Rational points on Shimura curves and Galois representations

Carlos de Vera Piquero

2010 *Mathematics Subject Classification.* 11G18, 11G20, 14G35, 14G05.

Key words and phrases. Shimura curves, Atkin-Lehner quotients, rational points, Galois representations, Hasse principle, Brauer-Manin obstruction.

During the elaboration of this thesis, the author has been financially supported by an FI-DGR grant from the *Agency for Management of University and Research Grants* of the Government of Catalonia and by the FPU program of the Spanish *Ministry of Education and Science*. Part of the research has also been supported by projects 2009 SGR 1220, MTM2009-13060-C02-01 and MTM2012-34611.

Rational points on Shimura curves and Galois representations

Thesis submitted by

Carlos de Vera Piquero

for the degree of Doctor in Mathematics in the

Universitat Politècnica de Catalunya - BarcelonaTech

Thesis Advisor

Victor Rotger i Cerdà

Barcelona, 2014
Departament de Matemàtica Aplicada II
Universitat Politècnica de Catalunya - BarcelonaTech

A la meva mare

Contents

Introduction 1

Acknowledgements 9

Chapter 1. Preliminaries 11
1. Abelian varieties and their endomorphism algebras 11
2. Quaternion algebras 16
3. Shimura curves 25
4. Obstructions to the existence of rational points 35
5. Admissible curves, Drinfeld's upper half plane and Mumford uniformisation 42

Chapter 2. Shimura coverings of a Shimura curve 47
1. The Shimura curve $X_{D,\ell}$ 48
2. The cyclic Galois covering $X_{D,\ell} \to X_D$ 50
3. Atkin-Lehner involutions and their lifts to $X_{D,\ell}$ 52
4. The group $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ of modular automorphisms 55
5. Cyclic étale Galois coverings of $X_D^{(m)}$ 59
6. Moduli interpretations 62

Chapter 3. Local points on Shimura coverings at bad reduction primes 67
1. Shimura coverings of X_D 69
2. Čerednik-Drinfeld theory 73
3. Local points on the curves Y_d 77
4. $\mathbb{Q}_p$-rational points on Atkin-Lehner quotients of Y_d 88

Chapter 4. Galois representations over fields of moduli 101
1. Galois representations attached to abelian varieties 102
2. Galois representations attached to points on Shimura varieties 103
3. The case of Shimura curves 106
4. The case of Atkin-Lehner quotients of Shimura curves 109

Chapter 5. Rational points on Shimura curves via Galois representations 115
1. Proof of Theorem 5.1 117
2. Proof of Theorem 5.2 124
3. A different approach for $X_D^{(m)}$ 130

Bibliography 133

Introduction

This thesis explores one of the essential arithmetic properties of Shimura curves and their Atkin-Lehner quotients. Namely, the existence of rational points on these families of curves over both number fields and their completions. To some extent, the goal of this work can be therefore framed into the more general problem of describing the set of rational points of an algebraic variety over a number field or a local field[1].

Suppose for simplicity that X is a smooth projective curve over a number field K. The most important geometric invariant of X, its *genus* $g = g(X)$, not only measures the geometric complexity of X, but also influences the existence of rational points over K. When $g = 0$, for example, the Riemann-Roch Theorem shows that the anticanonical divisor class on X induces an embedding of X into $\mathbb{P}^2$ as a degree 2 curve. That is to say, X is isomorphic over K to a conic in $\mathbb{P}^2$. By virtue of the Hasse-Minkowski Theorem ([**Ser73**, Ch. IV, Thm. 8]), it is known that the Hasse principle (or local-global principle) holds for X, hence the set $X(K)$ is non-empty if and only if so is the set $X(K_v)$ for every place v of K. Even more, when $X(K) \neq \emptyset$, one can easily parametrise $X(K)$ by intersecting lines in $\mathbb{P}^2$ through a distinguished point $P \in X(K)$; in particular, $X(K)$ is an infinite set. Since the problem of determining whether X has local points everywhere is effectively computable, one can hope to describe the set $X(K)$ precisely.

If $g = 1$ and X has at least one K-rational point, then X is an elliptic curve over K. By the Mordell-Weil Theorem ([**Sil86**, Chapter VIII, Theorem 6.7]), the set $X(K)$ of K-rational points on X inherits a structure of a finitely generated abelian group, thus $X(K) \simeq \mathbb{Z}^r \times T$, where $r := \mathrm{rank}(X(K)) \geq 0$ is an integer, usually referred to as the *algebraic rank* of X over K, and T is a finite group (the torsion part of $X(K)$). Unfortunately, the proof of the Mordell-Weil Theorem does not provide a recipe for r, as its effectiveness for finding a set of generators for $X(K)$ relies on the conjectural finiteness of the Shafarevich-Tate group $Ш(X/K)$ of X. In its more crude version, the Birch and Swinnerton-Dyer (BSD) conjecture (which was formulated in the early 60's in [**BSD63, BSD65**]) predicts that r coincides with the so-called *analytic rank* of X/K, defined as the order of vanishing of the Hasse-Weil L-series $L(X, s)$ attached to X/K at the central point $s = 1$. The strongest evidence in support of the BSD conjecture is given by the Theorems of Gross-Zagier and Kolyvagin (see [**GZ86, Kol90**]), which imply that the BSD conjecture holds true for elliptic curves over $\mathbb{Q}$ of analytic rank at most 1. The proof of this result exploits the construction of Heegner systems arising from CM points on modular curves, thus it relies crucially on the modularity of elliptic curves over $\mathbb{Q}$, conjectured by Shimura, Taniyama and Weil and proved after a series of works building on a fundamental breakthrough of Wiles [**Wil95**] and Taylor-Wiles [**TW95**], see [**BCDT01**]. Although the recent work of Bhargava and Shankar shows that a large proportion of elliptic curves over $\mathbb{Q}$ have analytic rank at most 1 (see [**BS13d, BS13b**]), hence they satisfy the BSD conjecture thanks to the Theorem of Gross-Zagier and Kolyvagin, the general conjecture still remains widely open. So even if one knows a priori that X possesses a K-rational point, describing the set $X(K)$ is in general a hard problem.

Nevertheless, a general curve X/K of genus one need not have a rational point. Two of the most famous examples in the literature illustrating this phenomenon are the smooth projective

[1]From a computational point of view, this problem is closely related to Hilbert's 10th problem, which asked for an algorithm to determine whether a given polynomial Diophantine equation with integer coefficients has an integer solution; by the work of Matiyasevich [**Mat70**], such an algorithm does not exist.

models of the affine quartic curve $2y^2 = 1 - 17x^4$, due to Lind and Reichardt, and of Selmer's cubic $3x^3+4y^3 = 5$. These curves have rational points locally everywhere, but fail to have global $\mathbb{Q}$-rational points, thus they are counterexamples to the Hasse principle (see [**Lin40, Rei42, Sel51**]). Genus one curves violating the Hasse principle, like the previous ones, represent non-trivial elements in certain Shafarevich-Tate groups. Indeed, the Jacobian $\mathrm{Jac}(X)$ of a genus one curve X/K is an elliptic curve over K, and X is a *principal homogeneous space* of its Jacobian $\mathrm{Jac}(X)$. This is the same as saying that there is an isomorphism $X \times_K \bar{K} \simeq \mathrm{Jac}(X) \times_K \bar{K}$, and also a morphism of algebraic varieties $\mathrm{Jac}(X) \times X \to X$ over K which becomes equivalent to the addition law on $\mathrm{Jac}(X) \times_K \bar{K}$ after base change to $\bar{K}$ (using the previous isomorphism). The Shafarevich-Tate group $Ш(\mathrm{Jac}(X)/K)$ of $\mathrm{Jac}(X)/K$ is then defined as the set of principal homogeneous spaces for $\mathrm{Jac}(X)$ which have K_v-rational points for all places v of K, up to isomorphism of principal homogeneous spaces for $\mathrm{Jac}(X)$ over K (see [**Cas91**, §23]). The trivial class in this group corresponds to the isomorphism class of those principal homogeneous spaces having a K-rational point, thus $Ш(\mathrm{Jac}(X)/K)$ measures the failure of the Hasse principle for X. If $Ш(\mathrm{Jac}(X)/K)$ is finite, which is conjecturally true, then there should be an algorithm for deciding whether the set $X(K)$ is empty or not.

Concerning the question of deciding whether a genus one curve has a rational point or not, we shall mention the recent work of Bhargava in [**Bha14**], where he investigates the problem of determining how frequently does a plane cubic have a rational point. In particular, he shows that a positive proportion of plane cubics fail the Hasse principle, using the results of Bhargava-Shankar on the average size of the n-Selmer groups (for $n \leq 5$) of elliptic curves over $\mathbb{Q}$ when ordered by height ([**BS13c, BS13d, BS13a, BS13b**]).

Finally, the paradigm for curves X/K of genus $g \geq 2$ is totally different. As conjectured by Mordell [**Mor22**] and proved by Faltings [**Fal83**], the set of K-rational points on X is *finite*. The distinct proofs of Falting's Theorem provide upper bounds for the cardinality of the set $X(K)$, but they do not provide an effective algorithm to describe this set. In fact, they are not able to even determine whether $X(K)$ is empty or not. One can first attempt to prove the emptiness of $X(K)$ by local methods, that is to say, by showing that $X(K_v)$ is empty for some place v of K, which a priori is an effectively computable problem. If this does not succeed, a plethora of methods trying to describe the set $X(K)$ or to find a point in this set exist in the literature (see [**Bru13**]). If one knows a priori or can prove that X has points everywhere locally but fails to have K-rational points, it is also an interesting question to find an explanation to the failure of the local-global principle, i.e. to detect an obstruction for the Hasse principle to hold for X. In this direction, several cohomological obstructions have been investigated by the school of Skorobogatov, Colliot-Thélène, Sansuc, Demarche, and others, like for example the Brauer-Manin and descent obstructions, as well as refinements of them (see [**Sko01**]). We develop a bit more on this topic in Section 4 of Chapter 1. From a distinct point of view, Poonen and Stoll [**PS14**] have recently proved that a positive proportion of hyperelliptic curves over $\mathbb{Q}$ have at most one rational point, using a reformulation of Chabauty's method and results of Bhargava and Gross in [**BG13**] on the average behavior of 2-Selmer groups of hyperelliptic Jacobians.

Back to our purposes, modular and Shimura curves have great arithmetic significance, for they are moduli spaces of (fake) elliptic curves and, at the same time, thanks to the work of Eichler, Shimura and Wiles, give rise to modular parametrisations of all elliptic curves over $\mathbb{Q}$. The study of diophantine properties of these curves is therefore of fundamental importance in number theory. We shall emphasise that equations for Shimura curves are in general hard to find (the interested reader may consult, for example, the works of Kurihara [**Kur79**], Gonzàlez-Rotger [**GR04, GR06**], Molina [**Mol12**], Franc-Masdeu [**FM14**] and Voight-Willis [**VW14**]), and this is one of the reasons why they are seldom used to study rational points, as many of the methods alluded to above require the equations of the curve under investigation.

In his celebrated article [**Maz77**], Mazur proved that for integers $N \geq 13$ the only rational points on the modular curve $X_1(N)$ are cusps. This result yields in turn the classification of

rational torsion subgroups of elliptic curves over $\mathbb{Q}$. Mazur's work started a research line which was intensively and successfully explored by Kenku [**Ken81**], Momose [**Mom84, Mom87**], Jordan [**Jor86**] and many others, both for modular and Shimura curves. The general philosophy is that rational points on modular and Shimura curves should correspond only to cusps or (fake) elliptic curves with complex multiplication, except for a few exceptional cases.

Keeping in mind the circle of ideas already present in some of these works, this thesis aims to investigate and propose new approaches for studying the lack of rational points over number fields on Shimura curves and their Atkin-Lehner quotients, and to exhibit more evidence in support of the above general philosophy. Furthermore, it is also our purpose to show that these curves provide a wealth of counterexamples to the Hasse principle, thus they can be used to test cohomological obstructions to this local-global principle, as for example the Brauer-Manin obstruction.

