'_R\{F', V'\}$-ideals.

Algorithm 1.
Input: The order R.
Output: A set of fractional $\widetilde{W}_R$-ideals representing $\mathcal{W}(W'_R)$.

(1) Compute the orders $\mathcal{O}_{\widetilde{A}}$ and $\widetilde{W}_R$;

(2) Compute the set $\widetilde{\mathfrak{p}}_1, \dots, \widetilde{\mathfrak{p}}_n$ of maximal ideals of $\widetilde{W}_R$ that lie below the maximal ideals of $\mathcal{O}_{\widetilde{A}}$ extending the places of E_p with slope in $(0, 1)$;

(3) Set $k = \mathrm{val}_p([\mathcal{O}_{\widetilde{A}} : \widetilde{W}_R])$;

(4) For each $\widetilde{\mathfrak{p}}_i$ compute a set of representatives $\mathcal{W}_i$ of $\mathcal{W}(\widetilde{W}_R + \widetilde{\mathfrak{p}}_i^k \mathcal{O}_{\widetilde{A}})$, for example, using [23, Algorithm ComputeW];

(5) Construct a set of representatives of $\mathcal{W}(W'_R)$ by combining the sets $\mathcal{W}_1, \dots, \mathcal{W}_n$, using Lemma 3.7.

Theorem 6.5. *Algorithm 1 is correct.*

Proof. This is an immediate consequence of Lemma 6.4 and Proposition 3.10. □

6.3 Step 2: Δ'-isomorphism classes

In this section, given a fractional W_R'-ideal I, we will denote by $[I]_{W_R'}$ its class in $\mathcal{W}(W_R')$ and by $[I]_{\Delta'}$ its Δ'-isomorphism class. Since every Δ'-isomorphism is also a W_R'-linear isomorphism, we see that $[I]_{W_R'}$ splits into a disjoint union of Δ'-isomorphism classes. We denote by e_I the extension map $[I']_{\Delta'} \mapsto [I'\mathcal{O}_A']_{\Delta'}$ from the set of Δ'-isomorphism classes of fractional W_R'-ideals that are W_R'-isomorphic to I, to the set of Δ'-isomorphism classes of fractional $\mathcal{O}_A$-ideals.

In the next proposition, we describe the fibers of the extension map $e_I : [I']_{\Delta'} \mapsto [I'\mathcal{O}_A']_{\Delta'}$. Then we include a series of results dedicated to explicitly computing these fibers using global elements. The whole procedure to obtain Δ'-isomorphism classes of W_R'-ideals is wrapped up in Algorithm 2 below.

Proposition 6.6. *Let I be a fractional W_R'-ideal. Set $S = (I : I)$ and $J = I\mathcal{O}_{A'}$. The association $\gamma \mapsto \gamma I$ for $\gamma \in \mathcal{O}_{A'}^\times$ induces a free and transitive group action of $\mathcal{O}_{A'}^\times / S^\times \Delta'(\mathcal{O}_{E_p'}^\times)$ on the fiber $e_I^{-1}([J]_{\Delta'})$.*

Proof. If $\gamma \in \mathcal{O}_{A'}^\times$ then $\gamma I\mathcal{O}_{A'} = J$. Now $\gamma I = I$ if and only if $\gamma \in S^\times$, and γI is Δ'-isomorphic to I if and only if $\gamma \in \Delta'({E_p'}^\times)$. We claim that

$$\mathcal{O}_{A'}^\times \cap S^\times \Delta'({E_p'}^\times) = S^\times \Delta'(\mathcal{O}_{E_p'}^\times).$$

Recall that $A' = \prod_\nu A_\nu$ where ν runs over the places of E_p' and that A_ν is a direct product of g_ν-copies of LE_ν. We denote here by val_ν both the valuation on E_ν and its (unramified) extension to LE_ν. Indeed, for any $y \in \mathcal{O}_{A'}^\times \cap S^\times \Delta'({E_p'}^\times)$ there exist $s \in S^\times$ and $x \in \Delta'({E_p'}^\times)$ such that $y = sx \in \mathcal{O}_{A'}^\times$. Then $0 = \mathrm{val}_\nu(s_{\nu,i}x_{\nu,i}) = \mathrm{val}_\nu(x_{\nu,i})$ for each ν and each $0 \le i \le g_\nu$, and hence $x_{\nu,i} \in \mathcal{O}_{E_\nu'}^\times$. Note that $x_{\nu,i} = x_{\nu,j}$ for all i, j by assumption, so $x \in \Delta'(\mathcal{O}_{E_p'}^\times)$. This shows that the group action is well-defined and free.

Pick $[I_0]_{\Delta'}$ in $e_I^{-1}([J]_{\Delta'})$. By assumption there are $\delta \in {A'}^\times$ and $\beta \in \Delta({E_p'}^\times)$ such that $I_0 = \delta I$ and $I_0\mathcal{O}_{A'} = \beta J$. Put $\gamma = \delta/\beta$. By construction, we have $\gamma I = \beta^{-1} I_0$ which shows that $[\gamma I]_{\Delta'} = [I_0]_{\Delta'}$. So, to conclude that the group action is also transitive, it suffices to show that $\gamma \in \mathcal{O}_{A'}^\times$, as we now do. Recall that by hypothesis we have $J = I\mathcal{O}_{A'}$. Hence

$$\gamma I\mathcal{O}_{A'} = \frac{\delta}{\beta} I\mathcal{O}_{A'} = \frac{1}{\beta} I_0\mathcal{O}_{A'} = J = I\mathcal{O}_{A'},$$

which implies that $\gamma \in \mathcal{O}_{A'}^\times$. □

In Algorithm 2 below, we will use that, given an overorder S of W_R' the quotient $\mathcal{O}_{A'}^\times / S^\times \Delta(\mathcal{O}_{E_p'}^\times)$ is the cokernel of the inclusion

$$\frac{S^\times \Delta'(\mathcal{O}_{E_p'}^\times)}{S^\times} \longrightarrow \frac{\mathcal{O}_{A'}^\times}{S^\times},$$

as we now show.

Lemma 6.7. *The subgroup $H = W_R^\times \Delta'(\mathcal{O}_{E_p'}^\times)/W_R^\times$ is generated by the elements of $\mathcal{O}_{A'}^\times / W_R^\times$ fixed by the action induced by the automorphisms $\sigma\colon A_\nu \to A_\nu$ for ν ranging over the places of E_p with $s(\nu) \in (0,1)$.*

Let S be any overorder of W_R. The subgroup $S^\times \Delta'(\mathcal{O}_{E_p'}^\times)/S^\times$ is generated by the image of H via the natural projection $\mathcal{O}_{A'}^\times / W_R^\times \twoheadrightarrow \mathcal{O}_{A'}^\times / S^\times$.

Proof. Recall from Equation (11) that σ acts on $A_\nu = \oplus LE_\nu$ as a cyclic permutation on the g_ν copies of LE_ν followed by τ_ν on the last component. Therefore, the elements of $\mathcal{O}_{A_\nu}^\times$ fixed by σ are those whose components are all the same, hence in the image of Δ', and are fixed by τ_ν. This is precisely $\Delta'(\mathcal{O}_{E_\nu'}^\times)$. The first statement then follows since σ acts also on $W_{R,\nu}$. The second statement is a consequence of the fact that we have $S^\times W_R^\times \Delta'(\mathcal{O}_{E_p'}^\times) = S^\times \Delta'(\mathcal{O}_{E_p'}^\times)$. □

In what follows, we will describe how to compute $\mathcal{O}_{A'}^\times / S^\times$, and consequently also $\mathcal{O}_{A'}^\times / S^\times \Delta(\mathcal{O}_{E_p'}^\times)$, using global representatives; see Remark 6.9 for a summary.

Lemma 6.8. *Let $\widetilde{\mathfrak{f}}$ be the conductor of $\widetilde{S}$ in $\mathcal{O}_{\widetilde{A}}$ and $\widetilde{\mathfrak{p}}_1, \ldots, \widetilde{\mathfrak{p}}_r$ the maximal ideals of $\widetilde{S}$ corresponding to the finitely many maximal ideals of S. For $i = 1 \ldots, r$, set $k_i = \mathrm{val}_p(|\widetilde{S}/\widetilde{\mathfrak{f}}|)/\mathrm{val}_p(|\widetilde{S}/\widetilde{\mathfrak{p}}_i|)$. Then the natural ring homomorphism*

$$\widetilde{S} \longrightarrow \frac{\mathcal{O}_{\widetilde{A}}}{\widetilde{\mathfrak{f}} + \prod_{i=1}^{r} \widetilde{\mathfrak{p}}_i^{k_i} \mathcal{O}_{\widetilde{A}}}$$

has kernel $\widetilde{\mathfrak{f}} + \prod_{i=1}^{r} \widetilde{\mathfrak{p}}_i^{k_i}$ and it induces a group isomorphism

$$\frac{\mathcal{O}_{A'}^{\times}}{S^{\times}} \simeq \frac{\left(\dfrac{\mathcal{O}_{\widetilde{A}}}{\widetilde{\mathfrak{f}} + \prod_{i=1}^{r} \widetilde{\mathfrak{p}}_i^{k_i} \mathcal{O}_{\widetilde{A}}}\right)^{\times}}{\left(\dfrac{\widetilde{S}}{\widetilde{\mathfrak{f}} + \prod_{i=1}^{r} \widetilde{\mathfrak{p}}_i^{k_i}}\right)^{\times}}.$$

Proof. By [15, Lemma 2.3], for $i = 1, \ldots, r$, we have $\widetilde{\mathfrak{p}}_i^{k_i} \widetilde{S}_{\widetilde{\mathfrak{p}}_i} \subseteq \widetilde{\mathfrak{f}}_{\widetilde{\mathfrak{p}}_i}$ and hence also $\widetilde{\mathfrak{p}}_i^{k_i} \mathcal{O}_{\widetilde{A},\widetilde{\mathfrak{p}}_i} \subseteq \widetilde{\mathfrak{f}}_{\widetilde{\mathfrak{p}}_i} \mathcal{O}_{A,\widetilde{\mathfrak{p}}_i} = \widetilde{\mathfrak{f}}_{\widetilde{\mathfrak{p}}_i}$. The kernel of the homomorphism in the statement is

$$\widetilde{S} \cap (\widetilde{\mathfrak{f}} + \prod_{i=1}^{r} \widetilde{\mathfrak{p}}_i^{k_i} \mathcal{O}_{\widetilde{A}});$$

we now show that it equals $\widetilde{\mathfrak{f}} + \prod_{i=1}^{r} \widetilde{\mathfrak{p}}_i^{k_i}$. It suffices to check the equality locally at every maximal ideal of $\widetilde{S}$. Let $\mathfrak{p}$ be a maximal ideal not in the set $\{\widetilde{\mathfrak{p}}_1, \ldots, \mathfrak{p}_r\}$. Then

$$\left(\widetilde{\mathfrak{f}} + \prod_{i=1}^{r} \widetilde{\mathfrak{p}}_i^{k_i}\right)_{\mathfrak{p}} = \widetilde{S}_{\mathfrak{p}} = \left(\widetilde{S} \cap (\widetilde{\mathfrak{f}} + \prod_{i=1}^{r} \widetilde{\mathfrak{p}}_i^{k_i} \mathcal{O}_{\widetilde{A}})\right)_{\mathfrak{p}},$$

while

$$\left(\widetilde{\mathfrak{f}} + \prod_{i=1}^{r} \widetilde{\mathfrak{p}}_i^{k_i}\right)_{\widetilde{\mathfrak{p}}_i} = \widetilde{\mathfrak{f}}_{\widetilde{\mathfrak{p}}_i} = \left(\widetilde{S} \cap (\widetilde{\mathfrak{f}} + \prod_{i=1}^{r} \widetilde{\mathfrak{p}}_i^{k_i} \mathcal{O}_{\widetilde{A}})\right)_{\widetilde{\mathfrak{p}}_i}$$

for $i = 1, \ldots, r$.

The argument used above shows that, for each i, we have isomorphisms

$$\frac{S_{\mathfrak{p}_i}}{\mathfrak{f}_{\mathfrak{p}_i}} \simeq \frac{\widetilde{S}_{\widetilde{\mathfrak{p}}_i}}{\widetilde{\mathfrak{f}}_{\widetilde{\mathfrak{p}}_i}} \simeq \frac{\widetilde{S}_{\widetilde{\mathfrak{p}}_i}}{\left(\widetilde{\mathfrak{f}} + \prod_{i=1}^{r} \widetilde{\mathfrak{p}}_i^{k_i}\right)_{\widetilde{\mathfrak{p}}_i}}, \tag{19}$$

inducing

$$\frac{\mathcal{O}_{A',\mathfrak{p}_i}}{\mathfrak{f}_{\mathfrak{p}_i}} \simeq \frac{\mathcal{O}_{\widetilde{A},\widetilde{\mathfrak{p}}_i}}{\widetilde{\mathfrak{f}}_{\widetilde{\mathfrak{p}}_i}} \simeq \frac{\mathcal{O}_{\widetilde{A},\widetilde{\mathfrak{p}}_i}}{\left(\widetilde{\mathfrak{f}} + \prod_{i=1}^{r} \widetilde{\mathfrak{p}}_i^{k_i} \mathcal{O}_{\widetilde{A}}\right)_{\widetilde{\mathfrak{p}}_i}}. \tag{20}$$

For the second part of the statement, we observe that the decomposition $S \simeq \oplus_{\mathfrak{p}} S_{\mathfrak{p}}$, where the direct sum is over the finitely many maximal ideals $\mathfrak{p}$ of S, induces a decomposition $\mathcal{O}_{A'} \simeq \oplus_{\mathfrak{p}} \mathcal{O}_{A',\mathfrak{p}}$. If $\mathfrak{p}$ does not lie above the conductor $\mathfrak{f}$ of S in $\mathcal{O}_{A'}$ then $S_{\mathfrak{p}} = \mathcal{O}_{A',\mathfrak{p}}$. Hence we have the following isomorphism:

$$\frac{\mathcal{O}_{A'}^{\times}}{S^{\times}} \simeq \bigoplus_{\mathfrak{f} \subseteq \mathfrak{p}} \frac{\mathcal{O}_{A',\mathfrak{p}}^{\times}}{S_{\mathfrak{p}}^{\times}}. \tag{21}$$

For $\mathfrak{p}$ lying above the conductor $\mathfrak{f}$, there is a natural bijection between the finite set of primes of $\mathcal{O}_{A',\mathfrak{p}}$ and the set of maximal ideals of $\mathcal{O}_{A',\mathfrak{p}}/\mathfrak{f}_{\mathfrak{p}}$, where $\mathfrak{f}_{\mathfrak{p}}$ is the completion of $\mathfrak{f}$ at $\mathfrak{p}$. Hence the map

$$\mathcal{O}_{A',\mathfrak{p}}^{\times} \to \left(\frac{\mathcal{O}_{A',\mathfrak{p}}}{\mathfrak{f}_{\mathfrak{p}}}\right)^{\times}$$

induced by taking quotients is surjective. The composition

$$\mathcal{O}_{A',\mathfrak{p}}^{\times} \to \left(\frac{\mathcal{O}_{A',\mathfrak{p}}}{\mathfrak{f}_{\mathfrak{p}}}\right)^{\times} \to \frac{(\mathcal{O}_{A',\mathfrak{p}}/\mathfrak{f}_{\mathfrak{p}})^{\times}}{(S_{\mathfrak{p}}/\mathfrak{f}_{\mathfrak{p}})^{\times}}$$

has kernel $S_{\mathfrak{p}}^{\times}$. Therefore, by Equation (21), we get

$$\frac{\mathcal{O}_{A'}^{\times}}{S^{\times}} \simeq \bigoplus_{\mathfrak{f}\subseteq\mathfrak{p}} \frac{(\mathcal{O}_{A',\mathfrak{p}}/\mathfrak{f}_{\mathfrak{p}})^{\times}}{(S_{\mathfrak{p}}/\mathfrak{f}_{\mathfrak{p}})^{\times}}. \tag{22}$$

We conclude by combining Equations (19), (20) and (22) and the fact that we have canonical ring isomorphisms

$$\frac{\widetilde{S}}{\widetilde{\mathfrak{f}}+\prod_{i=1}^{r}\widetilde{\mathfrak{p}}_i^{k_i}} \simeq \prod_{i=1}^{r} \frac{\widetilde{S}_{\widetilde{\mathfrak{p}}_i}}{\left(\widetilde{\mathfrak{f}}+\prod_{i=1}^{r}\widetilde{\mathfrak{p}}_i^{k_i}\right)_{\widetilde{\mathfrak{p}}_i}}$$

and

$$\frac{\mathcal{O}_{\widetilde{A}}}{\widetilde{\mathfrak{f}}+\prod_{i=1}^{r}\widetilde{\mathfrak{p}}_i^{k_i}\mathcal{O}_{\widetilde{A}}} \simeq \prod_{i=1}^{r} \frac{\mathcal{O}_{\widetilde{A},\widetilde{\mathfrak{p}}_i}}{\left(\widetilde{\mathfrak{f}}+\prod_{i=1}^{r}\widetilde{\mathfrak{p}}_i^{k_i}\mathcal{O}_{\widetilde{A}}\right)_{\widetilde{\mathfrak{p}}_i}}.$$

□

Remark 6.9. Lemma 6.8 gives a method to describe $\mathcal{O}_{A'}^{\times}/S^{\times}$ using $\mathbb{Z}$-lattices. Algorithms to concretely compute the quotient can be found in [12] and [17]. As pointed out in Remark 6.2.(iv), the action of σ can be realized on the $\mathbb{Z}$-order $\mathcal{O}_{\widetilde{A}}$. Hence, using Lemma 6.7, we get a method to compute the group $\mathcal{O}_{A'}^{\times}/S^{\times}\Delta(\mathcal{O}_{E'_p}^{\times})$ together with a set of generators in $\mathcal{O}_{\widetilde{A}}$ using only $\mathbb{Z}$-lattices. This is desirable in order to avoid precision issues that could arise from working with $\mathbb{Z}_p$-lattices.

For the remainder of the article, we fix F' of W-type (cf. Definition 4.4). Thanks to Proposition 4.19, we understand the $W'_R\{F',V'\}$-ideals with maximal endomorphism ring. We now show in Proposition 6.10 that e_I sends $W'_R\{F',V'\}$-ideals to $W'_R\{F',V'\}$-ideals. This implies that, in order to compute all $W'_R\{F',V'\}$-ideals, it suffices to consider the fibers of $W'_R\{F',V'\}$-ideals with multiplicator ring $\mathcal{O}'_A$. This fact will be used in Algorithm 2 below.

Proposition 6.10. *Let I be a fractional W'_R-ideal. If I is a $W'_R\{F',V'\}$-ideal, then $I\mathcal{O}_{A'}$ is also a $W'_R\{F',V'\}$-ideal.*

Proof. Any element of $I\mathcal{O}_{A'}$ can be written as a finite sum $z=\sum_i x_i a_i$ with $x_i\in I$ and $a_i\in\mathcal{O}_{A'}$. Recall that F' is of the form $z\mapsto \alpha z^{\sigma}$ on each component A_ν. The action of σ is multiplicative, so we can write

$$F'(z)=\sum_i F'(x_i a_i)=\sum_i F'(x_i)\sigma(a_i).$$

Since $F'(x_i)\in I$ by assumption and $\sigma(a_i)\in\mathcal{O}_{A'}(\simeq W\otimes\mathcal{O}_{E'_p})$ we see that $F'(z)\in I\mathcal{O}_{A'}$. Hence

$$V'(z)=\sum_i V'(x_i a_i)=\sum_i V'(x_i)\sigma^{-1}(a_i).$$

Now, $V'(x_i)\in I$ by assumption and $\sigma^{-1}(a_i)\in\mathcal{O}_{A'}$. So $V'(z)\in I\mathcal{O}_{A'}$. This shows that $I\mathcal{O}_{A'}$ is a $W'_R\{F',V'\}$-ideal. □

We are now ready to combine all the results presented in this section into an algorithm to compute Δ'-isomorphism classes.

Algorithm 2.
Input: A set of fractional $\widetilde{W}_R$-ideals $\widetilde{I}_1,\dots,\widetilde{I}_n$ representing the W'_R-isomorphism classes of all fractional W'_R-ideals.
Output: A set of fractional $\widetilde{W}_R$-ideals representing the Δ'-isomorphism classes of all fractional W'_R-ideals whose extension to $\mathcal{O}_{A'}$ is in Υ (see Definition 4.20).

(1) For each place ν of E_p of slope in $(0,1)$, compute the maximal ideals $\widetilde{\mathfrak{P}}_{\nu,1},\dots,\widetilde{\mathfrak{P}}_{\nu,g_\nu}$ of $\mathcal{O}_{\widetilde{A}}$ extending ν; see Remark 6.2.(v). For each i, compute an element $t_{\nu,i}$ defined as in Lemma 6.3.

(2) Use Proposition 4.19 to compute, up to Δ'-isomorphism, all $W'\{F',V'\}$-ideals $J_1,\dots,J_m$ having maximal multiplicator ring $\mathcal{O}_{A'}$. Each J_j is stored as a tuple of vectors of the form $(\varepsilon_{j,\nu,1},\dots,\varepsilon_{j,\nu,g_\nu})_\nu$ (as in Υ).

(3) For each $\widetilde{I}_i$, do the following:

(3.a) Compute the multiplicator ring $\widetilde{S}$ of $\widetilde{I}_i$.

(3.b) Compute the extension $\widetilde{J} = \widetilde{I}_i\mathcal{O}_{\widetilde{A}}$.

(3.c) Compute the factorization

$$\widetilde{J} = \widetilde{J}^{\dagger} \times \prod_{\nu} \prod_{i=1}^{g_\nu} \widetilde{\mathfrak{P}}_{\nu,i}^{\eta_{\nu,i}},$$

where ν runs over the places of E_p of slope in $(0,1)$, and $\widetilde{J}^{\dagger}$ is the product of all the other maximal ideals.

(3.d) For each $j = 1, \ldots, m$, set $\delta_j = \prod_\nu \prod_{i=1}^{g_\nu} t_{\nu,i}^{\eta_{\nu,i} - \varepsilon_{j,\nu,i}}$.

(3.e) Use Remark 6.9 to compute $\gamma_1, \ldots, \gamma_r$ in $\mathcal{O}_{\widetilde{A}}$ representing the elements of $\mathcal{O}_{A'}^{\times}/S^{\times}\Delta(\mathcal{O}_{E'_p}^{\times})$.

(3.f) Define the set of fractional $\widetilde{W}_R$-ideals $\mathcal{I}_i = \{\delta_j^{-1}\gamma_k\widetilde{I}_i \ : 1 \le j \le m, 1 \le k \le r\}$.

(4) Return $\bigcup_{i=1}^{n} \mathcal{I}_i$.

Theorem 6.11. *Algorithm 2 is correct.*

Proof. Let $L, L' \in \bigcup_{i=1}^{n} \mathcal{I}_i$ with $L \neq L'$. If $L \in \mathcal{I}_i$ and $L' \in \mathcal{I}_{i'}$ for indices $1 \le i < i' \le n$ then L and L' are not Δ'-isomorphic since they are not W'_R-isomorphic. If L and L' belong to the same $\mathcal{I}_i$ then they are not Δ'-isomorphic by Proposition 6.6. Hence, all fractional W'_R-ideals in $\bigcup_{i=1}^{n} \mathcal{I}_i$ are pairwise non-Δ'-isomorphic.

To conclude we need to show that $\bigcup_{i=1}^{n} \mathcal{I}_i$ contains representatives of all Δ'-isomorphism class of W'_R-ideals whose extension to $\mathcal{O}'_A$ is a $W'_R\{F', V'\}$-ideal. For each $\widetilde{I}_i$ denote by $\widetilde{J}_i^{\dagger\dagger}$ the part of the factorization of $\widetilde{I}_i\mathcal{O}_{\widetilde{A}}$ over the maximal ideals $\widetilde{\mathfrak{P}}_{\nu,1}, \ldots, \widetilde{\mathfrak{P}}_{\nu,g_\nu}$. Note that $\widetilde{J}_i^{\dagger\dagger}$ is isomorphic to $\widetilde{I}_i\mathcal{O}_{\widetilde{A}}$ locally at every maximal ideal $\mathfrak{P}_{\nu,k}$. By the way each $t_{\nu,i}$ is constructed, we get that J_i and $\delta_j^{-1}\widetilde{J}_i^{\dagger\dagger}$ are equal locally at every maximal ideal $\mathfrak{P}_{\nu,k}$. Hence, the result follows from Propositions 4.19, 6.6 and 6.10. □

Remark 6.12. In order to perform Step (3.e) in Algorithm 2, following Remark 6.9, we need to compute the action of $\widetilde{\sigma}$ on the finite ring

$$\mathfrak{o}_A := \frac{\mathcal{O}_{\widetilde{A}}}{\widetilde{\mathfrak{f}} + \prod_{i=1}^{r} \widetilde{\mathfrak{p}}_i^{k_i}\mathcal{O}_{\widetilde{A}}}.$$

Set $\mathfrak{o}_L = \mathcal{O}_{\widetilde{L}}/(p\mathcal{O}_{\widetilde{L}})^m$, where m is defined by $|\mathfrak{o}_A| = |\mathcal{O}_{\widetilde{L}}/(p\mathcal{O}_{\widetilde{L}})|^m$. By Remark 6.2.(iv), the finite ring $\mathfrak{o}_A$ is an $\mathfrak{o}_L$-algebra. If $b_1, \ldots, b_{2g}$ is the image of a $\mathbb{Z}$-basis of $\mathcal{O}_E$ in $\mathfrak{o}_A$ then we can give a σ-equivariant presentation of $\mathfrak{o}_A$ as an $\mathfrak{o}_L$-algebra by

$$\begin{aligned} \mathfrak{o}_L \times \ldots \times \mathfrak{o}_L &\longrightarrow \mathfrak{o}_A \\ (c_1, \ldots, c_{2g}) &\longmapsto \sum_{i=1}^{2g} c_i b_i. \end{aligned}$$

Hence, in order to compute the action of $\widetilde{\sigma}$ on $\mathfrak{o}_A$ it suffices to compute an approximation of the (p-adic) Frobenius automorphism of L on $\mathfrak{o}_L$. This can be done as follows. Let u be a lift in $\mathfrak{o}_L$ of a generator of $\left(\mathcal{O}_{\widetilde{L}}/p\mathcal{O}_{\widetilde{L}}\right)^{\times}$. Compute u^{q^i} for $i > 0$ until $u^{q^i} = u^{q^{i+1}}$ and set $z = u^{q^i}$. Then z is the image of an inertial element of $\mathcal{O}_L \simeq \mathbb{Z}_p[z]$ in $\mathfrak{o}_L$. Hence, by computing an explicit isomorphism $\mathbb{Z}_p[z]/(p\mathbb{Z}[z])^m \simeq \mathfrak{o}_L$, we can compute the action of σ on $\mathfrak{o}_L$ by pushing forward the action of σ on $\mathbb{Z}_p[z]$ which is given by $z \mapsto z^p$.