In order to describe more precisely the contents of this thesis, let us denote by $X_D/\mathbb{Q}$ the Shimura curve associated with a maximal order $\mathcal{O}_D$ in an indefinite rational quaternion algebra B_D of reduced discriminant D, which is the coarse moduli scheme for abelian surfaces with quaternionic multiplication (QM) by $\mathcal{O}_D$ (see Section 3 of Chapter 1 below). By a Theorem of Shimura (see [**Shi75**]), X_D has no real points, so a fortiori $X_D(\mathbb{Q}) = \emptyset$. Besides, Jordan and Livné [**JL85**] characterised the existence of local points at non-archimedean places on X_D over arbitrary number fields. However, despite having a good control of local points, the existence of *global* points on curves X_D over number fields is much more challenging, yet the works available so far do support the general philosophy referred to above: such global points seem to correspond only to abelian surfaces with complex multiplication, apart from exceptional cases. Similarly, after the work of Ogg [**Ogg83, Ogg85**] and Rotger-Skorobogatov-Yafaev [**RSY05**], the existence of ($\mathbb{Q}$-)adèlic points on Atkin-Lehner quotients is completely characterised, but although these curves are expected to fail having (global) rational points very often, there exists no general approach to prove this belief so far. From a moduli point of view, the expected absence of rational points on Atkin-Lehner quotients is related to a finiteness conjecture attributed to Coleman about the possible isomorphism classes of $\bar{\mathbb{Q}}$-endomorphism algebras of abelian surfaces of GL_2-type (see [**BFGR06**]).

Inspired by the results of Jordan [**Jor81, Jor86**] and Skorobogatov [**Sko05**], one of the main ingredients in this thesis is a cyclic Galois covering of Shimura curves over $\mathbb{Q}$

$$X_{D,\ell} \longrightarrow X_D$$

associated with an odd prime ℓ dividing D. It was firstly introduced by Jordan in [**Jor81**, Chapter 5], and its maximal étale quotient is referred to[2] as the *Shimura covering of X_D at ℓ*. Here, $X_{D,\ell}/\mathbb{Q}$ is the coarse moduli scheme classifying abelian surfaces with QM by $\mathcal{O}_D$ together with a generator for their canonical torsion subgroup at ℓ (cf. Section 1 of Chapter 2 below).

Although it will not be relevant for the goals of this thesis, we must mention that curves $X_{D,\ell}$ are of arithmetic interest also in other scenarios. For instance, the Jacobian variety $J_{D,\ell}$ of $X_{D,\ell}$ provides a compatible system of Galois representations whose local conductor at ℓ is ℓ^2. Furthermore, if we set $D_0 := D/\ell$, the theory of Jacquet-Langlands on automorphic representations of twists of GL_2 shows that automorphic forms on the classical modular curve $X_0(\ell^2 D_0)$ may be lifted to $X_{D,\ell}$. This affords a modular parametrisation $\pi_{D,\ell} : J_{D,\ell} \to E$ of any elliptic curve $E/\mathbb{Q}$ of conductor $\ell^2 D_0$, which becomes particularly interesting for applications to the theory of Heegner systems and the BSD conjecture when the local root number of E at ℓ is -1 (cf. [**LRV**]).

The results obtained in this thesis can be divided into two parts. The first part, which we next describe, is concerned with the geometry and the arithmetic of the covering $X_{D,\ell} \to X_D$, and explores the existence of local points at bad reduction primes on its intermediate curves and their Atkin-Lehner quotients.

First of all, and in contrast to the case of the Shimura curve X_D, the curve $X_{D,\ell}$ is not geometrically connected. Indeed, let $\mathbb{Q}(\mu_\ell)/\mathbb{Q}$ denote the ℓ-th cyclotomic extension over $\mathbb{Q}$. Then $X_{D,\ell} \times_{\mathbb{Q}} \mathbb{Q}(\mu_\ell)$ decomposes as a union of $\ell - 1$ geometrically connected curves, which are conjugated

[2] This terminology was already used by Mazur in [**Maz77**, p. 67] in the classical setting of modular curves.

freely and transitively by the action of $\mathrm{Gal}\,(\mathbb{Q}(\mu_\ell)/\mathbb{Q})$. Further, the group $\Delta := \mathrm{Aut}(X_{D,\ell}/X_D) \subseteq \mathrm{Aut}_{\mathbb{Q}}(X_{D,\ell})$ of covering automorphisms of $X_{D,\ell} \to X_D$ is cyclic of order $(\ell^2-1)/2$, and it can be described by local means. More precisely, let us write $\mathcal{O}_{D,\ell} := \mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ for the $\mathbb{Z}_\ell$-order of the local quaternion algebra $B_{D,\ell} := B_D \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$, and let I_ℓ be the unique maximal ideal in $\mathcal{O}_{D,\ell}$. Then one has explicit isomorphisms

$$\Delta \simeq \mathcal{O}_{D,\ell}^\times/\{\pm 1\}(1+I_\ell) \simeq \mathbb{F}_{\ell^2}^\times/\{\pm 1\}.$$

A precise description of the geometry of $X_{D,\ell}$ and the group Δ is elaborated in Sections 1 and 2 of Chapter 2.

On the other hand, the Atkin-Lehner involutions ω_m associated to positive divisors m of D acting on X_D can be lifted to rational involutions $\hat{\omega}_m$ on $X_{D,\ell}$ (cf. Section 3 of Chapter 2). They behave in the same manner as the classical involutions ω_m do, and give rise to an abelian subgroup $W_{D,\ell} \simeq (\mathbb{Z}/2\mathbb{Z})^{2r}$ of $\mathrm{Aut}_{\mathbb{Q}}(X_{D,\ell})$, where $2r$ is the number of prime factors of D.

Actually, both Δ and $W_{D,\ell}$ are subgroups of the so-called group of *modular automorphisms* $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ of $X_{D,\ell}$ (see Definition 1.35), and even more, $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ is recovered as a semi-direct product of Δ and $W_{D,\ell}$ (see Theorem 2.1). As a consequence of the study of $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$, we can obtain Galois étale coverings of both $X_D/\mathbb{Q}$ and $X_D^{(m)}/\mathbb{Q}$, where $X_D^{(m)}$ denotes the Atkin-Lehner quotient of X_D by the action of the involution ω_m.

Indeed, let us denote by $Y_d \to X_D$ the unique intermediate covering of $X_{D,\ell} \to X_D$ of degree d, where d is a positive divisor of $(\ell^2-1)/2$. Namely, $Y_d/\mathbb{Q}$ arises as the quotient of $X_{D,\ell}$ by the action of the unique index d subgroup of Δ. It was already proved by Jordan [**Jor81**, Chapter 5] that the cyclic covering $Y_d \to X_D$ is étale if and only if d divides $d_{\text{ét}} := (\ell^2-1)/2e$, where $e = e(D)$ is a positive integer dividing 6 which depends only on the arithmetic of B_D (cf. Section 5 of Chapter 2 below). If for a positive divisor m of D we write $Y_d^{(m)}/\mathbb{Q}$ for the quotient of Y_d by the action of the lifted Atkin-Lehner involution $\hat{\omega}_m$, it is not true in general that the induced covering $Y_d^{(m)} \to X_D^{(m)}$ is étale, even if $d \mid d_{\text{ét}}$. Actually, it might also fail being a Galois covering. However, we can impose certain conditions under which $Y_d \to X_D$ induces a cyclic étale covering $Y_d^{(m)} \to X_D^{(m)}$ (see Theorem 2.2).

The construction of (cyclic) étale coverings of curves X_D and their Atkin-Lehner quotients allows to set out a descent strategy for the study of rational points on these curves over number fields. Suppose for example that $g_d^{(m)} : Y_d^{(m)} \to X_D^{(m)}$ is an étale covering as above, with cyclic automorphism group of order d. Descent theory provides a partition of the set $X_D^{(m)}(\mathbb{Q})$ of rational points on $X_D^{(m)}$ in terms of the twisted forms of $g_d^{(m)}$. Namely, one has

$$X_D^{(m)}(\mathbb{Q}) = \bigsqcup_{\tau \in \mathrm{H}^1(G_{\mathbb{Q}}, \mathbb{Z}/d\mathbb{Z})} {}^{\tau}g_d^{(m)}({}^{\tau}Y_d^{(m)}(\mathbb{Q})),$$

where $G_{\mathbb{Q}} = \mathrm{Gal}\,(\bar{\mathbb{Q}}/\mathbb{Q})$ denotes the absolute Galois group of $\mathbb{Q}$, ${}^{\tau}g_d^{(m)} : {}^{\tau}Y_d^{(m)} \to X_D^{(m)}$ stands for the twisted form of the étale covering $g_d^{(m)}$ by the cohomology class τ, and we identify $\mathrm{Aut}_{\mathbb{Q}}(Y_d^{(m)}/X_D^{(m)}) = \mathrm{Aut}(Y_d^{(m)}/X_D^{(m)})$ with the cyclic group $\mathbb{Z}/d\mathbb{Z}$ of d elements. In particular, since $G_{\mathbb{Q}}$ acts trivially on $\mathbb{Z}/d\mathbb{Z}$, notice that cohomology classes in $\mathrm{H}^1(G_{\mathbb{Q}}, \mathbb{Z}/d\mathbb{Z})$ can be regarded as group homomorphisms $\tau : G_{\mathbb{Q}} \to \mathbb{Z}/d\mathbb{Z}$. Moreover, it follows from a standard result from descent theory that one only needs to consider those characters τ such that the field extension $L_\tau := \bar{\mathbb{Q}}^{\ker(\tau)} \subseteq \bar{\mathbb{Q}}$ over $\mathbb{Q}$ cut out by τ is unramified away from D, as otherwise the set ${}^{\tau}Y_d^{(m)}(\mathbb{Q})$ is empty. Then, a plausible strategy consists in proving that $Y_d^{(m)}$ and its twists by the (finitely many) cohomology classes satisfying the previous condition fail to have local points at some place of $\mathbb{Q}$. By virtue of the above partition of $X_D^{(m)}(\mathbb{Q})$, this forces the set $X_D^{(m)}(\mathbb{Q})$ to be empty.

Motivated by this strategy, in Chapter 3 we prove criteria for the existence of local points on the intermediate curves Y_d of the covering $X_{D,\ell} \to X_D$ and their Atkin-Lehner quotients at primes of bad reduction distinct from ℓ, i.e. at primes p dividing D/ℓ. The $\mathbb{Z}_p$-integral models $\mathcal{Y}_d$ of the curves Y_d naturally arising from their moduli interpretation are admissible curves over $\mathbb{Z}_p$ in the sense of Jordan-Livné (see Definition 1.65), so that their special fibres are dual to suitable

finite graphs with lengths. More precisely, the theory of Čerednik and Drinfeld on the p-adic uniformisation of Shimura curves (see, e.g., [**Dri76, BC91**]) shows that curves $\mathcal{Y}_d$ are quadratic twists of quotients of Drinfeld's p-adic upper half plane obtained by Mumford uniformisation (commonly known as *Mumford curves*, or rather *Mumford quotients*). In particular, their special fibres are dual to finite quotients of the Bruhat-Tits tree associated to $\mathrm{PGL}_2(\mathbb{Q}_p)$. Appealing to Hensel's Lemma, this combinatorial description can be used to predict the existence of $\mathbb{Q}_p$-rational points on the curves Y_d. Hence, our approach borrows some ideas from Kurihara [**Kur79**], Jordan-Livné [**JL85**] and Ogg [**Ogg85**], and to some extent our results generalise these works. Actually, the existence of local points on curves Y_d and $Y_d^{(m)}$ at bad reduction primes is characterised by congruence conditions of the same nature as in the classical case of X_D and $X_D^{(m)}$, together with conditions on the solutions of certain quadratic equations over finite fields (cf. Theorems 3.1, 3.2 and 3.3).

The reader may notice that we leave aside the case $p = \ell$, and we do so not because that case lacks interest, but rather because the methods required to approach that setting are strikingly different from the ones employed in Chapter 3 (see the comments after Theorem 3.3). Nevertheless, this case is being worked out and we hope to cover it elsewhere. On the other hand, the study of local points at good reduction primes on curves Y_d and $Y_d^{(m)}$ (that is to say, at primes not dividing D) and of real points on curves $Y_d^{(m)}$ leads also to completely different scenarios from the one described above, and we do not deal with them here. Besides, a detailed study of local points on the twists of $Y_d^{(m)}$ completing the descent strategy outlined above has remained beyond the scope of this thesis. We also hope to tackle this problem in the future.

The second part of the thesis is devoted to propose and investigate a method for proving the non-existence of rational points over a number field K on a coarse moduli space X of abelian varieties with additional structure, with special interest in cases where the moduli problem is *not fine* and K-rational points may not be represented by abelian varieties admitting a model over K (this is the generic situation when the abelian varieties that are being classified have even dimension). We exemplify our approach when X is a Shimura curve and K is an imaginary quadratic field, and also when X is an Atkin-Lehner quotient of a Shimura curve and K is the field $\mathbb{Q}$ of rational numbers. Our main results provide new counterexamples to the Hasse principle in both scenarios, and in the first one we also prove that such counterexamples are accounted for by the Brauer-Manin obstruction.