Note that this construction does not require $\widetilde{L}$ to be normal; cf Remark 6.2.(iv). We stress that the output of Step (3.e) in Algorithm 2 is independent of choice of the approximation of $\widetilde{\sigma}$ we computed, which is certainly not unique.

Proposition 6.13 below shows that Δ'-isomorphism classes are the orbits of the action of a group G' on the W'_R-isomorphism classes. In particular, each W'_R-isomorphism class is a disjoint union of Δ'-isomorphism classes. However, the group G' is finite only when $g_\nu = 1$ for every place ν of slope in $(0,1)$. And only under this assumption, there is exactly one Δ'-isomorphism class of fractional $W'_R\{F', V'\}$-ideals I with $(I : I) = \mathcal{O}_{A'}$, cf. [33, p. 546]. That is, since there is only one fiber of the extension map to consider, Corollary 6.14 below can be viewed as a special case of the method presented above. We will not use Proposition 6.13 and Corollary 6.14 in the rest of the paper.

Proposition 6.13. *Let I be a fractional W_R'-ideal with multiplicator ring S. Then $[I]_{W_R'}$ is a disjoint union of Δ'-isomorphism classes, which are in bijection with the orbits of the natural action of the group $G' := {A'}^\times/S^\times\Delta'({E'_p}^\times)$ on $[I]_{W_R'}$.*

Proof. Recall that $[I]_{W_R'}$ splits into a disjoint union of Δ'-isomorphism classes. The quotient ${A'}^\times/S^\times$ acts freely and transitively on $[I]_{W_R'}$. Since Δ'-linear isomorphisms are given by multiplication by elements of $\Delta'({E'_p}^\times)$, the bijection between ${A'}^\times/S^\times\Delta'({E'_p}^\times)$ and the Δ'-isomorphism classes in $[I]_{W_R'}$ follows. □

Corollary 6.14. *If $g_\nu = 1$ for every ν with $s(\nu) \in (0,1)$ then the quotient ${A'}^\times/S^\times\Delta'({E'_p}^\times)$ is finite, and isomorphic to*

$$\frac{\mathcal{O}_{A'}^\times}{S^\times\Delta'(\mathcal{O}_{E'_p}^\times)}.$$

If moreover $S = \mathcal{O}_{A'}$, then there is only one W_R'-isomorphism class of ideals I with $(I:I) = S$ and every representative of this class is a $W_R'\{F', V'\}$-ideal.

Proof. We consider $\Delta'(E'_p) = E'_p \subseteq A'$ by slight abuse of notation. Since $g_\nu = 1$, we also have that $A_\nu = LE_\nu$, which is an unramified field extension of E_ν. Hence $A_\nu^\times = \mathcal{O}_{A_\nu}^\times E_\nu^\times$. Since this is the case for every ν with slope in $(0,1)$, we get ${A'}^\times = \mathcal{O}_{A'}^\times {E'_p}^\times$. Therefore, we have that

$$\frac{{A'}^\times}{S^\times {E'_p}^\times} = \frac{\mathcal{O}_{A'}^\times {E'_p}^\times}{S^\times {E'_p}^\times} = \frac{\mathcal{O}_{A'}^\times S^\times {E'_p}^\times}{S^\times {E'_p}^\times} \simeq \frac{\mathcal{O}_{A'}^\times}{\mathcal{O}_{A'}^\times \cap S^\times {E'_p}^\times} = \frac{\mathcal{O}_{A'}^\times}{S^\times \mathcal{O}_{E'_p}^\times},$$

which is finite.

Finally, assume that $S = \mathcal{O}_{A'}$. There is only W_R'-isomorphism class of fractional $\mathcal{O}_{A'}$-ideals. To conclude the proof, we show that every representative I of this class is a $W_R'\{F', V'\}$-ideal. Let $\gamma \in {A'}^\times$. We write $\tau' = \oplus_\nu \tau_\nu$ with τ_ν as above. Then

$$F'(\gamma I) = \gamma^{\tau'} F'(I) \subseteq \gamma I \iff F'(I) \subseteq \frac{\gamma}{\gamma^{\tau'}} I.$$

Since $\gamma/\gamma^{\tau'}$ has valuation 0, it is an element of $\mathcal{O}_{A'}^\times = S^\times$; equivalently, we have $\gamma/\gamma^{\tau'} I = I$. □

6.4 Step 3: Stability under the action of F and V

Algorithm 2 returns a list of fractional $\widetilde{W}_R$-ideals representing the Δ'-isomorphism classes of fractional W_R'-ideals. Consider the class $[I]_{\Delta'}$ represented by $\widetilde{I}$, which we can assume to be contained in $\mathcal{O}_{\widetilde{A}}$. We want to determine whether $[I]_{\Delta'}$ consists of $W_R'\{F', V'\}$-ideals. Since F' and V' cannot be realized on the $\mathbb{Q}$-algebra $\widetilde{A}$, we cannot compute $\widetilde{F'I}$ and $\widetilde{V'I}$ directly from $\widetilde{I}$. The first step is to reduce to working in a finite quotient.

Lemma 6.15. *Fix a $W_R'\{F', V'\}$-ideal J and a fractional W_R'-ideal $I \subseteq J$. Let $\widetilde{J}$, $\widetilde{I}$, $\widetilde{V'I}$ and $\widetilde{F'I}$ be defined as in Remark 6.2.(vi). Let N be the exponent of the finite quotient $\widetilde{J}/\widetilde{I}$. Let m be an integer such that $m \geq \mathrm{val}_p(N)$. Denote by $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ the maximal ideals of W_R which lie below the maximal ideals of $\mathcal{O}_A$ above the places of E of slope in $(0,1)$. For each $i = 1, \ldots, n$, let m_i be a positive integer such that $|J/p^m J| \leq |W_R/\mathfrak{p}_i|^{m_i}$. Then the following statements are equivalent:*

(i) $[I]_{\Delta'}$ consists of $W_R'\{F', V'\}$-ideals;

(ii) $I = I + F'I + V'I$;

(iii) $\widetilde{I} = \widetilde{I} + \widetilde{F'I} + \widetilde{V'I}$;

(iv) The images of $\widetilde{I}$ and $\widetilde{I} + \widetilde{F'I} + \widetilde{V'I}$ in the finite quotient $\widetilde{J}/p^m\widetilde{J}$ are equal;

(v) The images of $\widetilde{I}$ and $\widetilde{I} + \widetilde{F'I} + \widetilde{V'I}$ in the finite quotient $\widetilde{J}/\left(p^m\widetilde{J} + \prod_{i=1}^n \mathfrak{p}_i^{m_i}\widetilde{J}\right)$ are equal.

Proof. The equivalence of (i) and (ii) follows from Corollary 4.8. Consider the finite $\widetilde{W}_R$-module

$$M = \frac{\widetilde{I} + \widetilde{F'I} + \widetilde{V'I}}{\widetilde{I}}.$$

By Remark 6.2.(ii), we have a canonical isomorphism

$$M \simeq \frac{I + F'I + V'I}{I}.$$

Hence (iii) and (ii) are equivalent.

The assumption on m implies that we have inclusions

$$p^m \widetilde{J} \subseteq \widetilde{I} \subseteq \widetilde{I} + \widetilde{F'I} + \widetilde{V'I} \subseteq \widetilde{J}.$$

Hence, conditions (iii) and (iv) are equivalent.

Set $Q = \widetilde{J}/p^m\widetilde{J}$. The splitting of $W_R \simeq W_R^{\{0\}} \times W_R' \times W_R^{\{1\}}$ induces a decomposition $Q \simeq Q^{\{0\}} \oplus Q' \oplus Q^{\{1\}}$. Observe that $Q' \simeq \widetilde{J}/\left(p^m\widetilde{J} + \prod_{i=1}^n \mathfrak{p}_i^{m_i}\widetilde{J}\right)$. Hence (iv) implies (v). The converse follows from Remark 6.2.(vi), which states that the (0)-parts (resp. (1)-parts) of $\widetilde{I}$ and $\widetilde{I} + \widetilde{F'I} + \widetilde{V'I}$ coincide. □

The next lemma will be used in Algorithm 3 below to construct a presentation of F_ν on a finite quotient of the form

$$\prod_{i=1}^{g_\nu} \frac{\mathcal{O}_{A_\nu}}{\mathfrak{P}_{\nu,i}^m} \simeq \prod_{i=1}^{g_\nu} \frac{\mathcal{O}_{LE_\nu}}{\mathfrak{p}_{LE_\nu}^m},$$

for m a big enough positive integer.

Lemma 6.16. *Fix an integer $j \geq 1$ and a place ν of E_p. Let t_ν be a uniformizer of E_ν. Let γ_0 be an element of $\mathcal{O}_{LE_\nu}^\times$ such that*

$$N_{LE_\nu/E_\nu}(\gamma_0) - \pi_\nu/t_\nu^{\mathrm{val}_\nu(\pi_\nu)} \in \mathfrak{p}_{E_\nu}^j.$$

Then there exists $\gamma_1 \in \mathfrak{p}_{LE_\nu}^j$ such that

$$N_{LE_\nu/E_\nu}(\gamma_0 + \gamma_1) = \pi_\nu/t_\nu^{\mathrm{val}_\nu(\pi_\nu)}$$

Proof. For ease of notation, set $N = N_{LE_\nu/E_\nu}$. Since $\pi_\nu/t_\nu^{\mathrm{val}_\nu(\pi_\nu)}$ is a unit in $\mathcal{O}_{E_\nu}$ we can write $\pi_\nu/t_\nu^{\mathrm{val}_\nu(\pi_\nu)} = \zeta(1+x)$ for some root of unity ζ and some $x \in \mathfrak{p}_{E_\nu}$. Then there is an $\epsilon_0 \in \mathfrak{p}_{E_\nu}^j$ such that $N(\gamma_0) = \zeta(1 + x + \epsilon_0)$. By [29, Proposition 3, page 82] the norm N surjectively maps $(1+\mathfrak{p}_{LE_\nu}^j)$ onto $(1+\mathfrak{p}_{E_\nu}^j)$. Hence, there is an element $\delta_0 \in \mathfrak{p}_{LE_\nu}^j$ such that $N(1+\delta_0) = 1 + (-\epsilon_0)$. Then $N(\gamma_0(1+\delta_0)) = \zeta(1+x+\epsilon_1)$ with $\epsilon_1 \in \mathfrak{p}_{E_\nu}^{j+1}$ and we can find $\delta_1 \in \mathfrak{p}_{LE_\nu}^{j+1}$ such that $N(1+\delta_1) = 1+(-\epsilon_1)$. Then $N(\gamma_0(1+\delta_0)(1+\delta_1)) = \zeta(1+x+\epsilon_2)$ with $\epsilon_2 \in \mathfrak{p}_{E_\nu}^{j+2}$. Continuing this process (since $\mathcal{O}_{E_\nu}^\times$ and $\mathcal{O}_{LE_\nu}^\times$ are complete with respect to the topology induced by $1+\mathfrak{p}_{E_\nu}^n$ respectively $1+\mathfrak{p}_{LE_\nu}^n$), we find $\delta \in \mathfrak{p}_{E_\nu}^j$ such that $N(\gamma_0(1+\delta)) = \zeta(1+x)$. Setting $\gamma_1 = \gamma_0\delta$ concludes the proof. □

We are now ready to give the algorithm that achieves Step 3, allowing us to compute the isomorphism classes of $W_R'\{F', V'\}$-ideals, for F' of W-type, as described at the beginning of the section. The algorithm determines whether a given W_R'-ideal is a $W_R'\{F', V'\}$-ideal by pushing it into a finite quotient Q_{m_0} which depends on a precision parameter m_0. This parameter is chosen minimally so that we can realize the actions F_{m_0} (resp. V_{m_0}) of F' (resp. V') on Q_{m_0}. For further analysis it is desirable to record F_{m_0} and V_{m_0} together with the output of the algorithm (cf. Remark 6.19).