The original inspiration for our investigation arises from the work of Jordan in [**Jor86**]. If $X_D/\mathbb{Q}$ denotes the Shimura curve as above and K is an imaginary quadratic field, Jordan's approach is to study the Galois representations of $\mathrm{Gal}\,(\bar{K}/K)$ attached to the abelian surfaces with QM corresponding to K-rational points on X_D. These Galois representations impose certain congruence conditions on B_D and K, thus whenever they are not fulfilled it follows that the set $X_D(K)$ must be empty (see Theorem 6.3 in *ibid.*). However, this strategy requires assuming that such abelian surfaces admit a model rational over K, which is equivalent to assuming that K splits the quaternion algebra B_D, and there is a priori no reason why this hypothesis should be correlated with the existence or non-existence of K-rational points on X_D. When K is not assumed to split B_D, we overcome this by attaching Galois representations to K-rational points on X_D rather than to the abelian surfaces corresponding to them.

More generally, the main idea of our method, inspired by the work of Ellenberg and Skinner [**ES01**] on the modularity of $\mathbb{Q}$-curves, is that one may still attach to a point $P = [A] \in X(K)$ represented by an abelian variety $A/\bar{K}$ (with additional structure) a *Galois representation over its field of moduli*. Namely, a representation

$$\mathrm{Gal}\,(\bar{K}/K) \longrightarrow \mathrm{GL}(T_\ell(A))/\mathrm{Aut}(A),$$

provided that $\mathrm{Aut}(A)$ lies in the centre of $\mathrm{GL}(T_\ell(A))$, regardless A admits a model rational over K or not. As quoted above, we prove how this method applies in the case of Shimura curves and their Atkin-Lehner quotients (see Chapter 5), and we think the same method could be applied also

to more general scenarios (for example, one could extend the ideas to moduli spaces for abelian varieties of higher dimension or with other level structures, or work over higher degree number fields).

Both in the case of Shimura curves and of their Atkin-Lehner quotients, we combine the study of the above Galois representations over fields of moduli with the étale coverings induced by $X_{D,\ell} \to X_D$, in an analogous way as Skorobogatov [**Sko05**] interpreted Jordan's results in [**Jor86**] in terms of descent and the Brauer-Manin obstruction.

More precisely, given the Shimura curve X_D and an imaginary quadratic field K, Theorem 5.1 gives sufficient conditions for the set $X_D(K)$ to be empty. Even more, if $X_D(\mathbb{A}_K)^{\mathrm{Br}}$ denotes the subset of $X_D(\mathbb{A}_K)$ cut out by the Brauer-Manin relations (see Section 4 of Chapter 1 below), the same conditions ensure that $X_D(\mathbb{A}_K)^{\mathrm{Br}}$ is empty, hence all the counterexamples to the Hasse principle arising from Theorem 5.1 are accounted for by the Brauer-Manin obstruction. Special attention is deserved to those pairs (D, K) such that $X_D(K_v) \neq \emptyset$ for every place v of K but which do not fulfill the hypotheses of [**Jor86**, Theorem 6.3]. These pairs were called *exceptional* by Jordan, as the emptiness of $X_D(K)$ in these cases can be tackled neither by using local methods nor by using [**Jor86**, Theorem 6.3]. In Table 1 of Chapter 5 we list some exceptional pairs (D, K) for which X_D is a counterexample to the Hasse principle over K that can be produced using Theorem 5.1; in particular, they are accounted for by the Brauer-Manin obstruction. To the best of our knowledge, these exceptional pairs were rather inaccessible so far, thus these examples were not known before.

Regarding the case of Atkin-Lehner quotients $X_D^{(m)}$ of X_D, we exploit the moduli interpretation of these curves in terms of abelian surfaces with real multiplication and potential quaternionic multiplication (see Section 3.4 of Chapter 1 below) and apply again the method introduced in Chapter 4 using Galois representations over fields of moduli combined with the étale coverings of $X_D^{(m)}$ constructed as in Chapter 2. The main result is stated in Theorem 5.2, whose proof goes along the same lines as the one of Theorem 5.1. Combined with the criterion in [**RSY05**, Theorem 3.1] for the existence of adèlic points on Atkin-Lehner quotients of Shimura curves, Theorem 5.2 can be used to produce curves $X_D^{(m)}$ violating the Hasse principle over $\mathbb{Q}$: some particular instances are listed in Table 2 of Chapter 5. However, in this case we cannot prove that such counterexamples to the Hasse principle are accounted for by the Brauer-Manin obstruction. And the reason seems to rely on the fact that the obstruction for a point $Q \in X_D^{(m)}(\mathbb{Q})$ to be represented by an abelian surface admitting a model over $\mathbb{Q}$ does a priori depend on the point Q (see Theorem 4.26). This is in contrast with the previous scenario, where the obstruction for an abelian surface representing a point $P \in X_D(K)$ to admit a model over K does not depend on the point P (see Theorem 4.20).

We shall mention here that Theorem 5.2 (together with Corollary 5.21), predicting the non-existence of rational points on Atkin-Lehner quotients of Shimura curves, complements previous works on this problem by other authors. In [**Cla03**], for example, Clark investigated the existence of local and global rational points on the quotient of Shimura curves X_D by the Atkin-Lehner involution ω_D, and showed that $X_D^{(D)}$ has rational points over every completion of $\mathbb{Q}$. In [**RSY05**], as we have already mentioned, Rotger, Skorobogatov and Yafaev characterised the existence of adèlic points on curves $X_D^{(m)}$ for an arbitrary positive divisor m of D, building on previous work of Ogg. When D is the product of two distinct odd primes ℓ and m, and the natural quotient map $X_{\ell m} \to X_{\ell m}^{(m)}$ is unramified, they also applied descent techniques to this torsor under the constant group scheme $\mathbb{Z}/2\mathbb{Z}$ to prove the emptiness of $X_{\ell m}^{(m)}(\mathbb{Q})$ under certain conditions, showing for example that $X_{23\cdot 107}^{(107)}$ is a counterexample to the Hasse principle over $\mathbb{Q}$.

On the other hand, Parent and Yafaev [**PY07**] have given a method for studying global rational points on some Atkin-Lehner quotients of Shimura curves. Namely, they tackle the problem under the assumption that $D = pm$ is the product of two odd primes with $p \equiv 1 \pmod 4$ and $m \equiv 3 \pmod 4$, which in the terminology of Ogg [**Ogg85**] corresponds to the "non-ramifié" case. The work of Parent and Yafaev then gives sufficient conditions for rational points on $X_{pm}^{(m)}$ to arise

necessarily from CM points on X_{pm}, and they find an infinite family of such quotients satisfying these conditions. This work was taken a step further by Gillibert in [**Gil13**], where Parent-Yafaev conditions are made explicit.

Especially when comparing Theorem 5.2 and Corollary 5.21 with the results in [**PY07, Gil13**], we must emphasise that we place ourselves in cases where $D = pm$ is odd, with $p \geq 7$ a prime number such that $p \equiv 3 \pmod 4$. Therefore, our results do not overlap with the work in [**PY07, Gil13**].

Finally, in Section 3 of Chapter 5 we show still another approach to prove the scarcity of rational points on certain Atkin-Lehner quotients of Shimura curves, which follows essentially from the ideas and techniques in [**Rot08**]. Notice that the proof of Theorem 5.25 is much simpler than the one of Theorem 5.2, mainly because all rational points can be represented by an abelian surface that admits a model over $\mathbb{Q}$, and therefore one can work directly with the usual Galois representations. Nevertheless, we find it is worth including it, as it strengthens the results of [**RSY05**] and is directly related to Coleman's conjecture as described in [**BFGR06**].

Organisation of this thesis. Although the above exposition already outlines how the contents of this thesis are organised, let us briefly explain the distribution of this work into chapters. The first chapter reviews and summarises some fundamental notions of the theories and techniques that are used along the thesis, and we obviously claim no authorship on the results appearing in it. Chapter 2 is devoted to study the geometry of the cyclic Galois covering $X_{D,\ell} \to X_D$ of a Shimura curve $X_D/\mathbb{Q}$ attached to an odd prime ℓ dividing D. We also determine the structure of $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ as an abstract group, and as an application we construct Galois étale coverings of Atkin-Lehner quotients of X_D. The material of Chapter 2 corresponds essentially to the work published in [**Ver13**].

In Chapter 3 we accomplish the first part of the descent strategy sketched above towards the study of (global) rational points on Atkin-Lehner quotients of Shimura curves. Namely, we give criteria for the existence of local points at bad reduction primes $p \mid D/\ell$ on intermediate curves of the covering $X_{D,\ell} \to X_D$ and their Atkin-Lehner quotients. The main results are stated in Theorems 3.1, 3.2 and 3.3, and the work in this chapter has been submitted for publication in [**Verb**].

The goal of Chapter 4 is to introduce the method we have explained above for studying rational points over number fields on coarse moduli spaces for abelian varieties with additional structure, by using what we call Galois representations over fields of moduli. We do this first in a quite general setting, and then we work in detail the two particular scenarios we are concerned with in this thesis: the case of Shimura curves over imaginary quadratic fields and the case of Atkin-Lehner quotients of Shimura curves over the field of rational numbers. Finally, in Chapter 5 we combine this method with descent techniques applied to the étale coverings obtained in Chapter 2 to prove new results on the scarcity of global points on Shimura curves and their Atkin-Lehner quotients over imaginary quadratic fields and over $\mathbb{Q}$, respectively, as we outlined above. The contents of Chapters 4 and 5 are joint work with V. Rotger and have appeared in [**RV14**].

Acknowledgements

First and foremost, it is a pleasure to thank Victor Rotger for his enormous support and guidance during these years. He has taught me how to do and write research, and without him this thesis would not have been possible. He has always been open to attend my questions and help me when I was stuck, and I have enjoyed many fruitful conversations with him, sharing a blackboard or just a piece of paper in a cafeteria. I hope we can continue collaborating for many years. Thank you very much for your time, patience and advice, Victor.

I am also indebted to Jordi Quer, who first encouraged me to embark on a PhD and drawed my attention to number theory. I would like to extend this gratitude to the whole number theory research group at UPC. My thanks also go to the members of the *Seminari de Teoria de Nombres de Barcelona*, who have doubtless contributed to broaden my number-theoretic background. Among them, I am especially grateful to Elisa, Piermarco, Nuno, Laia, Daniele and Pietro, with whom I have shared and enjoyed many moments.

During my time at the Departament de Matemàtica Aplicada II, the daily work has been much more pleasant with Arnau, Maria, Rodrigo, Inês, Aaron, Elisa, Lander, Matias and Anna. Thank you for sharing lunches, coffees and laughs every day.

I wish to thank the Number Theory Group of the University of Warwick for their warm hospitality during the spring of 2012, especially to Professors John Cremona and Samir Siksek for many inspiring conversations. I benefited a lot from numerous seminars at the Warwick Mathematics Institute during that period, and also from several discussions at the tea room.

Vorrei ringraziare il Professore Matteo Longo (e il Gruppo di Geometria Algebrica e Teoria dei Numeri dell'Università degli Studi di Padova) per la loro gentile ospitalità durante la primavera del 2013. Per avermi fatto sentire come a casa, per il loro interesse in questa tesi e per portare la mia attenzione su nuove direzioni di ricerca. Je remercie aussi le Professeur Pierre Parent pour s'être intéressé à ce travail et pour en avoir fait une lecture du manuscrit finale.

Aquesta tesi tampoc hauria estat possible sense totes aquelles persones que durant aquests anys han estat a prop meu. Més del que potser imaginen, totes elles han contribuït a que aquest treball hagi tirat endavant, compartint riures, alegries, i també oferint-me el seu suport quan ho he necessitat. Gràcies a tots i totes. Però sobretot, vull agrair a la meva família, per encoratjar-me a emprendre aquesta aventura fa quatre anys i per fer-me costat en tot moment. En especial, al meu germà Marcos, per ser un germà gran excepcional, i també a l'Helena i al petit Raül, capaç de fer-me somriure tan sols mirant-me. Al meu pare, José Luis, perquè sempre ha estat i serà un referent per mi. I a la meva mare, Gema, per estimar-me com ho va fer i per ensenyar-me tant i tant amb el seu exemple.

Barcelona, setembre de 2014.

CHAPTER 1

Preliminaries

We devote this first chapter to review some fundamental notions concerning the main objects of study in this thesis and the techniques that we use. Starting with a (very) brief summary of the general theory of abelian varieties and quaternion algebras, in Section 3 we introduce Shimura curves in a fairly general framework according to the purposes of this work, and after this we devote a few pages to the Brauer-Manin and descent obstructions to the existence of rational points on varieties. Finally, the last section collects some useful definitions and results related to admissible curves obtained by Mumford's uniformisation, which will be especially useful in Chapter 3.

1. Abelian varieties and their endomorphism algebras

We start by reviewing some basic facts about abelian varieties, with special emphasis on the study of the endomorphisms of simple abelian varieties. A standard reference for the complex theory, in which abelian varieties are the same as polarisable complex tori, is [**BL92**]. We rather present here an algebraic point of view, for which we refer the reader to [**Mum70**] and [**Mil08**], for example.

1.1. Basic definitions and properties. Let k be a field, and fix a separable closure k^s of k. All the field extensions of k that we consider should be regarded as subfields of k^s. An *abelian variety over* k is by definition a complete group variety defined over k. That is to say, a complete algebraic variety A defined over k together with a k-rational point $o \in A(k)$ and morphisms $m : A \times A \to A$ and $i : A \to A$ defined over k satisfying the group axioms. Recall that an algebraic variety V is said to be *complete* if for every algebraic variety W, the projection $q : V \times W \to W$ is closed. Complete varieties are then the analogues in the category of algebraic varieties of compact topological spaces in the category of Hausdorff topological spaces.

The completeness of A implies that its group law is abelian. Then, it is usually written by $+$, and the identity element is denoted by 0_A, or just by 0 if the abelian variety A is clear by the context. Moreover, abelian varieties are non-singular, and this allows one to identify Weil divisors and invertible sheaves. Indeed, recall that a *Weil divisor on* A is a formal sum $D = \sum n_Y Y$, where Y runs over the subvarieties of codimension 1 of A and $n_Y \in \mathbb{Z}$. Then it is usual to write

$$\mathrm{CH}^1(A) := \{\text{Weil divisors on } A\}/\{\text{Principal divisors on } A\}$$

for the *first Chow group* of A. On the other hand, an *invertible sheaf on* A is a locally free sheaf $\mathcal{L}$ of rank 1 on A. The set $\mathrm{Pic}(A)$ of isomorphism classes of invertible sheaves on A has a natural group structure, with the group law induced by the tensor product of sheaves and for which $\mathcal{O}_A$, the structural sheaf of A, is the identity element. Since A is non-singular, there is an isomorphism

$$\mathrm{CH}^1(A) \xrightarrow{\simeq} \mathrm{Pic}(A), \quad [D] \longmapsto \mathcal{O}_A(D).$$

Let $\mathcal{L} \in \mathrm{Pic}(A)$ be an invertible sheaf, and write $\mathcal{L} = \mathcal{O}_A(D)$ for some Weil divisor D. Then, if the k-vector space of global sections

$$\mathrm{H}^0(A, \mathcal{L}) \simeq \{f \in k(A)^\times : \mathrm{div}(f) + D \geq 0\} \cup \{0\}$$

has a k-basis $\{s_1, \ldots, s_n\}$, $\mathcal{L}$ induces a morphism

$$\Psi_{\mathcal{L}} : A \longrightarrow \mathbb{P}^{n-1}, \qquad a \longmapsto [s_1(a) : \cdots : s_n(a)].$$

DEFINITION 1.1. *The invertible sheaf $\mathcal{L}$ is said to be* very ample *if $\Psi_{\mathcal{L}}$ induces a closed immersion. An* ample invertible sheaf *or* polarisation *is an invertible sheaf $\mathcal{L}$ such that $\mathcal{L}^{\otimes n}$ is very ample for some $n \geq 1$.*

A theorem of Lefschetz states that if $\mathcal{L}$ is an ample invertible sheaf, then $\mathcal{L}^{\otimes n}$ is very ample for $n \geq 3$. When $\mathcal{L}$ is a polarisation, the global sections $s \in \mathrm{H}^0(A, \mathcal{L})$ are called the *theta functions* of A with respect to $\mathcal{L}$, and we say that the pair $(A, \mathcal{L})$ is a *polarised abelian variety*. Observe that from the very definitions:

PROPOSITION 1.2. *An abelian variety is projective if and only if it admits a polarisation.*

As a complex variety, $A(\mathbb{C}) \simeq \mathbb{C}^g/\Lambda$, where $\Lambda \subseteq \mathbb{C}^g$ is a complete lattice. Then, the first Chern class $c_1(\mathcal{L})$ of an invertible sheaf $\mathcal{L} \in \mathrm{Pic}(A)$ can be regarded as a Hermitian form

$$H : \mathbb{C}^g \times \mathbb{C}^g \longrightarrow \mathbb{C}$$

such that $\mathrm{Im}H(\Lambda \times \Lambda) \subseteq \mathbb{Z}$. Equivalently, as an alternate $\mathbb{R}$-bilinear form

$$E = \mathrm{Im}H : \mathbb{C}^g \times \mathbb{C}^g \longrightarrow \mathbb{R}$$

which is integral when restricted to $\Lambda \times \Lambda$ and such that

$$E(\sqrt{-1}x, \sqrt{-1}y) = E(x, y) \quad \forall\ x, y \in \mathbb{C}^g.$$

An invertible sheaf $\mathcal{L}$ on A is a polarisation if and only if H is positive definite, and if this is the case the *degree* of $\mathcal{L}$ is defined by

$$\deg(\mathcal{L}) := \sqrt{\det(E)},$$

which is also the dimension of $\mathrm{H}^0(A, \mathcal{L})$ as a complex vector space.

With the same notations, assume that $(A, \mathcal{L})$ is a polarised abelian variety, and choose a symplectic basis of the lattice Λ. That is, a $\mathbb{Z}$-basis of Λ for which the matrix expression of E is of the form

$$\begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix}$$

for some $D = \mathrm{diag}(d_1, d_2, \ldots, d_g)$, $d_i \in \mathbb{N}$, with $d_j | d_{j+1}$ for $j = 1, \ldots, g-1$. The existence of such a basis is guaranteed by the Elementary Divisor Theorem. Then, the tuple $(d_1, d_2, \ldots, d_g)$ is called the *type* of the polarisation $\mathcal{L}$, which does not depend on the choice of the symplectic basis, and its degree is easily read: $\deg(\mathcal{L}) = d_1 \cdots d_g$. The polarisation $\mathcal{L}$ is *primitive* if $d_1 = 1$, and it is *principal* if $d_1 = \cdots = d_g = 1$.

EXAMPLE 1.3. *Elliptic curves are abelian varieties of dimension one.* Over the field $\mathbb{C}$ of complex numbers, it is well-known that every elliptic curve is isomorphic to a complex torus $A_\tau = \mathbb{C}/\Lambda_\tau$, with $\Lambda_\tau = \mathbb{Z} \oplus \mathbb{Z}\tau$ for some $\tau \in \mathcal{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$. Moreover, every one-dimensional complex torus is polarisable, hence every complex torus of dimension one is an elliptic curve. However, in higher dimension this is not true, and a *generic* complex torus of dimension $g > 1$ is not algebraic.

EXAMPLE 1.4. *The Jacobian of a curve.* If C is an irreducible non-singular curve of genus g over a field k, then the subgroup $\mathrm{Pic}^0(C_{\bar{k}}) \subseteq \mathrm{Pic}(C_{\bar{k}})$ of invertible sheaves on $C_{\bar{k}} := C \times_k \bar{k}$ invariant under translation is the set of $\bar{k}$-rational points of an abelian variety of dimension g, *the Jacobian of C*. Furthermore, the Jacobian of C is equipped with a canonical principal polarisation (see [**Mil08**, Chapter III]).

1.2. Homomorphisms and isogenies. Suppose A and B are two abelian varieties over k. A regular morphism of algebraic varieties $A \to B$ over k is said to be a *homomorphism (of abelian varieties)* if the induced map $A(k^s) \to B(k^s)$ is a group homomorphism. The set of all such homomorphisms will be denoted by $\mathrm{Hom}_k(A,B)$. It has a group structure in the natural way.

The group of endomorphisms $\mathrm{End}_k(A) := \mathrm{Hom}_k(A,A)$ of an abelian variety over k is of particular interest. As a $\mathbb{Z}$-module, $\mathrm{End}_k(A)$ is torsion-free and finitely generated. Moreover, $\mathrm{End}_k(A)$ is endowed with a natural ring structure in which the product law is given by the composition of endomorphisms. When this structure is considered, $\mathrm{End}_k(A)$ is rather referred to as the *endomorphism ring* of A. Further, $\mathrm{End}_k^0(A) := \mathrm{End}_k(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ inherits a natural structure of a $\mathbb{Q}$-algebra: it is the so-called *endomorphism algebra* of A.

Remark 1.5. The subscript k in $\mathrm{Hom}_k(A,B)$, $\mathrm{End}_k(A)$ reminds the reader that we are considering homomorphisms defined over k. When the field k is clear, it might be omitted, but it is often convenient to keep it in order to avoid confusions. It is important to note that, if k is not algebraically closed, there may exist homomorphisms $A \to B$ not defined over k, but over some field extension K/k. We will write $\mathrm{Hom}_K(A,B)$ for the group $\mathrm{Hom}_K(A_K, B_K)$ of homomorphisms $A_K \to B_K$ defined over K, where $A_K := A \times_k K$ is the base change of A from k to K, and similarly for B_K. In particular, $\mathrm{End}_K(A)$ stands for $\mathrm{Hom}_K(A,A)$.

The natural Galois action of $\mathrm{Gal}\,(k^s/k)$ on both $A(k^s)$ and $B(k^s)$ induces an action of $\mathrm{Gal}\,(k^s/k)$ on $\mathrm{Hom}_{k^s}(A,B)$ given by the following rule: if $\sigma \in \mathrm{Gal}\,(k^s/k)$ and $f \in \mathrm{Hom}_{k^s}(A,B)$, then $(\sigma \cdot f)(x) := {}^{\sigma}(f({}^{\sigma^{-1}}x))$. This way, for every field extension K/k we have

$$\mathrm{Hom}_K(A,B) = \{f \in \mathrm{Hom}_{k^s}(A,B) : \sigma \cdot f = f \text{ for all } \sigma \in \mathrm{Gal}\,(k^s/K)\}.$$

Given A and B, there exists a finite field extension L/k such that L is the smallest field of definition of all the homomorphisms from A to B (see [**Sil92**]), that is to say, $\mathrm{Hom}_L(A,B) = \mathrm{Hom}_{k^s}(A,B)$.

Suppose now that $f : A \to B$ is a homomorphism of abelian varieties defined over k. Then f is said to be an *isogeny* if it is surjective and has finite kernel. When this is the case, the extension of function fields given by the induced morphism $f^* : k(B) \to k(A)$ is finite, and its degree is by definition the *degree* of f, $\deg(f) := [k(A) : k(B)]$. Hence, the degree of an isogeny is clearly multiplicative: if $g : B \to C$ is another isogeny, then $\deg(g \circ f) = \deg(g)\deg(f)$. If there exists an isogeny $f : A \to B$ over k, it is said that A and B are *isogenous* over k, and it is denoted by $A \sim_k B$.

The first examples of isogenies are the 'multiplication by n maps' on an abelian variety A. For a positive integer n, the multiplication by n on A is usually denoted by $n_A : A \to A$, and given by $x \mapsto nx$ on points using the group law. The endomorphism n_A is an isogeny of degree n^{2g}, where $g = \dim(A)$. These isogenies are important since they give us information about the torsion part of the group $A(k^s)$ of k^s-rational points of A. The group structure of the kernel $A[n]$ of n_A is well-known:

$$\begin{cases} A[n](k^s) \simeq (\mathbb{Z}/n\mathbb{Z})^{2g} & \text{if } \mathrm{char}(k) \nmid n, \\ A[p^m](k^s) \simeq (\mathbb{Z}/p^m\mathbb{Z})^i & \text{if } \mathrm{char}(k) = p > 0, \text{ for some integer } 0 \le i \le g. \end{cases}$$

Observe that being n_A defined over k, there is a natural action of $\mathrm{Gal}\,(k^s/k)$ on $A[n](k^s)$. Indeed, if $x \in A[n](k^s)$ and $\sigma \in \mathrm{Gal}\,(k^s/k)$, then the point ${}^{\sigma}x$ plainly lies in $A[n](k^s)$ again.