Algorithm 3.
Input: A set $\mathcal{I} = \{\widetilde{I}_1, \ldots, \widetilde{I}_r\}$ of fractional $\widetilde{W}_R$-ideals representing the Δ'-isomorphism classes of all fractional W_R'-ideals whose extension to $\mathcal{O}_{A'}$ is in Υ (see Definition 4.20).
Output: A set of elements in $\mathcal{I}$, possibly scaled by elements in $\widetilde{\Delta}(E) \subseteq \widetilde{A}$ so that they are contained in $\widetilde{J}$, consisting of representatives of the Δ'-isomorphism classes of $W_R'\{F', V'\}$-ideals.

(1) Pick a $W_R'\{F', V'\}$-ideal J with maximal multiplicator ring $\mathcal{O}_{A'}$ using Proposition 4.19, and compute $\widetilde{J}$.

(2) If necessary, scale $\widetilde{J}$ by multiplying by an element in $\widetilde{\Delta}(E)$ so that $\widetilde{J} \subseteq \mathcal{O}_{\widetilde{A}}$; see Remark 6.20.

(3) If necessary, scale each $\widetilde{I}_k \in \mathcal{I}$ by multiplying by an element in $\widetilde{\Delta}(E)$ so that $\widetilde{I}_k \subseteq \widetilde{J}$; see Remark 6.20.

(4) Set $m_0 = \max\{\mathrm{val}_p(N_k)\}$, where N_k is the exponent of the finite quotient $\widetilde{J}/\widetilde{I}_k$.

(5) For each ν with slope $s(\nu) \in (0,1)$ do the following:

(5.a) Let u_ν be an element of E representing a uniformizer for ν.

(5.b) Compute $w_\nu = \pi / u_\nu^{\mathrm{val}_\nu(\pi)}$.

(5.c) Compute the maximal ideals $\widetilde{\mathfrak{P}}_{\nu,1}, \ldots, \widetilde{\mathfrak{P}}_{\nu,g_\nu}$ of $\mathcal{O}_{\widetilde{A}}$ above ν together with their ramification indices $e_{\nu,1}, \ldots, e_{\nu,g_\nu}$, see Remark 6.2.(v).

(5.d) Set $Q_\nu = \prod_{i=1}^{g_\nu} \mathcal{O}_{\widetilde{A}} / \widetilde{\mathfrak{P}}_{\nu,i}^{e_{\nu,i}(m_0+1)}$.

(5.e) Compute the multiplicative subgroup $U_\nu = \prod_{i=1}^{g_\nu} \left(\mathcal{O}_{\widetilde{A}} / \widetilde{\mathfrak{P}}_{\nu,i}^{e_{\nu,i}(m_0+1)}\right)^\times$ of Q_ν, cf. [12].

(5.f) Compute σ_{Q_ν}, the automorphism of Q_ν induced by $\widetilde{\sigma} : \widetilde{A} \to \widetilde{A}$.

(5.g) Compute the group homomorphism

$$\begin{aligned} \varphi : \left(\mathcal{O}_{\widetilde{A}} / \widetilde{\mathfrak{P}}_{\nu,g_\nu}^{e_{\nu,g_\nu}(m_0+1)}\right)^\times &\longrightarrow U_\nu \longrightarrow U_\nu \\ \gamma &\longmapsto (1, \ldots, 1, \gamma) \\ &\qquad \beta \longmapsto \beta \beta^{\sigma_{Q_\nu}} \cdots \beta^{\sigma_{Q_\nu}^{a-1}}. \end{aligned}$$

(5.h) Let w_{U_ν} be the image of $\widetilde{\Delta}(w_\nu)$ in U_ν.

(5.i) Let γ_0 be any preimage of w_{U_ν} via φ.

(5.j) Let u_0 be the image of $\Delta(u_\nu^{\mathrm{val}_\nu(\pi) g_\nu / a})$ in $\mathcal{O}_{\widetilde{A}} / \widetilde{\mathfrak{P}}_{\nu,g_\nu}^{e_{\nu,g_\nu}(m_0+1)}$.

(5.k) Set $\alpha_{Q_\nu} = (1, \ldots, 1, \gamma_0) \cdot (1, \ldots, u_0) \in Q_\nu$.

(6) Use the Chinese Remainder Theorem to compute an element α' in $\widetilde{A}$ which maps to α_{Q_ν} in Q_ν for each place ν of E of slope in $(0,1)$.

(7) Compute the maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ of $\widetilde{W_R}$ which lie below the maximal ideals of $\mathcal{O}_{\widetilde{A}}$ above the places ν of E of slope in $(0,1)$.

(8) For each $i = 1, \ldots, n$, compute a positive integer m_i such that $|\widetilde{J}/p^{m_0+1}\widetilde{J}| \leq |\widetilde{W_R}/\mathfrak{p}_i|^{m_i}$.

(9) Set $Q_{m_0+1} = \widetilde{J} / \left(p^{m_0+1}\widetilde{J} + \prod_{i=1}^n \mathfrak{p}_i^{m_i} \widetilde{J}\right)$ and $Q_{m_0} = \widetilde{J} / \left(p^{m_0}\widetilde{J} + \prod_{i=1}^n \mathfrak{p}_i^{m_i} \widetilde{J}\right)$ and compute the natural projection $\mathrm{pr} : Q_{m_0+1} \to Q_{m_0}$.

(10) Let α_{m_0+1} (resp. α_{m_0}) denote the multiplication-by-α' map on Q_{m_0+1} (resp. Q_{m_0}).

(11) Compute the reduction σ_{m_0+1} (resp. σ_{m_0}) of $\widetilde{\sigma}$ on Q_{m_0+1} (resp. Q_{m_0}).

(12) Define $F_{m_0+1} : Q_{m_0+1} \to Q_{m_0+1}$ as $x \mapsto \alpha_{m_0+1}(x^{\sigma_{m_0+1}})$, and $F_{m_0} : Q_{m_0} \to Q_{m_0}$ as $x \mapsto \alpha_{m_0}(x^{\sigma_{m_0}})$.

(13) Compute the homomorphism $m_p : Q_{m_0+1} \to Q_{m_0+1}$ induced by the multiplication-by-p map.

(14) For each generator as a finite group γ of Q_{m_0}:

(14.a) Pick $x_\gamma \in Q_{m_0+1}$ such that $\mathrm{pr}(x_\gamma) = \gamma$.

(14.b) Pick $z_\gamma \in Q_{m_0+1}$ such that $F_{m_0+1}(z_\gamma) = m_p(x_\gamma)$.

(15) Compute $V_{m_0} : Q_{m_0} \to Q_{m_0}$ by setting $V_{m_0}(\gamma) = \mathrm{pr}(z_\gamma)$ for each $\gamma \in Q_{m_0}$.

(16) For each $\widetilde{I}_k \in \mathcal{I}$ compute its image I_{k,m_0} in Q_{m_0} under the projection map from $\widetilde{J}$.

(17) Return $\{\widetilde{I}_k \in \mathcal{I}$ such that $I_{k,m_0} = I_{k,m_0} + F_{m_0}(I_{k,m_0}) + V_{m_0}(I_{k,m_0})\}$.

Theorem 6.17. *Algorithm 3 is correct.*

Proof. By Proposition 6.10, the extension of a $W_R'\{F', V'\}$-ideal to $\mathcal{O}_{A'}$ is a $W_R'\{F', V'\}$-ideal. Hence, considering only such ideals (that is, whose extension is in Υ) in the input is not a limitation.

The algorithm is an application of Lemma 6.15: for each $I \in \mathcal{I}$, we want to check whether it is stable by the action of F' and V', by looking at its image in the finite quotient Q_{m_0} defined in Step (9). In order to do so, we need to compute representations of F' and V' in Q_{m_0}.

First consider F'. In Step (5.i), we produce an element $\gamma_0 \in \mathcal{O}_{\widetilde{A}}/\widetilde{\mathfrak{P}}_{\nu,g_\nu}^{e_{\nu,g_\nu}(m_0+1)} \cong \mathcal{O}_{LE_\nu}/\mathfrak{p}_{LE_\nu}^{e_\nu(m_0+1)}$. Under this isomorphism we get an element that with slight abuse of notation we also call $\gamma_0 \in \mathcal{O}_{LE_\nu}$. The property in (5.i) then translates to the equality $N_{LE_\nu/E_\nu}(\gamma_0) = \pi_\nu/t_\nu^{\mathrm{val}_\nu(\pi_\nu)}$ in $\mathcal{O}_{LE_\nu}/\mathfrak{p}_{LE_\nu}^{e_\nu(m_0+1)}$, for some uniformizer t_ν in E_ν. We can now apply Lemma 6.16 to find an element $\gamma_1 \in \mathfrak{p}_{LE_\nu}^{m_0+2}$ such that $N_{LE_\nu/E_\nu}(\gamma_0 + \gamma_1) = \pi_\nu/t_\nu^{\mathrm{val}_\nu(\pi_\nu)}$. This means that if we define $F'_\nu = \alpha_\nu \circ \sigma$ with

$$\alpha_\nu = (1, \ldots, t_\nu^{\mathrm{val}_\nu(\pi_\nu)g_\nu/a}(\gamma_0 + \gamma_1)),$$

then F'_ν has the Frobenius property and is of W-type, by Lemma 4.3. Putting $\alpha = (\alpha_\nu)_{\nu|p} \in A'$ we get $F' = \alpha \circ \sigma$, an additive map on A' of W-type. Step (6) produces an element $\alpha' \in \widetilde{A}$, from which we define the additive map $F_{m_0+1} : Q_{m_0+1} \to Q_{m_0+1}$ in Step (12). We see that F_{m_0+1} is the reduction of F' restricted to J' under the isomorphism $Q_{m_0+1} \cong J'/p^{m_0+1}J'$. Note that F' also induces F_{m_0} on Q_{m_0}.

Now consider V'; we need to show that V_{m_0} as defined in Step 15 is the map induced by V' on Q_{m_0}. As we now explain, in fact V_{m_0} is computed from the representation of F_{m_0+1} of F' on the larger quotient Q_{m_0+1}. Let $\mathrm{pr}_{m_0} : J \to Q_{m_0}$ and $\mathrm{pr}_{m_0+1} : J \to Q_{m_0+1}$ be the natural projections. Observe that $\mathrm{pr}_{m_0} = \mathrm{pr} \circ \mathrm{pr}_{m_0+1}$. Let x_{m_0} be an element of Q_{m_0}. Denote by x a preimage of x_{m_0} in J via pr_{m_0}. Set $x_{m_0+1} = \mathrm{pr}_{m_0+1}(x)$ and $y = V'(x) \in J$. It remains to show that $\mathrm{pr}_{m_0}(y) = V_{m_0}(x_{m_0})$. By the construction of V_{m_0}, we have

$$V_{m_0}(x_{m_0}) = \mathrm{pr}(z_{m_0+1}),$$

where z_{m_0+1} is an element of Q_{m_0+1} such that

$$p \cdot x_{m_0+1} = F_{m_0+1}(z_{m_0+1}).$$

Let z be a preimage of z_{m_0+1} in J via pr_{m_0+1}. Note that $F'(y) = p \cdot x$. Hence

$$\mathrm{pr}_{m_0+1}(F'(y)) = p \cdot x_{m_0+1} = F_{m_0+1}(z_{m_0+1}) = \mathrm{pr}_{m_0+1}(F'(z)),$$

where the last equality follows by the definition of F_{m_0+1}. Therefore

$$F'(y) - F'(z) = F'(y - z) \in p^{m_0+1}J.$$

By applying V', we then get

$$p(y - z) \in V'(p^{m_0+1}J) \subseteq p^{m_0+1}J.$$

Dividing by p gives

$$y - z \in p^{m_0}J.$$

By applying pr_{m_0} we obtain

$$\mathrm{pr}_{m_0}(y) = \mathrm{pr}_{m_0}(z) = \mathrm{pr} \circ \mathrm{pr}_{m_0+1}(z) = \mathrm{pr}(z_{m_0+1}) = V_{m_0}(x_{m_0}),$$

as required. □

Remark 6.18. In Algorithm 3, we need to compute the action of σ_{Q_ν} on Q_ν in Step (5.g) for each place ν of E, and of σ_{m_0+1} and σ_{m_0} on Q_{m_0+1} and Q_{m_0} in Step (11), all induced by the action of $\widetilde{\sigma}$.