If $f : A \to B$ is an isogeny over k, then there exists an isogeny $g : B \to A$ over k and a positive integer n such that $f \circ g = n_B$, the multiplication by n map on B. In particular, every isogeny $f : A \to B$ has an inverse in the $\mathbb{Q}$-algebra $\mathrm{Hom}_k^0(A,B) := \mathrm{Hom}_k(A,B) \otimes_{\mathbb{Z}} \mathbb{Q}$. Or in other words, isogenies become isomorphisms in the category of abelian varieties over k up to isogeny (see [**Pyl02, Gui10**]).

1.3. Tate modules and ℓ-adic representations. Let ℓ be a prime number. The natural maps $A[\ell^{n+1}](k^s) \to A[\ell^n](k^s)$ induced by the multiplication by ℓ map ℓ_A, make $\{A[\ell^n](k^s)\}_{n\geq 1}$ into an inverse system. The inverse limit

$$T_\ell(A) := \varprojlim A[\ell^n](k^s)$$

is the so-called *ℓ-adic Tate module*. An element $a = (a_n) \in T_\ell(A)$ can therefore be regarded as a sequence of points $a_n \in A(k^s)$, $n \geq 1$, such that $\ell a_1 = 0$ and $\ell a_n = a_{n-1}$ for every $n > 1$.

When $\ell \neq \mathrm{char}(k)$, $T_\ell(A)$ is a free $\mathbb{Z}_\ell$-module of rank $2g$, and sometimes is convenient to consider the $\mathbb{Q}_\ell$-vector space $V_\ell(A) := T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, which has dimension $2g$. Moreover, if E is a subfield of $\mathrm{End}_k^0(A)$, then the action of E on $V_\ell(A)$ gives a structure of free $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$-module of rank $2g/[E : \mathbb{Q}]$ on $V_\ell(A)$.

A homomorphism $f : A \to B$ of abelian varieties induces group homomorphisms $A[n](k^s) \to A[n](k^s)$ for every integer $n \geq 1$, which are compatible with the natural projections, and therefore a $\mathbb{Z}_\ell$-homomorphism $T_\ell(f) : T_\ell(A) \to T_\ell(B)$. In this way, we obtain a map

$$\mathrm{Hom}_k(A, B) \longrightarrow \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell(A), T_\ell(B)), \qquad f \longmapsto T_\ell(f).$$

When $\ell \neq \mathrm{char}(k)$, this map is an injective homomorphism, and it extends to a homomorphism

$$\mathrm{Hom}_k^0(A, B) \longrightarrow \mathrm{Hom}_{\mathbb{Q}_\ell}(V_\ell(A), V_\ell(B)).$$

In particular, when $A = B$ the above argument leads to an injective ring homomorphism

$$T_\ell : \mathrm{End}_k(A) \longrightarrow \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(A)) \simeq \mathrm{M}_{2g}(\mathbb{Z}_\ell),$$

where the isomorphism depends on the choice of a $\mathbb{Z}_\ell$-basis of $T_\ell(A)$. As a consequence, the rank of $\mathrm{End}_k(A)$ as a $\mathbb{Z}$-module is at most $4g^2$.

If $\ell \neq \mathrm{char}(k)$ and $f \in \mathrm{End}_k(A)$, the characteristic polynomial $P_f(T)$ of $T_\ell(f)$ has integral coefficients and, moreover, it does not depend on the prime ℓ, hence it makes sense to call $P_f(T)$ *the characteristic polynomial* of f. Then the *degree* and the *trace* of f are defined as usual in terms of $P_f(T)$. Working with the ℓ-adic representation $V_\ell : \mathrm{End}_k^0(A) \to \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A)) \simeq \mathrm{M}_{2g}(\mathbb{Q}_\ell)$ of $\mathrm{End}_k^0(A)$, the notions of characteristic polynomial, degree and trace can be extended naturally to elements $f \in \mathrm{End}_k^0(A)$.

Finally, the action of $\mathrm{Gal}\,(k^s/k)$ on each of the torsion subgroups $A[\ell^n](k^s)$ for $n \geq 1$ quoted above induces a continuous action of $\mathrm{Gal}\,(k^s/k)$ on $T_\ell(A)$, which gives rise to an *ℓ-adic representation of* $\mathrm{Gal}\,(k^s/s)$. That is to say, a continuous homomorphism

$$\rho_{A,\ell} : \mathrm{Gal}\,(k^s/k) \longrightarrow \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(A)) \simeq \mathrm{GL}_{2g}(\mathbb{Z}_\ell),$$

where again the isomorphism depends on the choice of a $\mathbb{Z}_\ell$-basis of $T_\ell(A)$.

1.4. The dual abelian variety and the Rosati involution. Because of the importance of the dual abelian variety and the Rosati involution in the study of the endomorphism algebra of an abelian variety, we briefly recall the basic properties concerning them. If A is an abelian variety over k, then $\mathrm{Pic}(A)$ denotes the group of invertible sheaves on A. As usual, let $\mathrm{Pic}^0(A)$ be the subgroup consisting of the invertible sheaves invariant under translation:

$$\mathrm{Pic}^0(A) = \{\mathcal{L} \in \mathrm{Pic}(A) : t_a^*\mathcal{L} \simeq \mathcal{L} \text{ on } A_{\bar{k}} \text{ for all } a \in A(\bar{k})\}.$$

The *dual abelian variety of* A is then an abelian variety $A^\vee$ over k such that $A^\vee(\bar{k}) = \mathrm{Pic}^0(A_{\bar{k}})$, where this identification is given by the so-called Poincaré sheaf $\mathcal{P}$: it is an invertible sheaf on $A \times A^\vee$ such that for all $a \in A^\vee(\bar{k})$, the restriction $\mathcal{P}_{|A\times a}$ represents a in $\mathrm{Pic}^0(A_{\bar{k}})$.

As it is expected, the dual abelian variety $A^\vee$ has dimension equal to the dimension of A, $A^{\vee\vee}$ is canonically isomorphic to A and every homomorphism of abelian varieties $f : A \to B$ over k induces a homomorphism $f^\vee : B^\vee \to A^\vee$ over k.

Given an invertible sheaf $\mathcal{L}$ on $A_{\bar{k}}$, there is an induced homomorphism $\varphi_\mathcal{L} : A_{\bar{k}} \to A_{\bar{k}}^\vee$ given by $\varphi_\mathcal{L}(a) = t_a^*\mathcal{L} \otimes \mathcal{L}^{-1}$. It is a well-known fact that giving a *polarisation* of A is equivalent to giving

an isogeny $\lambda : A \to A^\vee$ over k such that, over $\bar{k}$, it is of the form $\varphi_{\mathcal{L}}$ for some ample sheaf $\mathcal{L}$ on $A_{\bar{k}}$. The pair (A, λ) is then also called a *polarised abelian variety*.

Associated to a polarisation $\lambda = \varphi_{\mathcal{L}}$ of an abelian variety A over k there is a canonical (anti-)involution of the endomorphism algebra $\mathrm{End}_k^0(A)$, which is called the *Rosati involution*. It is defined by the map

$$\begin{array}{ccc} \mathrm{End}_k^0(A) & \longrightarrow & \mathrm{End}_k^0(A) \\ \phi & \longmapsto & \phi' = \lambda^{-1} \circ \phi^\vee \circ \lambda. \end{array}$$

It is easily checked that it is really an involution, i.e. $\phi'' = \phi$ for all $\phi \in \mathrm{End}_k^0(A)$, and moreover it satisfies

$$(\phi + \alpha)' = \phi' + \alpha', (a\phi)' = a\phi' \text{ and } (\phi \circ \alpha)' = \alpha' \circ \phi' \text{ for all } \phi, \alpha \in \mathrm{End}_k^0(A), a \in \mathbb{Q}.$$

One of the most important properties of the Rosati involution is that *it is positive definite*. That is, for every non-zero $\phi \in \mathrm{End}_k^0(A)$, we have $\mathrm{Tr}(\phi \circ \phi') > 0$. Here $\mathrm{Tr}(\phi \circ \phi')$ means the trace of $\phi \circ \phi'$ as an endomorphism, in the sense we have mentioned above.

1.5. The endomorphism algebra of an abelian variety. An abelian variety over k is said to be *simple* over k (or k-simple) if there does not exist any abelian variety $B \subseteq A$ over k except from 0 and A itself. If K/k is a field extension, A is simple over K if A_K is simple over K according to this definition. Then, note that a k-simple abelian variety A can be non-simple over K. A is said to be *absolutely simple* if it is simple over k^s.

The first key point in the study of the endomorphism algebra of an abelian variety is the following decomposition result:

THEOREM 1.6. *Let A be an abelian variety over k. There exist k-simple and pairwise non-isogenous abelian varieties $A_1, \ldots, A_r$ and positive integers $n_1, \ldots, n_r$ such that*

$$A \sim_k A_1^{n_1} \times \cdots \times A_r^{n_r}.$$

Moreover, the abelian varieties A_i are uniquely determined up to k-isogeny and permutation, and the associated integers n_i are uniquely determined.

Now assume that A is simple over k, and let $f \in \mathrm{End}_k(A)$. The connected component of $\ker(f)$ containing the identity element 0 is an abelian variety, so that it must be either 0 or A itself, since A is k-simple. This shows that every non-zero endomorphism of A is an isogeny, and therefore it is an invertible element in $\mathrm{End}_k^0(A)$. In other words, for a k-simple abelian variety A, $\mathrm{End}_k^0(A)$ is a division algebra of finite dimension over $\mathbb{Q}$. Clearly, if n is a positive integer, the endomorphism algebra of A^n is isomorphic to $\mathrm{M}_n(\mathrm{End}_k^0(A))$. And finally, if A and B are non-isogenous abelian varieties over k, then $\mathrm{Hom}_k^0(A, B) = 0$ and $\mathrm{End}_k^0(A \times B) \simeq \mathrm{End}_k^0(A) \times \mathrm{End}_k^0(B)$. From these facts and the above theorem, the following result is deduced:

PROPOSITION 1.7. *Let A be an abelian variety over k, whose decomposition into k-simple varieties up to isogeny is as in Theorem 1.6. Then*

$$\mathrm{End}_k^0(A) \simeq \mathrm{M}_{n_1}(D_1) \times \cdots \times \mathrm{M}_{n_r}(D_r),$$

where D_i is the division algebra $\mathrm{End}_k^0(A_i)$.

As a consequence, the endomorphism algebra of an abelian variety is a semisimple finite-dimensional algebra over $\mathbb{Q}$. The particular form of the division algebras D_i allows one to use Albert's classification as we now recall briefly.

As before, assume that A is a (polarised) k-simple abelian variety, with endomorphism algebra $D = \mathrm{End}_k^0(A)$. Since the reduced trace $\mathrm{Tr}_{D/\mathbb{Q}}$ of D over $\mathbb{Q}$ is a positive multiple of Tr, the positivity of the Rosati involution $'$ on D associated to a choice of polarisation means that $\mathrm{Tr}_{D/\mathbb{Q}}(\phi\phi') > 0$ for every $\phi \neq 0$ in D. Albert's classification on involuting simple algebras can be applied to the pair $(D, ')$ in order to give the following structure theorem for endomorphism algebras of simple abelian varieties (cf. [**Mum70**, Chapter IV]):

THEOREM 1.8. *Let A be a k-simple abelian variety of dimension g. Let F be the center of $D = \mathrm{End}_k^0(A)$, and let $F_0 = \{x \in D : x' = x\}$ be the subfield fixed by the Rosati involution. Define the integers $d := [D : F]^{1/2}$, $e := [F : \mathbb{Q}]$, $e_0 := [F_0 : \mathbb{Q}]$. Then the isomorphism type of D is one of the following four ones:*

I) *$D = F = F_0$ is a totally real number field, and the Rosati involution is the identity. In this case, $e|g$.*
II) *$F = F_0$ is a totally real number field and D is a totally indefinite division quaternion algebra over F, i.e. for any embedding $\sigma : F \to \mathbb{R}$, we have $D \otimes_\sigma \mathbb{R} \simeq \mathrm{M}_2(\mathbb{R})$. In this case $2e|g$.*
III) *$F = F_0$ is a totally real number field and D is a totally definite division quaternion algebra over F, i.e. for any embedding $\sigma : F \to \mathbb{R}$, we have $D \otimes_\sigma \mathbb{R} \simeq \mathbb{H}$, the Hamilton quaternion algebra. In this case $e^2|g$.*
IV) *F_0 is a totally real number field, F is a CM extension of F_0 (that is, a totally imaginary quadratic extension of F_0) and D is a division algebra with center F. In this case, $e_0 d^2|g$ if $\mathrm{char}(k) = 0$, and $e_0 d|g$ if $\mathrm{char}(k) > 0$.*

Observe that, in all cases, F_0 is a totally real number field and F is either F_0 or a CM extension of F_0. The abelian variety A is said to be of the *first* (resp. *second*) *kind* if the first (resp. second) case holds.