Note that, in Step (5.g), Q_ν (defined in Step (5.d)) for each place ν, is a factor of $\mathfrak{o}_A = \mathcal{O}_{\widetilde{A}}/p^{m_0+1}\mathcal{O}_{\widetilde{A}}$. So, we proceed exactly as in Remark 6.12, by computing a σ-equivariant presentation of $\mathfrak{o}_A$ as an $\mathcal{O}_{\widetilde{L}}/(p\mathcal{O}_{\widetilde{L}})^m$-module for m defined by $|\mathfrak{o}_A| = |\mathcal{O}_{\widetilde{L}}/p\mathcal{O}_{\widetilde{L}}|^m$.

In Step (11), we proceed as follows. By Step 2, we have $\widetilde{J} \subseteq \mathcal{O}_{\widetilde{A}}$. Set $m' = m_0 + 1 + \mathrm{val}_p([\mathcal{O}_{\widetilde{A}} : \widetilde{J}])$, so that

$$p^{m'}\mathcal{O}_{\widetilde{A}} \subseteq p^{m_0+1}\widetilde{J} \subseteq \left(p^{m_0+1}\widetilde{J} + \prod_{i=1}^{n} \mathfrak{p}_i^{m_i}\widetilde{J}\right) \subseteq \widetilde{J} \subseteq \mathcal{O}_{\widetilde{A}}.$$

Then a reduction $\sigma_{m'}$ of σ on $\mathfrak{o}_A = \mathcal{O}_{\widetilde{A}}/p^{m'}\mathcal{O}_{\widetilde{A}}$, computed as in the preceding paragraph, will induce well-defined approximations σ_{m_0} on Q_{m_0} and σ_{m_0+1} on Q_{m_0+1}.

We stress that this construction does not require $\widetilde{L}$ to be normal; cf Remark 6.2.(iv).

Remark 6.19. The semilinear operators F' and V' are p-adic in nature. Hence, we can compute them only up to a finite precision. In Step 4 in Algorithm 3, we choose the smallest possible m_0 that allows us to check whether the ideals in the input set $\mathcal{I}$ represent $W'_R\{F', V'\}$-ideals. This choice of m_0 also allows us to compute the a-numbers of the Dieudonné modules. Indeed, if $\widetilde{I}_k$ is in the output set, then the a-number of the corresponding Dieudonné module equals

$$\dim_{\mathbb{F}_q}\left(\frac{I_{k,m_0}}{F_{m_0}(I_{k,m_0}) + V_{m_0}(I_{k,m_0})}\right).$$

If one needs to know the action of F' and V' to higher precision, it suffices to increase the value of m_0 in Step 4.

Remark 6.20. In Step 3, we need to scale each ideal $\widetilde{I}_k$ inside $\widetilde{J}$ by some element x of $\widetilde{\Delta}(E^\times)$, that is, $x \in \widetilde{\Delta}^{-1}(C)$, where $C = (\widetilde{J} : \widetilde{I}_k)$. Moreover, it is desirable to try to minimize $w = \mathrm{val}_p(\exp(\widetilde{J}/x\widetilde{I}_k))$, in order to keep the parameter m_0 as low as possible, since m_0 determines the size of the quotients appearing in the rest of the algorithm. One possibility is to compute $v = \mathrm{val}_p(\exp(\widetilde{I}_k + \widetilde{J}/\widetilde{J}))$ and $y = [p^v\widetilde{I}_k + \widetilde{J} : \widetilde{J}]$, which is coprime to p. Then $x = p^v y$ is the *integer* in $\widetilde{\Delta}^{-1}(C)$ giving the smallest possible value of w. Another possibility (dropping the restriction of x being an integer) is to use the fact that C is a fractional $\mathcal{O}_{\widetilde{A}}$-ideal. Compute the uniformizers $t_{\nu_1}, \ldots, t_{\nu_n}$ of the places $\nu_1, \ldots, \nu_n$ of E above p using Lemma 6.3. For each ν_i, let M_i be the maximum value of $\mathrm{val}_{\widetilde{\mathfrak{P}}}(C)$ for $\widetilde{\mathfrak{P}}$ ranging over the maximal ideals of $\mathcal{O}_{\widetilde{A}}$ above ν_i. Then set $x' = \widetilde{\Delta}(t_{\nu_1}^{M_1} \cdots t_{\nu_n}^{M_n})$, $y = [x'\widetilde{I}_k + \widetilde{J} : \widetilde{J}]$ and finally $x = x'y$. The second method might give smaller values of w but requires more expensive computations. Similar considerations apply in Step 2 if one is using the method described in Remark 6.18 for computing F_{m_0} and V_{m_0}.

7 Computing isomorphism classes of abelian varieties

In this section, we provide some algorithms that, building on the ones contained in the previous sections, allow us to compute the set $\mathcal{A}_\pi^{\mathrm{isom}}$ of isomorphism classes of abelian varieties in the isogeny class $\mathcal{A}_\pi$ together with their endomorphism rings. These algorithms will be used to exhibit some interesting examples in Section 8.

Algorithm 4.
Input: The order $R = \mathbb{Z}[\pi, q/\pi]$.
Output: Representatives of $\prod_{\ell \neq p} \mathfrak{X}_{\pi,\ell}$ given as a list of vectors $(I_{\mathfrak{l}_i})_{\mathfrak{l}_i}$ of fractional R-ideals indexed by the maximal ideals $\mathfrak{l}_1, \ldots, \mathfrak{l}_n$ of R which divide the conductor $(R : \mathcal{O})$ and do not contain p.

(1) For $i = 1, \ldots, n$ do the following:

   (i) Set $k_i = \mathrm{val}_{\ell_i}([\mathcal{O} : R])$ where ℓ_i is the rational prime below $\mathfrak{l}_i$;

   (ii) Compute a set of representatives $\mathcal{R}^{\mathfrak{l}_i}$ of $\mathcal{W}(R + \mathfrak{l}_i^{k_i}\mathcal{O})$, using, for example, [23, Algorithm ComputeW];

(2) Return $\prod_{i=1}^{n} \mathcal{R}^{\mathfrak{l}_i}$.

Theorem 7.1. *Algorithm 4 is correct.*

Proof. The result follows from Theorem 3.12. □

Algorithm 5.
Input: The order $R = \mathbb{Z}[\pi, q/\pi]$.
Output: Representatives of $\mathfrak{X}_{\pi,p}$ given as a list of triples $(I^{\{0\}}, I', I^{\{1\}})$ representing all Δ-isomorphism classes of $W_R\{F,V\}$-ideals; here $I^{\{0\}}$ and $I^{\{1\}}$ are R-ideals and I' is a $\widetilde{W}'_R$-ideal.

(1) Set $k = \mathrm{val}_p([\mathcal{O} : R])$.

(2) For each $\mathfrak{p}_\nu \in \mathcal{P}_{R_p}$ with $s(\nu) = 0$ compute a set of representatives $\mathcal{R}_{\mathfrak{p}_\nu}$ of $\mathcal{W}(R + \mathfrak{p}_\nu^k\mathcal{O})$, for example using [23, Algorithm ComputeW];

(3) Initialize an empty set $\mathcal{R}^{\{0\}}$;

(4) For each sequence $(I_{\mathfrak{p}_\nu})_{\mathfrak{p}_\nu} \in \prod_{\mathfrak{p}_\nu, s(\nu)=0} \mathcal{R}_{\mathfrak{p}_\nu}$ append to $\mathcal{R}^{\{0\}}$ a fractional R-ideal $I^{\{0\}}$ such that $I^{\{0\}}_{\mathfrak{p}_\nu} = I_{\mathfrak{p}_\nu}$ for each $\mathfrak{p}_\nu$ with $s(\nu) = 0$, built using Lemma 3.7;

(5) For each $\mathfrak{p}_\nu \in \mathcal{P}_{R_p}$ with $s(\nu) = 1$ compute a set of representatives $\mathcal{R}_{\mathfrak{p}_\nu}$ of $\mathcal{W}(R + \mathfrak{p}_\nu^k\mathcal{O})$, for example, using [23, Algorithm ComputeW];

(6) Initialize an empty set $\mathcal{R}^{\{1\}}$;

(7) For each sequence $(I_{\mathfrak{p}_\nu})_{\mathfrak{p}_\nu} \in \prod_{\mathfrak{p}_\nu, s(\nu)=1} \mathcal{R}_{\mathfrak{p}_\nu}$ append to $\mathcal{R}^{\{1\}}$ a fractional R-ideal $I^{\{1\}}$ such that $I^{\{1\}}_{\mathfrak{p}_\nu} = I_{\mathfrak{p}_\nu}$ for each $\mathfrak{p}_\nu$ with $s(\nu) = 1$, built using Lemma 3.7;

(8) Use Algorithms 1, 2 and 3 to compute a set $\mathcal{R}'$ of representatives of of $W'_R\{F', V'\}$-ideals;

(9) Return $\mathcal{R}^{\{0\}} \times \mathcal{R}' \times \mathcal{R}^{\{1\}}$.

Theorem 7.2. *Algorithm 5 is correct.*

Proof. The chosen value of k ensures that $\mathfrak{p}_\nu^k\mathcal{O} \subseteq R$ for each prime $\mathfrak{p}_\nu$ above p by Remark 3.11. Hence, $\mathcal{R}^*$ is a set of representatives of R_p^*-isomorphism classes of $W_R^*\{F,V\}$-ideals by Propositions 3.10 and 6.1, for $*$ in $\{\{0\},\{1\}\}$. Moreover, $\mathcal{R}'$ is a set of representatives of Δ'-isomorphism classes of $W'_R\{F',V'\}$-ideals by construction. Hence, the output of Algorithm 5 represents all Δ-isomorphism classes of $W_R\{F,V\}$-ideals by Equation 15. □

Lemma 7.3. *Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be maximal ideals of R, let $S_1, \ldots, S_n$ be overorders of R, and let $k_1, \ldots, k_n$ be positive integers such that for each i we have $\mathfrak{p}_i^{k_i}\mathcal{O}_{E,\mathfrak{p}_i} \subseteq S_{i,\mathfrak{p}_i}$. Define*

$$S := \cap_{i=1}^n (S_i + \mathfrak{p}_i^{k_i}\mathcal{O}_E).$$

Then S is an overorder of R such that $S_{\mathfrak{p}_i} = S_{i,\mathfrak{p}_i}$ for every i and $S_{\mathfrak{q}} = \mathcal{O}_{E,\mathfrak{q}}$ for every other maximal ideal $\mathfrak{q}$ of R.

Proof. Omitted. □

The following algorithm computes the endomorphism rings of the abelian varieties in $\mathcal{A}_\pi$, which are uniquely determined by the isomorphism classes of their local parts.

Algorithm 6.
Input: An element $(I^{\{0\}}, I', I^{\{1\}})$ of the output $\mathcal{R}^{\{0\}} \times \mathcal{R}' \times \mathcal{R}^{\{1\}}$ of Algorithm 5, and a vector $(I^{\mathfrak{l}})_{\mathfrak{l}}$ of fractional R-ideals belonging to the output $\prod_{\mathfrak{l}} \mathcal{R}^{\mathfrak{l}}$ of Algorithm 4.
Output: An overorder S of R which is the endomorphism ring of the element $Y \in \mathfrak{X}_{\pi,p} \times \prod_{\ell \neq p} \mathfrak{X}_{\pi,\ell}$ which is represented by $(I^{\{0\}}, I', I^{\{1\}}, (I^{\mathfrak{l}})_{\mathfrak{l}})$.

(1) Set $S^{\mathfrak{l}} = (I^{\mathfrak{l}} : I^{\mathfrak{l}})$;

(2) Set $S^{\{0\}} = (I^{\{0\}} : I^{\{0\}})$;

(3) Set $S'' = \widetilde{\Delta}^{-1}\left((\widetilde{I} : \widetilde{I})\right)$;

(4) Set $S^{\{1\}} = (I^{\{1\}} : I^{\{1\}})$;

(5) Let $\mathcal{P}_{\text{sing}}$ be set of maximal ideals of R which are singular;

(6) For each $\mathfrak{p} \in \mathcal{P}_{\text{sing}}$, set $S^{\mathfrak{p}}$ to be S^0, S'', S^1 or $S^{\mathfrak{l}}$ depending on whether $\mathfrak{p}$ is in $\mathcal{P}_{R_p}^{\{0\}}$, $\mathcal{P}_{R_p}^{(0,1)}$, $\mathcal{P}_{R_p}^{\{1\}}$ or not above p;

(7) Use Lemma 7.3 to compute the order S which is locally equal to $S_{\mathfrak{p}}$ for each $\mathfrak{p} \in \mathcal{P}_{\text{sing}}$ and maximal at every order maximal ideal;

(8) Return S.

Theorem 7.4. *Algorithm 6 is correct.*

Proof. The result follows since an order is determined by its localizations. □

The next and final algorithm combines all the previous ones to compute representatives of $\mathcal{A}_\pi^{\text{isom}}$.

Algorithm 7.
Input: An isogeny class $\mathcal{A}_\pi$ of abelian varieties with commutative endomorphism ring.
Output: A set of representatives of the isomorphism classes of in the category $\mathcal{C}_\pi$ (see Definition 5.1).

(1) Compute the order $R = \mathbb{Z}[\pi, q/\pi]$;

(2) Initialize an empty list $\mathcal{R}$;

(3) Run Algorithm 5 and let $\mathcal{R}^{\{0\}} \times \mathcal{R}' \times \mathcal{R}^{\{1\}}$ be the output;

(4) Run Algorithm 4 and let $\prod_{\mathfrak{l}} \mathcal{R}^{\mathfrak{l}}$ be the output;

(5) For each $Y = (I^{\{0\}}, \widetilde{I}, I^{\{1\}}, (I^{\mathfrak{l}})_{\mathfrak{l}})$ in $\mathcal{R}^{\{0\}} \times \mathcal{R}' \times \mathcal{R}^{\{1\}} \times \prod_{\mathfrak{l}} \mathcal{R}^{\mathfrak{l}}$, do the following:

   (1) Use Algorithm 6 to compute the endomorphism ring S_Y of Y;
   (2) Compute a set of representatives $J_1, \ldots, J_s$ of the class group $\mathrm{Cl}(S_Y)$ of S_Y;
   (3) For $j = 1, \ldots, s$, append (Y, J_j) to $\mathcal{R}$.

(6) Return $\mathcal{R}$.

Theorem 7.5. *Algorithm 7 is correct.*

Remark 7.6. Let $Y = (I^{\{0\}}, \widetilde{I}, I^{\{1\}}, (I^{\mathfrak{l}})_{\mathfrak{l}})$ be an element as in Step 5 of Algorithm 7. Let $\mathcal{P}$ be the set of maximal ideals of R that are either above p, or coprime to p and singular. For each $\mathfrak{p}$ in $\mathcal{P}$ set $I^{\mathfrak{p}}$ to be $I^{\{0\}}$, $\widetilde{\Delta}^{-1}(\widetilde{I})$, $I^{\{1\}}$ or $I^{\mathfrak{l}}$, depending on whether $\mathfrak{p}$ is in $\mathcal{P}_{R_p}^{\{0\}}$, $\mathcal{P}_{R_p}^{(0,1)}$, $\mathcal{P}_{R_p}^{\{1\}}$ or not above p. Use Lemma 3.7 to construct a fractional R-ideal I_Y whose localization at $\mathfrak{p}$ is $I^{\mathfrak{p}}$ for each $\mathfrak{p} \in \mathcal{P}$. Similarly, construct a fractional W_R-ideal M_Y whose localization at $\mathfrak{p}$ is $\widetilde{\Delta}(I^{\mathfrak{p}}) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ for $\mathfrak{p} \in \mathcal{P}_{R_p}^{\{0\}} \sqcup \mathcal{P}_{R_p}^{\{1\}}$ and $\widetilde{I} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ for $\mathfrak{p} \in \mathcal{P}_{R_p}^{(0,1)}$. Then for each representative J_j of $\mathrm{Cl}(S_Y)$ the pair (Y, J_j) represents the isomorphism class of the object $(I_Y J_j, M_Y \Delta(J_j \otimes_{\mathbb{Z}} \mathbb{Z}_p))$ of $\mathcal{C}_\pi$.

Proof of Theorem 7.5. The result follows from Theorem 4.9 as well as Theorem 3.12, combined with the fact that a fractional ideal in E is determined by its localizations together with an element of the Picard group. □

Remark 7.7. We could theoretically, in several of the algorithms presented above, use the duality of Subsection 4.3.2 to only make computations for places ν of E_p with slope in $[0, 1/2]$. This is not something that we have extensively implemented in practice, since we do not believe it would significantly improve the efficiency of our algorithms.

8 Examples

The examples in this section are computed using the implementations of the algorithms in this paper which are available at https://github.com/stmar89/IsomClAbVarFqCommEndAlg[2].

[2]The examples in this paper where computed using the code at commit c25be473adfeb1dba9932d47961e54649889fa78

Let $\mathcal{A}_\pi$ be an isogeny class of abelian varieties over $\mathbb{F}_q$ of dimension g with commutative endomorphism algebra $E = \mathbb{Q}[\pi]$. Put $R = \mathbb{Z}[\pi, q/\pi]$, as before. Let $\mathcal{S}$ be the set of overorders of R and let $\mathcal{E}$ be the subset of $\mathcal{S}$ consisting of endomorphism rings, that is, orders T such that there exists $X \in \mathcal{A}_\pi$ with $\mathrm{End}(X) = T$. Consider the following three statements:

(1) For every $S \in \mathcal{E}$ and $T \in \mathcal{S}$, if $S \subseteq T$ then $T \in \mathcal{E}$.

(2) The order $S = \cap_{T \in \mathcal{E}} T$ is in $\mathcal{E}$.

(3) For every S in $\mathcal{E}$, $n(\mathcal{O}_E)$ divides $n(S)$, where $n(S)$ (resp. $n(\mathcal{O}_E)$) is the number of isomorphism classes of abelian varieties in $\mathcal{A}_\pi$ with endomorphism ring S (resp. $\mathcal{O}_E$).

If $\mathcal{A}_\pi$ is ordinary, or almost ordinary, or if q is prime, then statements (1), (2) and (3) hold true; see [21, Corollary 4.4], [24, Theorem 4.5] (for odd characteristic) and Corollary 5.5 together with Example 5.6 (for all characteristics).

Now assume further that $\mathcal{A}_\pi$ has p-rank $< g$. Let $\mathfrak{p}$ be the maximal ideal of $R = \mathbb{Z}[\pi, q/\pi]$ corresponding to the local-local part. Consider the following statements:

(*) $\mathrm{End}(X)_\mathfrak{p}$ is maximal for every X in $\mathcal{A}_\pi$.

(a) There exists a unique maximal ideal $\mathfrak{P}$ of $\mathcal{O}_E$ above $\mathfrak{p}$ with slope $\leq 1/2$.

(b) All maximal ideals of $\mathcal{O}_E$ above $\mathfrak{p}$ have slope $1/2$.

(c) For each maximal ideal $\mathfrak{P}$ of $\mathcal{O}_E$ above $\mathfrak{p}$ we have that the slope equals $1/n_\mathfrak{P}$ or $1 - 1/n_\mathfrak{P}$, where $n_\mathfrak{P}$ is the dimension of $E_\mathfrak{P}$ over $\mathbb{Q}_p$, that is, the product of the ramification index and the inertia degree.

Note that $\mathcal{A}_\pi$ is almost ordinary if and only if all three conditions (a), (b) and (c) hold true.

Let $\mathcal{T}$ be the set of all maximal ideals of R except the one above p of slope $(0, 1)$. In the rest of the section, we will associate to each order $S \in \mathcal{S}$ four nonnegative integers: $n(S)$, the number of isomorphism classes of abelian varieties in $\mathcal{A}_\pi$ with endomorphism ring S (as defined above); $w(S)$, the number of elements of $\mathcal{W}_\mathcal{T}(S)$; $d(S)$, the number of $W_R'\{F', V'\}$-ideals with endomorphism ring S; and $h(S)$, the class number of S.

Proposition 8.1. *For all $S \in \mathcal{S}$,*

$$n(S) = w(S)d(S)h(S).$$

Proof. This follows from Theorem 5.2 combined with Propositions 3.8, 3.9 and 6.1. □

Hence, we have $S \in \mathcal{E}$, that is, S is the endomorphism ring for some $X \in \mathcal{A}_\pi$, if and only if $n(S) > 0$, which is also equivalent to $d(S) > 0$.

Proposition 8.2. *Let $\mathcal{A}_\pi$ be an isogeny class of g-dimensional abelian varieties over $\mathbb{F}_q$ with commutative endomorphism algebra and p-rank $< g$. We have the following implications:*

$$(a) + (b) + (c) \Longrightarrow (*) \Longrightarrow (1) + (2) + (3).$$

Proof. As pointed out above, (a), (b) and (c) all hold if and only if $\mathcal{A}_\pi$ is almost ordinary. The first implication is shown in Example 5.6.

Corollary 5.8 shows that (*) implies (1) and (2). We now show that (*) also implies (3), completing the proof of the second implication. By Proposition 8.1, the number $n(S)$ is divisible by $d(S)h(S)$. Observe that (*) implies that $d(S) = d(\mathcal{O}_E)$ for each $S \in \mathcal{E}$, and that $h(\mathcal{O}_E)$ divides $h(S)$ since the extension map $\mathrm{Cl}(S) \to \mathrm{Cl}(\mathcal{O}_E)$ is surjective. Every fractional $\mathcal{O}_E$-ideal is locally principal, hence $w(\mathcal{O}_E) = 1$. It follows that the number of abelian varieties with endomorphism ring $\mathcal{O}_E$ is determined only by the class group of $\mathcal{O}_E$ and by the local-local part. More precisely, we have $n(\mathcal{O}_E) = d(\mathcal{O}_E)h(\mathcal{O}_E)$. Combining all these statements we see that $n(\mathcal{O}_E)$ divides $n(S)$ for each $S \in \mathcal{E}$, as required. □

In each of following three examples (Examples 8.3, 8.4 and 8.5), we negate exactly one of the three statements (a), (b), (c), and show that (*) does not hold and that (1), (2) or (3) fails.

In Example 8.6, we exhibit an isogeny class with p-rank $< g$ for which all of (1), (2) and (3) hold true, but (*) fails. This examples also shows that (1) + (2) + (3) is not equivalent to the isogeny class being almost ordinary.

In Example 8.7, we exhibit an isogeny class with abelian varieties with the same endomorphism ring but whose a-numbers are different.

In all the examples below we have $w(S) = 1$ for all $S \in \mathcal{S}$. We would have $w(S) > 1$, for some $S \in \mathcal{S}$, if and only if R is not Bass at some maximal ideal of $\mathcal{T}$. For an example of an R with this property, see [21, Example 7.4].

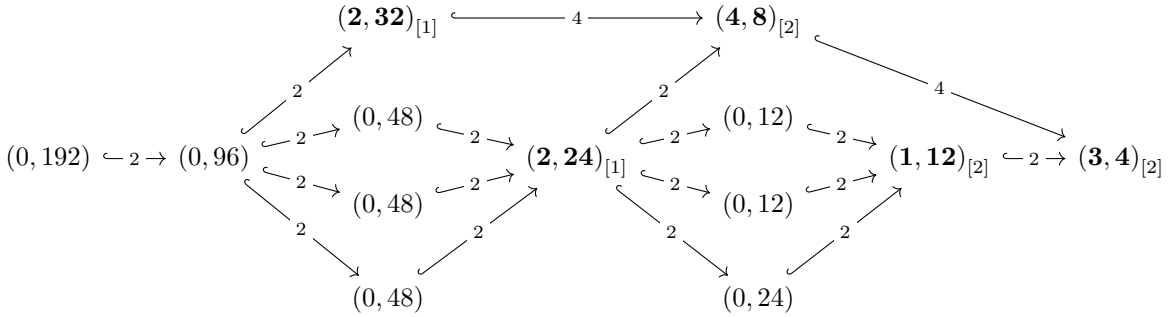
We conclude the section with some observations and a further example, arising from the computations we have performed. In the following graphs, each vertex represents an overorder S of R, labeled with the pair $(d(S), h(S))$, and each edge represents an inclusion, labeled with its index. If S is in $\mathcal{E}$, that is, S is the endomorphism ring for some $X \in \mathcal{A}_\pi$, then we add in the subscript of the label, the a-numbers of the isomorphism classes of Dieudonné modules. In all examples (except Example 8.7) we write only one value, since all the Dieudonné modules have the same a-number.

Example 8.3. Consider the polynomial

$$h = x^8 + x^7 + x^6 + 4x^5 - 4x^4 + 16x^3 + 16x^2 + 64x + 256.$$

It determines an isogeny class of geometrically simple abelian fourfolds over $\mathbb{F}_4$ with commutative endomorphism algebra $E = \mathbb{Q}[\pi] = \mathbb{Q}[x]/h$. The isogeny class has LMFDB label 4.4.b_b_e_ae and p-rank 2. The algebra E has 3 places above $p = 2$ with slopes, ramification indices and inertia degrees equal to $(0, 1, 2), (1, 1, 2), (1/2, 2, 2)$, respectively. Hence, this isogeny class satisfies conditions (a) and (b), but not condition (c).