In general, for a not necessarily simple abelian variety A over k of dimension g, it is said that A has *complex multiplication* (CM) over k if its endomorphism algebra $\mathrm{End}_k^0(A)$ contains a commutative semisimple algebra of dimension $2g$ over $\mathbb{Q}$, which is the maximal dimension of such a subalgebra. If $\mathrm{char}(k) = 0$ and A is k-simple, then A has CM over k if and only if $\mathrm{End}_k^0(A)$ is a CM number field of degree $2g$.

If we focus our attention in the case of abelian surfaces (i.e., abelian varieties of dimension $g = 2$) over a field k of characteristic zero, then the isomorphism type of the endomorphism algebra $\mathrm{End}_k^0(A)$ is one of the following:

I) either $\mathbb{Q}$ or a real quadratic field;
II) an indefinite rational quaternion algebra;
III) a definite rational quaternion algebra;
IV) an imaginary quadratic field.

The Shimura curves that will be considered in this thesis parametrise abelian surfaces $A/\bar{\mathbb{Q}}$ such that $\mathrm{End}_{\bar{\mathbb{Q}}}^0(A)$ is isomorphic to an indefinite rational quaternion algebra. Such abelian surfaces are often referred to as *fake* elliptic curves by some authors, or just as abelian surfaces *with quaternionic multiplication* (or QM, for short).

2. Quaternion algebras

The theory of quaternion algebras over a field k can be framed into the general theory of central simple algebras over k. There is a good treatment of this general theory in [**GS06**], and also a very detailed account in [**Pie82**]. In fact, the isomorphism classes of quaternion algebras over k correspond to the 2-torsion subgroup of the Brauer group $\mathrm{Br}(k)$ of k. For the specific theory of quaternion algebras the basic reference is [**Vig80**], where all the material in this section is more than covered.

2.1. Basic general notions. Let k be a field, and fix a separable closure k^s of k. As usual, by a field extension of k we will always mean a field extension of k contained in k^s.

DEFINITION 1.9. *A* quaternion algebra *B over k is a central simple algebra of rank 4 over k.*

There are essentially two basic constructions describing quaternion algebras. On the one hand, suppose L is a quadratic separable algebra[1] over k, and write $x \mapsto \bar{x}$ for the non-trivial involution

[1]By this we mean either a quadratic separable field extension of k or $k \oplus k$.

on L over k. If $\theta \in k^\times$ is any invertible element, then the algebra

$$B := L + Lu, \tag{1.1}$$

where $u \in B$ is such that

$$u^2 = \theta \quad \text{and} \quad ux = \bar{x}u \text{ for all } x \in L,$$

is a quaternion algebra over k, and it is usually denoted by $B = \{L, \theta\}$. Moreover, any quaternion algebra over k can be expressed in this form (cf. [**Vig80**]).

On the other hand, suppose that $\mathrm{char}(k) \neq 2$. Let $a, b \in k^\times$, and define

$$\left(\frac{a,b}{k}\right) := k + ki + kj + kij \tag{1.2}$$

to be the algebra with basis $1, i, j, ij$ over k and whose multiplication table is deduced from the relations

$$i^2 = a, \quad j^2 = b, \quad ij = -ji.$$

Then $(\frac{a,b}{k})$ is again a quaternion algebra over k, and it is also true that any quaternion algebra over k admits a presentation of this form. Indeed, observe that $(\frac{a,b}{k}) = \{k(i), b\}$. We will assume henceforth that $\mathrm{char}(k) \neq 2$, so that we can deal with both descriptions (1.1) and (1.2).

Remark 1.10. Clearly, the elements $a, b \in k^\times$ are not uniquely determined by the isomorphism class of the quaternion algebra $(\frac{a,b}{k})$. We refer the reader to [**Pie82**, §1.7] for a discussion about when two quaternion algebras $(\frac{a,b}{k})$ and $(\frac{a',b'}{k})$ are isomorphic.

From the very definitions, a quaternion algebra B over k admits a *canonical (anti-)involution* (or *main (anti-)involution*), also called *conjugation*. Using the description from (1.1), it is defined by extending the involution on L to B setting $\bar{u} = -u$. Alternatively, if $B = (\frac{a,b}{k})$ as in (1.2) and $\beta = x + yi + zj + tij$, then $\bar{\beta} = x - yi - zj - tij$. Thus if $\alpha, \beta \in B$ and $x, y \in k$ then

$$\overline{x\alpha + y\beta} = x\bar{\alpha} + y\bar{\beta}, \quad \bar{\bar{\alpha}} = \alpha, \quad \overline{\alpha\beta} = \bar{\beta}\bar{\alpha}.$$

Definition 1.11. *The* reduced trace *and* norm *are, respectively, the maps*

$$\mathrm{tr}, \mathrm{n} : B \longrightarrow k$$

defined by

$$\mathrm{tr}(\beta) = \beta + \bar{\beta} \quad \textit{and} \quad \mathrm{n}(\beta) = \beta\bar{\beta}.$$

Every element $\beta \in B$ is a root of the quadratic polynomial

$$(X - \beta)(X - \bar{\beta}) = X^2 - \mathrm{tr}(\beta)X + \mathrm{n}(\beta),$$

hence if $\beta \notin k$, then $k(\beta)/k$ is a quadratic extension. When restricted to $k(\beta)$, the reduced trace and norm coincide, respectively, with the trace and norm of the extension $k(\beta)/k$. This way, a quaternion algebra over k can be thought of as a *bunch* of quadratic extensions glued together in a non-commutative way.

Example 1.12. The matrix algebra $\mathrm{M}_2(k)$ is a quaternion algebra over k. Indeed, the assignment

$$i \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad j \mapsto \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}$$

induces an isomorphism $(\frac{1,b}{k}) \simeq \mathrm{M}_2(k)$ for every $b \in k^\times$. The quaternion algebra $\mathrm{M}_2(k)$ is the unique non-division quaternion algebra over k, up to isomorphism, and it is often referred to as the *split* quaternion algebra.

Example 1.13. The Hamilton quaternion algebra $\mathbb{H} = (\frac{-1,-1}{\mathbb{R}})$, generated over $\mathbb{R}$ by elements i, j satisfying $i^2 = j^2 = -1$, $ij = -ji$, is a division quaternion algebra over $\mathbb{R}$. By a theorem of Frobenius ([**Vig80**, Corollaire I.2.5], [**Pie82**, Corollary 13.1.c]), it is the unique finite-dimensional non-commutative division algebra over $\mathbb{R}$, up to isomorphism. Therefore, any quaternion algebra over $\mathbb{R}$ is isomorphic to either $\mathrm{M}_2(\mathbb{R})$ or $\mathbb{H}$.

EXAMPLE 1.14. If k is an algebraically closed field, Wedderburn's Theorem on the classification of simple algebras implies that every central simple algebra over k is isomorphic to $\mathrm{M}_n(k)$ for some integer $n \geq 1$ (see Theorem 2.1.3 and Corollary 2.1.7 in [**GS06**]). In particular, the only quaternion algebra over the field $\mathbb{C}$ of complex numbers (up to isomorphism) is $\mathrm{M}_2(\mathbb{C})$.

As it is shown in [**Vig80**, Corollaire I.2.4], a quaternion algebra over k is either isomorphic to the split quaternion algebra $\mathrm{M}_2(k)$ or a division quaternion algebra. In view of this fact, the *Hasse invariant* of a quaternion algebra B over k is defined to be

$$\varepsilon(B) = \begin{cases} -1 & \text{if } B \text{ is division,} \\ 1 & \text{otherwise.} \end{cases}$$

This dichotomy can be translated into the theory of quadratic forms, which is therefore strongly related to that of quaternion algebras (see [**Pie82**, §1.6]). The Hasse invariant of B depends only on its isomorphism class, and therefore defines a map

$$\mathcal{Q}_k \longrightarrow \{\pm 1\},$$

where $\mathcal{Q}_k$ denotes the set of isomorphism classes of quaternion algebras over k. In fact, $\mathcal{Q}_k$ can be identified with the 2-torsion subgroup $\mathrm{Br}(k)[2]$ of the Brauer group of k, hence it inherits a group structure (see [**Pie82**, §12.5] for the definition of $\mathrm{Br}(k)$).

The split quaternion algebras play also an important role in the study of the quadratic subfields of a quaternion algebra. If L is a quadratic subfield of B, then the quaternion algebra $B \otimes_k L$ over L is either isomorphic to $\mathrm{M}_2(L)$ or a division quaternion algebra over L. More in general, this motivates the following definition:

DEFINITION 1.15. *Let B be a quaternion algebra over k, and L/k be a field extension. Then L is said to be a* splitting field *for B if $B \otimes_k L \simeq \mathrm{M}_2(L)$. If this is the case, it is also said that* the field L splits B.

By [**Vig80**, Théorème I.2.8], a quadratic extension L/k splits the algebra B if and only if L is isomorphic to a maximal subfield of B. If a field L splits the algebra B, then by means of the natural inclusion $B \hookrightarrow B \otimes_k L \simeq \mathrm{M}_2(L)$ the reduced trace and norm of an element $\beta \in B$ can be computed inside $\mathrm{M}_2(L)$ as the usual trace and determinant, respectively.

Suppose now that k is the field of fractions of a Dedekind domain R. The non-commutativity of quaternion algebras over k makes the theory of R-orders a bit more subtle than its analogue in the case of number fields.

Let B be a quaternion algebra over k. An element $\beta \in B$ is said to be *integral* (over R) if $\mathrm{tr}(\beta), \mathrm{n}(\beta) \in R$. However, notice that the set of integral elements in B may not be a ring.

DEFINITION 1.16. *An* order $\mathcal{O} \subset B$ *over R is an R-lattice which is also a ring. Equivalently, it is a ring of integral elements of B, finitely generated as an R-module and such that $\mathcal{O} \otimes_R k = B$.*

An order $\mathcal{O}$ is said to be a *maximal order* if it is maximal with respect to the inclusion. If an order $\mathcal{O}$ is the intersection of two maximal orders $\mathcal{O}_1$ and $\mathcal{O}_2$, then $\mathcal{O}$ is called an *Eichler order*, and its *level* is defined as its index in either $\mathcal{O}_1$ or $\mathcal{O}_2$.

An *R-ideal* (or simply an *ideal*) is defined to be an R-lattice I in B such that $I \otimes_R k \simeq B$. Thus an order $\mathcal{O}$ in B is an R-ideal which is also a ring. An ideal is said to be *integral* if all its elements are integral.

DEFINITION 1.17. *If I is an ideal of B, its associated* left *and* right orders *are defined, respectively, by*

$$\mathcal{O}_\ell(I) := \{\beta \in B : \beta I \subseteq I\}, \quad \mathcal{O}_r(I) := \{\beta \in B : I\beta \subseteq I\}.$$

An ideal I is called *normal* if both $\mathcal{O}_\ell(I)$ and $\mathcal{O}_r(I)$ are maximal orders. Besides, I is *two-sided* if $\mathcal{O}_\ell(I) = \mathcal{O}_r(I)$, and it is *principal* if there exists $\beta \in B$ such that $I = \mathcal{O}_\ell(I)\beta = \beta\mathcal{O}_r(I)$.

For two-sided ideals I, J, their product IJ can be defined in the usual way, and the inverse of a two-sided ideal I is defined by $I^{-1} = \{\beta \in B : I\beta I \subseteq I\}$; it satisfies the relations

$$II^{-1} \subseteq \mathcal{O}_\ell(I), \quad I^{-1}I \subseteq \mathcal{O}_r(I).$$

Two ideals I, J are said to be *equivalent on the left* if $I = \beta J$ for some $\beta \in B$. As in the number field case, this is easily shown to be an equivalence relation. If $\mathcal{O}$ is an order, its set of left-ideal classes is denoted by $\mathrm{Pic}_\ell(\mathcal{O})$. That is, $\mathrm{Pic}_\ell(\mathcal{O})$ is the set of ideals with right order $\mathcal{O}$ modulo equivalence on the left. Analogously, one defines the set $\mathrm{Pic}_r(\mathcal{O})$ as the set of right-classes of left $\mathcal{O}$-ideals, which is in natural bijection with $\mathrm{Pic}_\ell(\mathcal{O})$.