The unique maximal ideal of the order $R = \mathbb{Z}[\pi, 16/\pi]$ in E above 2 is singular and in $\mathcal{P}_{R_2}^{(0,1)}$. One computes that R has 13 overorders S and for each of these $w(S) = 1$. It follows from Proposition 8.1 that $n(S) = d(S)h(S)$.



We see that statements (1), (2) and (3) do not hold true for this isogeny class. Hence, also statement (*) does not hold for this isogeny class: only the maximal order has maximal local-local part.

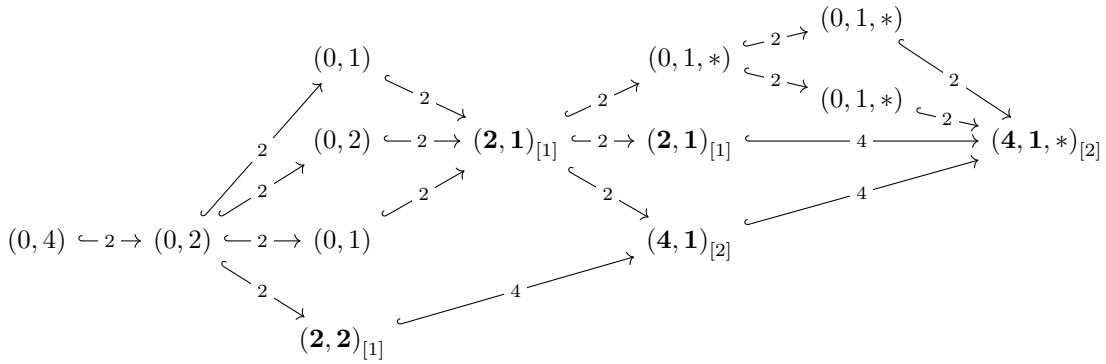
Example 8.4. Put $h_1 = x^2 - 2x + 4$, $h_2 = x^2 + 2x + 4$ and consider the polynomial

$$h = x^4 + 4x^2 + 16 = h_1 \cdot h_2.$$

It determines an isogeny class $\mathcal{A}_\pi$ of abelian surfaces over $\mathbb{F}_4$ with commutative endomorphism algebra $E = \mathbb{Q}[\pi] = \mathbb{Q}[x]/h$. Put $E_1 = \mathbb{Q}[\pi_1] = \mathbb{Q}[x]/h_1$ and $E_2 = \mathbb{Q}[\pi_2] = \mathbb{Q}[x]/h_2$. Any $X \in \mathcal{A}_\pi$ is isogenous to a product of supersingular elliptic curves $C_1 \times C_2$ with $C_i \in \mathcal{A}_{\pi_i}$. Note that the supersingular curves in $\mathcal{A}_{\pi_1}$ are quadratic twists of the ones in $\mathcal{A}_{\pi_2}$. The LMFDB labels of $\mathcal{A}_\pi$, $\mathcal{A}_{\pi_1}$, $\mathcal{A}_{\pi_2}$ are 2.4.a_e, 1.4.ac, 1.4.c, respectively. Therefore, conditions (b) and (c) hold, but not condition (a).

The unique maximal ideal of the order $R = \mathbb{Z}[\pi, 16/\pi]$ in E above 2 is singular and in $\mathcal{P}_{R_2}^{(0,1)}$. One computes that R has 13 overorders S and for each of these $w(S) = 1$. It follows from Proposition 8.1 that $n(S) = d(S)h(S)$.

An abelian variety X is isomorphic to a product $C_1 \times C_2$ with $C_i \in \mathcal{A}_{\pi_i}$ if and only if the order S is the direct product of $S_1 \times S_2$ with S_1 an order in E_1 and S_2 an order in E_2. Such orders are marked with a $*$ in the label in the graph below. The number of isomorphism classes which are products of elliptic curves can be derived from [28, Theorem 4.5] (which corrects parts of the statement of [33, Theorem 4.5]).



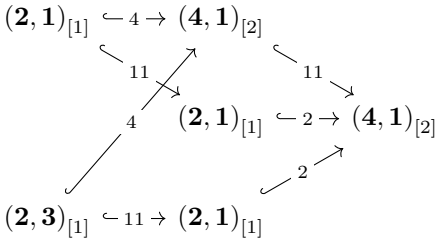
We see that statements (1), (2) and (3) do not hold true for this isogeny class. Hence, also statement (*) does not hold for this isogeny class: only the maximal order has maximal local-local part.

Example 8.5. Consider the polynomial

$$h = x^8 - 6x^7 + 18x^6 - 36x^5 + 68x^4 - 144x^3 + 288x^2 - 384x + 256.$$

It determines an isogeny class of geometrically simple abelian fourfolds over $\mathbb{F}_{16}$ with commutative endomorphism algebra $E = \mathbb{Q}[\pi] = \mathbb{Q}[x]/h$. The isogeny class has LMFDB label 4.4.ag_s_abk_cq and p-rank 0, but it is not supersingular. The algebra E has two places above $p = 2$ with slopes, ramification indices and inertia degrees equal to $(1/4, 2, 2), (3/4, 2, 2)$, respectively. Hence, this isogeny class satisfies conditions (a) and (c), but not condition (b).

The order $R = \mathbb{Z}[\pi, 4/\pi]$ has two singular maximal ideals: one above 11, and one above 2 which is in $\mathcal{P}_{R_2}^{(0,1)}$. The index of R in $\mathcal{O}_E$ is $704 = 11 \cdot 64$. The output of Algorithm 4 consists of exactly 2 classes, which can be represented by the maximal order $\mathcal{O}_E$ and the unique overorder T of R with index $[\mathcal{O}_E : T] = 11$. One then computes that R has 34 overorders S and for each of these $w(S) = 1$. It follows from Proposition 8.1 that $n(S) = d(S)h(S)$. Since the graph of inclusions of all overorders is too unwieldy, in the following graph, we draw the lattice of inclusion of the overorders S of R which are actually endomorphism rings for some $X \in \mathcal{A}_\pi$, that is, for which $d(S) > 0$.



On the one hand, we see from the graph that (2) and (3) do not hold true for this isogeny class. Hence, also statement (*) does not hold for this isogeny class: only the maximal order has maximal local-local part. On the other hand, if one considers all overorder of R, the inclusion with index 4 does not factor as the composition of two inclusions. It follows that this isogeny class satisfies condition (1).

Example 8.6. Consider the polynomial

$$h = x^6 - x^5 - 3x^4 + 45x^3 - 27x^2 - 81x + 729.$$

It determines an isogeny class of geometrically simple abelian threefolds over $\mathbb{F}_9$ with commutative endomorphism algebra $E = \mathbb{Q}[\pi] = \mathbb{Q}[x]/h$. The isogeny class has LMFDB label 3.9.ab_ad_bt and p-rank 1. The algebra E has three places above $p = 3$ with slopes, ramification indices and inertia degrees equal to $(0, 1, 1)$, $(1, 1, 1)$ and $(1/2, 1, 4)$, respectively. Hence, this isogeny class satisfies conditions (a) and (b), but not condition (c).

The unique singular maximal ideal of the order $R = \mathbb{Z}[\pi, 9/\pi]$ is the maximal ideal $(3, \pi, 9/\pi)$, which is in $\mathcal{P}^{(0,1)}_{R_3}$. One computes that R has 4 overorders S and for each of these $w(S) = 1$. It follows from Proposition 8.1 that $n(S) = d(S)h(S)$.

$$(0,60) \hookleftarrow 3 \rightarrow (0,30) \hookleftarrow 3 \rightarrow (\mathbf{2},\mathbf{20})_{[1]} \hookleftarrow 9 \rightarrow (\mathbf{2},\mathbf{2})_{[2]}$$

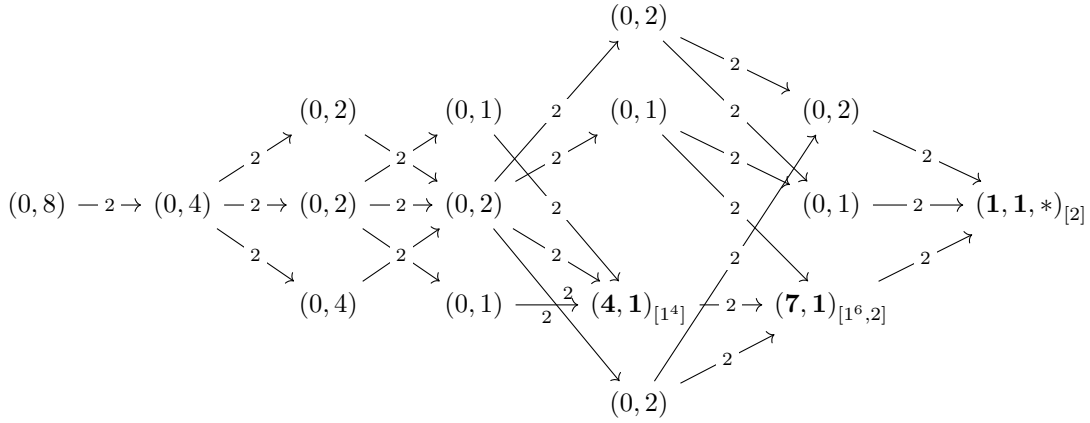
Statements (1), (2) and (3) hold true for this isogeny class, but statement (*) does not hold, since only the maximal order has maximal local-local part.

Example 8.7. Consider the polynomial

$$h = x^6 + 11x^5 + 60x^4 + 208x^3 + 480x^2 + 704x + 512.$$

It determines an isogeny class of abelian threefolds over $\mathbb{F}_8$ with commutative endomorphism algebra $E = \mathbb{Q}[\pi] = \mathbb{Q}[x]/h$. The isogeny class has LMFDB label 3.8.l_ci_ia and p-rank 1. Any $X \in \mathcal{A}_\pi$ is isogenous to a product of a supersingular elliptic curve and an almost ordinary abelian surface.

The unique singular maximal ideal of the order order $R = \mathbb{Z}[\pi, 8/\pi]$ is the maximal ideal $(2, \pi, 8/\pi)$, which is in $\mathcal{P}^{(0,1)}_{R_2}$. One computes that R has 16 overorders S and for each of these $w(S) = 1$. It follows from Proposition 8.1 that $n(S) = d(S)h(S)$. If $d(S) > 0$ for an overorder S, then we add in the subscript of the label, the a-numbers of the isomorphism classes of Dieudonné modules, using the exponent to denote the number of isomorphism classes of Dieudonné modules with the indicated a-number. The unique endomorphism ring with index 2 in the maximal order is the endomorphism ring of 7 isomorphism classes of abelian varieties, all with pairwise non-isomorphic Dieudonné modules. Six of these isomorphism classes of abelian varieties have a-number 1 while the last one has a-number 2. The only overorder of R which is a direct product of two orders is the maximal order. We highlight this in the graph with a $*$ in its label. This means that the only abelian varieties that are isomorphic to a product of an elliptic curve and an abelian surface are the ones with maximal endomorphism ring.



Observations 8.8. We have computed the isomorphism classes of abelian varieties for several thousands of isogeny classes (using lists of isogeny classes found in the LMFDB [19], which was compiled following [8]) with commutative endomorphism algebra $E = \mathbb{Q}[\pi]$ of dimension g and p-rank $< g-1$ over non-prime finite fields. We observed the following:

- the order R is never an endomorphism ring;
- there is always an endomorphism ring which is not maximal at the local-local part, that is, condition (*) does not hold. Note that if this observation would always hold then the first implication in Proposition 8.2 is actually an equivalence, and vice versa.

Remark 8.9. Over a prime field, every isogeny class contains an abelian variety with R as endomorphism ring, see [3]. Moreover, over any finite field, any isogeny class of ordinary abelian varieties contains an abelian variety with R as endomorphism ring, see [7].

Contrary to this, we showed in Example 5.6 that *no* almost-ordinary abelian variety over a non-prime finite field has R as endomorphism ring.

Recall that Proposition 4.14 says that if $\mathcal{A}_\pi$ is an isogeny class over $\mathbb{F}_q$ with commutative endomorphism algebra which is non-ordinary and such that $q = p^a$ is not a prime, then the order $R = \mathbb{Z}[\pi, q/\pi]$ is not maximal at the maximal ideal $\mathfrak{p} = (p, \pi, q/\pi)$. The converse does not hold, as we show in the following example.

Example 8.10. Let $\mathcal{A}_\pi$ be an isogeny class of simple abelian surfaces over $\mathbb{F}_2$ with p-rank 0 determined by the characteristic polynomial $h(x) = x^8 - 2x^5 - 4x^3 + 16$; see the LMFDB-label 4.2.a_a_ac_a. Let $E = \mathbb{Q}(\pi)$ be the endomorphism algebra of the isogeny class. The order $R = \mathbb{Z}[\pi, 2/\pi]$ has a unique maximal ideal above $p = 2$, which is $\mathfrak{p} = (2, \pi, 2/\pi)$. One computes that the quotient $\mathfrak{p}/\mathfrak{p}^2$ has 8 elements, while $R/\mathfrak{p} \simeq \mathbb{F}_2$. This shows that $\mathfrak{p}$ is singular, that is, the order $R_\mathfrak{p}$ is not maximal.

Notation

- $\mathbb{F}_q$, a finite field with $q = p^a$ elements of characteristic p.
- $\mathcal{A}_\pi$, an isogeny class of abelian varieties over $\mathbb{F}_q$ with commutative endomorphism algebra $E = \mathbb{Q}[\pi]$, where π is the Frobenius endomorphism.
- $\mathcal{A}_\pi^{\mathrm{isom}}$, the set of $\mathbb{F}_q$-isomorphism classes in $\mathcal{A}_\pi$.
- $\mathfrak{X}_\pi = \mathfrak{X}_{\pi,p} \times \prod_{\ell \neq p} \mathfrak{X}_{\pi,\ell}$, where $\mathfrak{X}_{\pi,p}$ (resp. $\mathfrak{X}_{\pi,\ell}$) is the set of isomorphism classes of Dieudonné modules (resp. ℓ-Tate modules) in $\mathcal{A}_\pi$.
- for an order S and a set $\mathcal{T}$ of maximal ideals of S: $\mathcal{W}(S)_\mathcal{T}$, the set of fractional S-ideals modulo the relation $I_\mathfrak{m} \simeq_\mathfrak{m} J_\mathfrak{m}$ for all $\mathfrak{m} \in \mathcal{T}$; see Definition 3.1 (also for variants).
- $h(x)$, the square-free characteristic polynomial of π.
- $\mathcal{O}_E$, the maximal order of E.
- $E_p = E \otimes_Q \mathbb{Q}_p = \prod_{\nu|p} E_\nu$.
- $R = \mathbb{Z}[\pi, q/\pi]$; $R_p = R \otimes_\mathbb{Z} \mathbb{Z}_p$.
- $L = \mathbb{Q}_p(\zeta_{q-1})$, the unramified extension of $\mathbb{Q}_p$ of degree a.
- $W = \mathcal{O}_L = \mathbb{Z}_p[\zeta_{q-1}]$.
- σ, the Frobenius automorphism of $L/\mathbb{Q}_p$.
- for a place ν of E_p: e_ν, the ramification index; f_ν, the inertia degree; $g_\nu = \gcd(a, f_\nu)$; $s(\nu) = \mathrm{val}_\nu(\pi)/ae_\nu$, the slope.
- τ_ν, the Frobenius automorphism of LE_ν/E_ν.
- $\mathfrak{p}_{E_\nu}$ (respectively $\mathfrak{p}_{LE_\nu}$), the maximal ideal of $\mathcal{O}_{E_\nu}$ (respectively $\mathcal{O}_{LE_\nu}$).
- $A = \prod_{\nu|p} A_\nu$, where $A_\nu = \prod_{j=1}^{g_\nu} LE_\nu$.
- $\Delta : E_p \hookrightarrow A$, induced by the diagonal embeddings $E_\nu \hookrightarrow A_\nu$.
- $F_\nu : A_\nu \to A_\nu$, an additive map satisfying the Frobenius property, that is, $F_\nu^a = \Delta_{|_{E_\nu}}(\pi_\nu)$ and $F_\nu \lambda = \lambda^\sigma F_\nu$, for every $\lambda \in L$.
- $F = (F_\nu)_{\nu|p}$ acting of $A = \prod_{\nu|p} A_\nu$.
- F_ν with the Frobenius property is of W-type if $F_\nu(z) = \alpha_\nu \cdot z^\sigma$, where $\alpha_\nu = (1, \ldots, 1, u_\nu) \in A_\nu$ with $N_{LE_\nu}(u_\nu) = \pi_\nu$; see Definition 4.4.
- $V = pF^{-1}$.
- $W_R = W \otimes_{\mathbb{Z}_p} R$.

- for $* = \{0\}, (0,1)$ or $\{1\}$: $\mathcal{P}^*_{R_p}$, the set of maximal ideal of R_p below a place ν with $s(\nu) \in *$.
- $R_p = R_p^{\{0\}} \sqcup R_p^{(0,1)} \sqcup R_p^{\{0\}}$, where $R_p^* = R_p \cap \prod_{\nu: s(\nu)\in *} E_\nu$.
- for $* = \{0\}, (0,1)$ or $\{1\}$: E^*, A^*, W_R^*, F^*, V^*, etc. denote the $*$-part of the corresponding object.
- for the local-local part (i.e the $(0,1)$-part), we use also $'$: E', A', W_R', F', V', etc.
- Υ, the set of Δ'-isomorphism classes of fractional $W_R'\{F', V'\}$-ideals with multiplicator ring $\mathcal{O}_{A'}$; see Definition 4.20.
- $\mathcal{C}_\pi$, a category of pairs (I, M) where I is a fractional R-ideal in E, and M is a $W_R\{F, V\}$-ideal such that $\Delta^{-1}(M) = i_p(I)R_p$; morphisms are $\mathrm{Hom}_{\mathcal{C}_\pi}((I, M), (J, N)) = \{\alpha \in E | \alpha I \subseteq J, \Delta(i_p(\alpha))M \subseteq N\}$; see Definition 5.1.
- $\widetilde{A}$ (resp. $\widetilde{A'}$, $\widetilde{W_R}$, etc.), the 'global version' of A (resp. A', W_R, etc.); see Subsection 6.1.

Acknowledgements

The authors are grateful to Sergey Rybakov for pointing out a mistake in a previous version of the paper.

The second author was partially supported by the Dutch Research Council (NWO), through grants VI.Veni.192.038 and VI.Vidi.223.028.

The third author was supported by NWO through grant VI.Veni.202.107, by Agence Nationale de la Recherche under the MELODIA project (grant number ANR-20-CE40-0013) and by Marie Skłodowska-Curie Actions - Postdoctoral Fellowships 2023 (project 101149209 - AbVarFq).

References

[1] Morton Abramson, *Restricted combinations and compositions*, Fibonacci Quart. **14** (1976), no. 5, pp. 439–452.

[2] Tejasi Bhatnagar and Yu Fu, *Abelian varieties with real multiplication: classification and isogeny classes over finite fields*, arXiv e-prints (2023), arXiv:2308.11105.

[3] Tommaso Centeleghe and Jakob Stix, *Categories of abelian varieties over finite fields, I: Abelian varieties over* $\mathbb{F}_p$, Algebra Number Theory **9** (2015), no. 1, pp. 225–265.

[4] ———, *Categories of abelian varieties over finite fields II: Abelian varieties over* $\mathbb{F}_q$ *and Morita equivalence*, Israel J. Math. **257** (2023), no. 1, pp. 103–170.

[5] Ching-Li Chai, Brian Conrad, and Frans Oort, *Complex multiplication and lifting problems*, Mathematical Surveys and Monographs, vol. 195, American Mathematical Society, Providence, RI, 2014.

[6] Everett Dade, Olga Taussky, and Hans Zassenhaus, *On the theory of orders, in particular on the semigroup of ideal classes and genera of an order in an algebraic number field*, Math. Ann. **148** (1962), pp. 31–64.

[7] Pierre Deligne, *Variétés abéliennes ordinaires sur un corps fini*, Invent. Math. **8** (1969), pp. 238–243.

[8] Taylor Dupuy, Kiran Kedlaya, David Roe, and Christelle Vincent, *Isogeny classes of abelian varieties over finite fields in the LMFDB*, Arithmetic geometry, number theory, and computation, Simons Symp., Springer, Cham, 2021, pp. 375–448.

[9] Cornelius Greither, *Cyclic Galois extensions of commutative rings*, Lecture Notes in Mathematics, vol. 1534, Springer-Verlag, Berlin, 1992.

[10] Robert Guralnick, *The genus of a module*, J. Number Theory **18** (1984), no. 2, pp. 169–177.

[11] Robert M. Guralnick, *The genus of a module. II. Roĭter's theorem, power cancellation and extension of scalars*, J. Number Theory **26** (1987), no. 2, pp. 149–165.

[12] Florian Hess, Sebastian Pauli, and Michael E. Pohst, *Computing the multiplicative group of residue class rings*, Math. Comp. **72** (2003), no. 243, pp. 1531–1548.

[13] Bruce Jordan, Allan Keeton, Bjorn Poonen, Eric Rains, Nicholas Shepherd-Barron, and John Tate, *Abelian varieties isogenous to a power of an elliptic curve*, Compos. Math. **154** (2018), no. 5, pp. 934–959.

[14] Ernst Kani, *Products of CM elliptic curves*, Collect. Math. **62** (2011), no. 3, pp. 297–339.

[15] Markus Kirschmer and Jürgen Klüners, *Chow groups of orders in number fields*, arXiv e-prints (2022), arXiv:2208.14688.

[16] Markus Kirschmer, Fabien Narbonne, Christophe Ritzenthaler, and Damien Robert, *Spanning the isogeny class of a power of an elliptic curve*, Math. Comp. **91** (2021), no. 333, pp. 401–449.

[17] Jürgen Klüners and Sebastian Pauli, *Computing residue class rings and Picard groups of orders*, J. Algebra **292** (2005), no. 1, 47–64.

[18] Lawrence Levy and Roger Wiegand, *Dedekind-like behavior of rings with 2-generated ideals*, J. Pure Appl. Algebra **37** (1985), no. 1, pp. 41–58.

[19] The LMFDB Collaboration, *The l-functions and modular forms database*, `http://www.lmfdb.org`, 2013, [Online; accessed 12 September 2024].

[20] Stefano Marseglia, *Computing the ideal class monoid of an order*, J. Lond. Math. Soc. (2) **101** (2020), no. 3, pp. 984–1007.

[21] ———, *Computing square-free polarized abelian varieties over finite fields*, Math. Comp. **90** (2021), no. 328, pp. 953–971.

[22] ———, *Cohen-Macaulay type of orders, generators and ideal classes*, arXiv e-prints (2022), arXiv:2206.03758.

[23] ———, *Local isomorphism classes of fractional ideals of orders in étale algebras*, arXiv e-prints (2023), arXiv:2311.18571.

[24] Abhishek Oswal and Ananth Shankar, *Almost ordinary abelian varieties over finite fields*, Journal of the London Mathematical Society **101** (2020), no. 3, pp. 923–937.

[25] Irving Reiner, *Maximal orders*, London Mathematical Society Monographs. New Series, vol. 28, The Clarendon Press, Oxford University Press, Oxford, 2003.

[26] Klaus Roggenkamp, *Lattices over orders. II*, Lecture Notes in Mathematics, vol. 142, Springer-Verlag, Berlin-New York, 1970.

[27] Klaus Roggenkamp and Verena Huber-Dyson, *Lattices over orders. I*, Lecture Notes in Mathematics, vol. 115, Springer-Verlag, Berlin-New York, 1970.

[28] René Schoof, *Nonsingular plane cubic curves over finite fields*, J. Combin. Theory Ser. A **46** (1987), no. 2, pp. 183–211.

[29] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, 1979, Translated from the French by Marvin Jay Greenberg.

[30] Peter Stevenhagen, *The arithmetic of number rings*, Algorithmic number theory: lattices, number fields, curves and cryptography, Math. Sci. Res. Inst. Publ., vol. 44, Cambridge Univ. Press, Cambridge, 2008, pp. 209–266.

[31] John Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), pp. 134–144.

[32] John Voight, *Quaternion algebras*, Graduate Texts in Mathematics, vol. 288, Springer, Cham, 2021.

[33] William Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) **2** (1969), pp. 521–560.

[34] Jiang Wei Xue and Chia-Fu Yu, *On counting certain abelian varieties over finite fields*, Acta Math. Sin. (Engl. Ser.) **37** (2021), no. 1, pp. 205–228.

[35] Chia-Fu Yu, *Simple mass formulas on Shimura varieties of PEL-type*, Forum Math. **22** (2010), no. 3, pp. 565–582.

[36] ———, *Superspecial abelian varieties over finite prime fields*, J. Pure Appl. Algebra **216** (2012), no. 6, pp. 1418–1427.

Matematiska institutionen, Stockholms Universitet, SE-106 91 Stockholm, Sweden
E-mail address: jonasb@math.su.se

Mathematisch Instituut, Universiteit Utrecht, Postbus 80010, 3508 TA Utrecht, The Netherlands
E-mail address: v.z.karemaker@uu.nl

Mathematisch Instituut, Universiteit Utrecht, Postbus 80010, 3508 TA Utrecht, The Netherlands
Laboratoire GAATI, Université de la Polynésie française, BP 6570 – 98702 Faaa, Polynésie française
Laboratoire Jean Alexandre Dieudonné, Université Côte Azur, 06108 Nice Cedex 2, France
E-mail address: stefano.marseglia@univ-cotedazur.fr