For an order $\mathcal{O}$, the *class number of* $\mathcal{O}$ is the integer $|\mathrm{Pic}_\ell(\mathcal{O})| = |\mathrm{Pic}_r(\mathcal{O})|$. All maximal orders have the same class number, and the *class number* of B, denoted by $h(B)$, is defined as the class number of any maximal order in B.

If I is an ideal, $\mathrm{n}(I)$ denotes the fractional R-ideal generated by the reduced norms of elements of I. If $\mathcal{O}$ is an order, the *different of* $\mathcal{O}$ is by definition the fractional ideal defined by $d(\mathcal{O}) := (\mathcal{O}^*)^{-1}$, where $\mathcal{O}^* = \{\beta \in B : \mathrm{tr}(\beta\mathcal{O}) \subseteq R\}$, and the *discriminant of* $\mathcal{O}$ is defined as the norm of its different, $D(\mathcal{O}) := \mathrm{n}(d(\mathcal{O}))$. If $\{v_i\}$ is an R-basis of the order $\mathcal{O}$, then $D(\mathcal{O})^2$ is the principal ideal $R\det(\mathrm{tr}(v_i v_j))$.

As we emphasised above, the quadratic subfields of a quaternion algebra B (i.e., the quadratic splitting fields) play an important role in the arithmetic of B. Concerning the integral theory, optimal embeddings of quadratic orders into orders of B are of central interest. Let L/k be a quadratic extension splitting B, so that there is an embedding of L into B as a k-subalgebra. By the Noether-Skolem Theorem, any pair of such embeddings are conjugate by an element of $B^\times$, and therefore the set of k-linear embeddings $L \hookrightarrow B$ is identified with $B^\times/L^\times$, as L is a maximal commutative k-subalgebra of B. Fix a k-linear embedding $\iota : L \hookrightarrow B$.

Definition 1.18. *Let S be a quadratic order in L, and $\mathcal{O}$ be an order in B. The embedding ι is said to be* S-optimal with respect to $\mathcal{O}$ *if $S = \iota^{-1}(\mathcal{O} \cap \iota(L))$. When this is the case, one also says that S* is optimally embedded in $\mathcal{O}$.

In other words, S is optimally embedded in $\mathcal{O}$ by ι if $\iota(S) \subseteq \mathcal{O}$ and this does not hold for any larger order in L. It is clear that if ι is an S-optimal embedding and we compose ι by the inner automorphism defined by any element in the normaliser

$$N(\mathcal{O}) := \mathrm{Norm}_{B^\times}(\mathcal{O})$$

of $\mathcal{O}$ in $B^\times$, then the resulting embedding is still S-optimal. Thus it is convenient to consider optimal embeddings up to conjugation by $N(\mathcal{O})$. More generally, for any intermediate subgroup $\mathcal{O}^\times \subseteq G \subseteq N(\mathcal{O})$, we set

$$v_G(S, \mathcal{O}) := \text{number of } S\text{-optimal embeddings } L \hookrightarrow B \text{ with respect to } \mathcal{O}, \text{ modulo } G\text{-conjugacy},$$

that is to say, $v_G(S, \mathcal{O})$ is the number of G-orbits of S-optimal embeddings $L \hookrightarrow B$ with respect to $\mathcal{O}$, where G acts by inner automorphisms.

2.2. Quaternion algebras over local fields. Quaternion algebras over local fields are far more simple than quaternion algebras over global fields. And by an *adèlisation* process, the study of the former ones allows to describe precisely the latter ones.

We have already quoted in Example 1.13 that there is a unique division quaternion algebra over the field $\mathbb{R}$ of real numbers. As it is proved in [**Vig80**, §I.1], the theorem of Frobenius quoted in Example 1.13 extends to the non-archimedean case, so that there is also a single division quaternion algebra over a non-archimedean local field, up to isomorphism.

In order to make precise this statement, we introduce some notation. Let k denote a non-archimedean local field, write R_k for its ring of integers and let π be a uniformiser in R_k, i.e. an element such that $(\pi) = \pi R_k$ is the (unique) maximal ideal of R_k. Choose also a discrete valuation

v on k, normalised so that $v(\pi) = 1$. Besides, let L_{nr} be the unique quadratic unramified extension of k inside a separable closure k^s of k. Recall that L_{nr} satisfies:

(a) π is a prime element in L_{nr},
(b) $R_k^\times = \mathrm{n}(R_L^\times)$, where R_L is the ring of integers of L_{nr}, and
(c) $[R_L/\pi : R_k/\pi] = 2$, where R_L/π is the residue field of L_{nr}.

Then the classification theorem we have just announced admits the following explicit form (cf. [**Vig80**, Théorème II.1.3]):

THEOREM 1.19. *There is a unique division quaternion algebra over k up to isomorphism, namely $B = \{L_{nr}, \pi\}$. Moreover, B contains a unique maximal order, which is $\mathcal{O} = \{\beta \in B : \mathrm{n}(\beta) \in R_k\}$, and the ideal πR_k ramifies: $\pi\mathcal{O} = \mathfrak{p}^2$, where $\mathfrak{p}$ is the unique maximal ideal of $\mathcal{O}$.*

Regarding $\mathcal{Q}_k$ as a group through an identification $\mathcal{Q}_k \simeq \mathrm{Br}(k)[2]$, as we quoted above, this theorem shows that $\mathcal{Q}_k \simeq \mathbb{Z}/2\mathbb{Z}$ for every non-archimedean local field k, and $\{L_{nr}, \pi\}$ represents the non-trivial element of this group. The idea of the proof is that the valuation v on k extends naturally to a valuation w on a quaternion algebra B over k through its reduced norm. Then one shows that L_{nr} necessarily embeds into B as a subfield and $B \simeq \{L_{nr}, \pi\}$. Further, the existence of the valuation w implies the uniqueness of the maximal order (which is the valuation ring of w) and the group structure of the normal ideals.

Concerning the split quaternion algebra over k, we can think $\mathrm{M}_2(k)$ as the endomorphism algebra of a two-dimensional k-vector space V and fix an isomorphism $\mathrm{M}_2(k) \simeq \mathrm{End}(V)$ (depending on the choice of a k-basis of V). The maximal orders of $\mathrm{End}(V)$ are the rings $\mathrm{End}(\Lambda)$, where Λ is a complete R_k-lattice of V, and the ideals of these orders are all of the form $\mathrm{Hom}(\Lambda_1, \Lambda_2)$ for some complete R_k-lattices Λ_1, Λ_2 of V. This provides a comprehensive description of $\mathrm{M}_2(k)$:

PROPOSITION 1.20. *All the maximal orders of $\mathrm{M}_2(k)$ are conjugate to $\mathrm{M}_2(R_k)$, and the two-sided ideals of $\mathrm{M}_2(R_k)$ form a cyclic group generated by the prime ideal $\mathrm{M}_2(R_k)\pi = \pi\mathrm{M}_2(R_k)$.*

The study of optimally embedded quadratic orders into maximal orders in a quaternion algebra over a local field is particularly simple. Let L/k be a quadratic separable algebra over k, and recall that the Artin symbol $(\frac{L}{\pi})$ is defined to be -1 if the extension L/k is unramified, and 0 if it is ramified. If S is an order of L, then the *Eichler symbol* is defined as

$$\left\{\frac{S}{\pi}\right\} := \begin{cases} \left(\frac{L}{\pi}\right) & \text{if } S \text{ is maximal,} \\ 1 & \text{otherwise.} \end{cases} \tag{1.3}$$

With these notations, the number of optimal embeddings of a quadratic order into a maximal order $\mathcal{O}$ of a quaternion algebra B over k, modulo conjugation by $\mathcal{O}^\times$ or $N(\mathcal{O})$ is computed in the next theorems.

THEOREM 1.21. *Let B be the unique division quaternion algebra over k, and $\mathcal{O}$ be its maximal order. Let L/k be a quadratic separable extension, and S be an order in L. If S is maximal, then*

$$v_{\mathcal{O}^\times}(S, \mathcal{O}) = 1 - \left(\frac{L}{\pi}\right) = 1 - \left\{\frac{S}{\pi}\right\} \quad \text{and} \quad v_{N(\mathcal{O})}(S, \mathcal{O}) = 1.$$

If S is not maximal, then S cannot be optimally embedded into $\mathcal{O}$.

THEOREM 1.22. *Let $\mathcal{O}$ be a maximal order of $\mathrm{M}_2(k)$, L/k be a quadratic separable extension and S be an order in L. Then S can be optimally embedded into $\mathcal{O}$, and the number of S-optimal embeddings with respect to $\mathcal{O}$ modulo conjugation by $\mathcal{O}^\times$ is 1. If $\mathcal{O}_{(\pi)}$ is an Eichler order of level (π) in $\mathrm{M}_2(k)$, then*

$$v_{\mathcal{O}_{(\pi)}^\times}(S, \mathcal{O}_{(\pi)}) = 1 + \left\{\frac{S}{\pi}\right\} \quad \text{and} \quad v_{N(\mathcal{O}_{(\pi)})}(S, \mathcal{O}_{(\pi)}) = 0 \text{ or } 1.$$

In this thesis, we mainly work with rational quaternion algebras and their localisations at rational places. In the non-archimedean case, we are therefore especially interested in quaternion algebras over the field $\mathbb{Q}_p$ of p-adic numbers, for some rational prime p. For the sake of clarity, let us summarise the above general discussion for the case $k = \mathbb{Q}_p$. As it is customary, we denote by $\mathbb{Q}_{p^2}$ the unique quadratic unramified extension of $\mathbb{Q}_p$, and write $\mathbb{Z}_{p^2}$ for its ring of integers.

COROLLARY 1.23. *The split algebra* $\mathrm{M}_2(\mathbb{Q}_p)$ *and the division algebra* $B = \{\mathbb{Q}_{p^2}, p\}$ *are the only quaternion algebras over* $\mathbb{Q}_p$*, up to isomorphism. Furthermore:*

i) *All the maximal orders of* $\mathrm{M}_2(\mathbb{Q}_p)$ *are conjugate to* $\mathrm{M}_2(\mathbb{Z}_p)$*, and the two-sided ideals of* $\mathrm{M}_2(\mathbb{Z}_p)$ *form a cyclic group generated by the prime ideal* $(p) = \mathrm{M}_2(\mathbb{Z}_p)p = p\mathrm{M}_2(\mathbb{Z}_p)$*. Every order in a quadratic separable extension of* $\mathbb{Q}_p$ *can be optimally embedded into every maximal order* $\mathcal{O}$ *of* $\mathrm{M}_2(\mathbb{Q}_p)$*, and the number of such optimal embeddings up to* $\mathcal{O}^\times$*-conjugation is* 1*.*

ii) *The unique maximal order of* B *is* $\mathcal{O} = \{\beta \in B : \mathrm{n}(\beta) \in \mathbb{Z}_p\}$*, and the ideal* $p\mathbb{Z}_p$ *ramifies:* $p\mathcal{O} = I_p^2$*, where* $I_p = \{\gamma \in \mathcal{O} : \mathrm{n}(\gamma) \in p\mathbb{Z}_p\}$ *is the unique maximal ideal of* $\mathcal{O}$*. If* S *is an order in a quadratic separable extension of* $\mathbb{Q}_p$*, then the number of* S*-optimal embeddings with respect to* $\mathcal{O}$*, modulo* $\mathcal{O}^\times$*-conjugacy is* $1 - \{\frac{S}{p}\}$*.*

If B is the unique division quaternion algebra over $\mathbb{Q}_p$, it is often useful to work with its matrix representation into $\mathrm{M}_2(\mathbb{Q}_{p^2})$. Namely, B is regarded as a matrix subring of $\mathrm{M}_2(\mathbb{Q}_{p^2})$ through the embedding

$$B \hookrightarrow B \otimes_{\mathbb{Q}_p} \mathbb{Q}_{p^2} \simeq \mathrm{M}_2(\mathbb{Q}_{p^2})$$

under which B is identified with the subring of elements of the form

$$\begin{pmatrix} a & b \\ p\bar{b} & \bar{a} \end{pmatrix}, \quad a, b \in \mathbb{Q}_{p^2}, \tag{1.4}$$

where $x \mapsto \bar{x}$ denotes the non-trivial automorphism in $\mathrm{Gal}\,(\mathbb{Q}_{p^2}/\mathbb{Q}_p)$. With this identification, the unique maximal order $\mathcal{O}$ of B corresponds to

$$\left\{ \begin{pmatrix} a & b \\ p\bar{b} & \bar{a} \end{pmatrix} \in B : a, b \in \mathbb{Z}_{p^2} \right\}, \tag{1.5}$$

and one can choose as a uniformiser π of $\mathcal{O}$ the element represented by

$$\begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix}.$$

Further, observe that since $\mathcal{O}$ is the unique maximal order, it is also the unique Eichler order in B. In contrast, consider the split quaternion algebra $\mathrm{M}_2(\mathbb{Q}_p)$ over $\mathbb{Q}_p$. Maximal orders in $\mathrm{M}_2(\mathbb{Q}_p)$ can be regarded as endomorphism rings of $\mathbb{Z}_p$-lattices in a two-dimensional $\mathbb{Q}_p$-vector space V, and therefore Eichler orders in $\mathrm{M}_2(\mathbb{Q}_p)$ are of the form $\mathrm{End}(\Lambda_1) \cap \mathrm{End}(\Lambda_2)$ for some $\mathbb{Z}_p$-lattices $\Lambda_1, \Lambda_2 \subset V$. Fixing an isomorphism $\mathrm{M}_2(\mathbb{Q}_p) \simeq \mathrm{End}(V)$ (which amounts to fixing a $\mathbb{Q}_p$-basis), one shows that an order $\mathcal{O} \subseteq \mathrm{M}_2(\mathbb{Q}_p)$ is an Eichler order if and only if $\mathcal{O}$ is conjugate to the order

$$\begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ p^n\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$$

for some integer $n \geq 1$ (see [**Vig80**, Ch. II, Lemme 2.4]). If this is the case, p^n is the level[2] of $\mathcal{O}$.

[2]The integer n is also called the *distance* between any two maximal orders whose intersection is $\mathcal{O}$, which is indeed the distance between the corresponding vertices of the Bruhat-Tits tree associated with $\mathrm{PGL}_2(\mathbb{Q}_p)$.

2.3. Quaternion algebras over number fields. Let K be a number field, with ring of integers R_K, and let B be a quaternion algebra over K. For every place v of K, the quaternion algebra $B_v := B \otimes_K K_v$ is a local quaternion algebra over the completion K_v of K at v, hence it is isomorphic to either the split algebra $\mathrm{M}_2(K_v)$ or the unique division quaternion algebra over K_v. This corresponds, respectively, to whether the Hasse invariant $\varepsilon(B_v)$ is 1 or -1. A place v of K is said to be *ramified* in B if $\varepsilon(B_v) = -1$, and *split* otherwise. The set of all ramified places of K in B is denoted by $\mathrm{Ram}(B)$.

Notice that every complex archimedean place of K (if any) is necessarily split, by Example 1.14. On the other hand, the localisation B_v of B at a real archimedean place v of K (if any) is isomorphic to either $\mathrm{M}_2(\mathbb{R})$ or $\mathbb{H}$, the Hamilton quaternion algebra, according to whether v is split or ramified in B, respectively. In the first case, we say B is *indefinite* at v, whereas in the second case we say B is *definite* at v.

Thanks to the classification of quaternion algebras over local fields, the quaternion algebras over K are classified by a local-to-global principle, as the next theorem shows. In other words, the set $\mathcal{Q}_K$ of isomorphism classes of quaternion algebras over K is described in terms of the sets of isomorphism classes $\mathcal{Q}_{K_v}$ of local quaternion algebras over K_v, as v ranges over all the places of K (see [**Vig80**, Ch. III, Théorème 3.1]):

THEOREM 1.24. *The set* $\mathrm{Ram}(B)$ *is finite and has even cardinality, and there is a short exact sequence*

$$1 \longrightarrow \mathcal{Q}_K \longrightarrow \bigoplus_v \mathcal{Q}_{K_v} \xrightarrow{\varepsilon} \{\pm 1\} \longrightarrow 1, \tag{1.6}$$

where v *runs over all the places of* K *and* ε *stands for the product of local Hasse invariants.*

Hence a quaternion algebra B over K is uniquely determined (up to isomorphism) by its (finite) set of ramified places. Further, for every finite set of places S of K of even cardinality, there exists a unique quaternion algebra B over K (up to isomorphism) such that $\mathrm{Ram}(B) = S$. Using the relation between quaternion algebras and quadratic forms, the Hasse principle for quadratic forms can be proved as a corollary of Theorem 1.24. Besides, the short exact sequence (1.6) also shows how the group law in $\mathcal{Q}_K \simeq \mathrm{Br}(K)[2]$ can be described locally.

Writing $\varepsilon_v(B) := \varepsilon(B_v)$ for the local Hasse invariant of B at a place v of K, it follows from the parity condition in the above theorem that

$$\prod_v \varepsilon_v(B) = 1, \tag{1.7}$$

where the product is over *all* the places of K.

Another immediate consequence of Theorem 1.24 is a criterion for a field extension F/K to split a quaternion algebra B over K: this holds if and only if $B_D \otimes_K F$ is locally split at every place of F. This leads to the result below, known as Hasse's criterion:

THEOREM 1.25 (Hasse's criterion). *Let* B *be a quaternion algebra over* K*, and* F/K *be a quadratic field extension. Then* F *splits* B *(that is to say,* $B \otimes_K F \simeq M_2(F)$*, or equivalently,* F *embeds as a subfield in* B*) if and only if* $F_v := F \otimes_K K_v$ *embeds in* B_v *for every place* v *of* K*.*

As is suggested by the previous theorems, the arithmetic of a quaternion algebra B over a global field K can be studied through *adèlisation*: roughly speaking, this means looking at all the localisations $B \hookrightarrow B_v$ at the same time. More precisely, let $\mathbb{A}_K$ be the ring of K-adèles, and consider the extension of scalars $B \otimes_K \mathbb{A}_K$. Then $B \otimes_K \mathbb{A}_K$ is isomorphic to the restricted product of the local quaternion algebras B_v with respect to the localisations of a fixed order in B which is locally integral at almost all the finite places of K (cf. [**Vig80**, p. 60]), and therefore we can embed B diagonally in $B \otimes_K \mathbb{A}_K$,

$$B \hookrightarrow \widehat{B} := B \otimes_K \mathbb{A}_K.$$

A starting point in this approach is the next result, often referred to as the *norm theorem*, which follows from the work of Hasse, Schilling, Maass and Eichler (see [**Vig80**, Ch. III, Théorème 4.1]):

THEOREM 1.26. *Let K_B be the set of elements of K which are non-negative at every real place of K ramifying in B. Then* $\mathrm{n}(B) = K_B$. *In particular, if B is split at every real place of K (i.e., B is* totally indefinite*), then* $\mathrm{n}(B) = K$.

Next we state one of the main applications of this theorem, which is due mainly to Kneser, and it is also known as the *strong approximation theorem for* B^1 (the group of units of reduced norm 1 in $B^\times$). Let S be a finite set of places of K, containing at least one archimedean place, and write $B_S^1 := \prod_{v\in S} B_v^1$. If v is a place of K, notice that B_v^1 is compact if and only if v is ramified. Thus B_S^1 is compact if and only if every place $v \in S$ is ramified in B. When this happens, observe that $B^1 B_S^1$ is closed in $\widehat{B}^1$, as B^1 is discrete in $\widehat{B}^1$.

THEOREM 1.27. *Let B^1 be the group of units of norm* 1 *in B. Let S be a finite set of places of K containing at least one archimedean place, and write $B_S^1 := \prod_{v\in S} B_v^1$. If B_S^1 is not compact, then $B^1 B_S^1$ is dense in $\widehat{B}^1$.*

The integral theory of orders and ideals (with respect to the ring of integers R_K of K) can also be described through *adèlisation*. Indeed, fix a complete lattice Θ in B, and write $\Theta_v := \Theta \otimes_R R_v$ for its localisation at each non-archimedean place v of K, where $R_v := R_{K,v}$ is the completion of R_K at v. Thus Θ_v is a complete R_v-lattice in B_v for each v. Then the set of complete R_K-lattices in B is in bijection with the set of families $(\Lambda_v)_v$ of local R_v-lattices, one for each non-archimedean place v, such that $\Lambda_v = \Theta_v$ for almost all v. Many of the properties concerning lattices are local, meaning that they hold for a lattice Λ if and only if they hold for all its localisations Λ_v at non-archimedean places. However, there are properties which are not local: for instance, an ideal in B which is locally principal at every place need not be principal.

As an example of a local statement concerning orders, we point out the following result, which will be important for us later in this thesis:

PROPOSITION 1.28. *If $\mathcal{O}$ is a maximal order in B, then $N(\mathcal{O})/K^\times\mathcal{O}^\times \simeq \mathbb{Z}/2\mathbb{Z}^r$, where r is the number of (finite) primes ramifying in B.*

PROOF. This is indeed a local statement, as $N(\mathcal{O})$ consists of those $b \in B$ such that $b \in N(\mathcal{O}_v)$ for all finite places v. There is no contribution from the split places, since every maximal order is conjugate to $\mathrm{M}_2(R_v)$ and $N(\mathrm{M}_2(R_v)) = K_v^\times \mathrm{GL}_2(R_v)$, whereas at the ramified primes one has $N(\mathcal{O}_v) = B_v^\times$, hence $N(\mathcal{O}_v)/K_v^\times\mathcal{O}_v^\times = B_v^\times/K_v^\times\mathcal{O}_v^\times \simeq \mathbb{Z}/2\mathbb{Z}$. □

For Eichler orders, a similar argument shows that $N(\mathcal{O})/K^\times\mathcal{O}^\times$ is still a finite elementary 2-group (one has to work out the places dividing the level of $\mathcal{O}$, defined as the product of local levels).

Let us define the *adèlisation* of a lattice Λ in B as the product

$$\widehat{\Lambda} := \prod_v \Lambda_v \quad (\text{with } \Lambda_v = B_v \text{ if } v \text{ is archimedean}),$$

regarded inside $\widehat{B}$. This way, we have for example the *adèlisation* $\widehat{\mathcal{O}}$ of an order $\mathcal{O}$ in $\widehat{B}$, its group of units $\widehat{\mathcal{O}}^\times$ and its normaliser $N(\widehat{\mathcal{O}})$ in $\widehat{B}^\times$. For a fixed Eichler order $\mathcal{O}$ of level N, one therefore obtains a global-adèlic dictionary related to $\mathcal{O}$: for instance, the set of left (resp. two-sided) $\mathcal{O}$-ideals is in bijection with $\widehat{\mathcal{O}}^\times \setminus \widehat{B}^\times$ (resp. $\widehat{\mathcal{O}}^\times \setminus N(\widehat{\mathcal{O}})$), whereas the set of Eichler orders of level N corresponds to $N(\widehat{\mathcal{O}}) \setminus \widehat{B}^\times$.

Similarly, the set $\mathrm{Pic}_r(\mathcal{O})$ of right-classes of left $\mathcal{O}$-ideals is in bijection with the double coset space $\widehat{\mathcal{O}}^\times \setminus \widehat{B}^\times / B^\times$, and the set of conjugacy classes of Eichler orders of level N corresponds to $B^\times \setminus \widehat{B}^\times / N(\widehat{\mathcal{O}})$. In analogy to the number field case, it is natural to think that these sets are finite, and their cardinality related to the class number of B. Indeed, using [**Vig80**, Ch. III, Théorème

fondamental, p. 61] one can prove that the set $\mathrm{Pic}_r(\mathcal{O})$ is finite, from which it follows that there are only finitely many conjugacy classes of Eichler orders of a given level.

Now we turn our attention to *not totally definite* quaternion algebras over K. That is to say, we assume that there exists a real place of K at which B is split (i.e. indefinite). Let $\mathrm{Frac}(K)$ be the group of fractional ideals of K, and let P_B be its subgroup of principal ideals which are generated by an element in K_B (that is, by an element which is positive at all real ramified places of B). If B is totally indefinite, notice that P_B is the whole subgroup of principal ideals of K. Let h_B be the cardinality of the quotient group $\mathrm{Frac}(K)/P_B$, and observe that $h_K \leq h_B \leq h_K^+$, where h_K and h_K^+ denote the class number and the narrow class number of K, respectively.

THEOREM 1.29 (Eichler). *Let B be a not totally definite quaternion algebra over K, and $\mathcal{O}$ be an Eichler order in B. The reduced norm induces a bijection* $\mathrm{n} : \mathrm{Pic}_r(\mathcal{O}) \to \mathrm{Frac}(K)/P_B$. *In particular, h_B is the class number of B.*

The proof of Eichler's theorem relies mainly on the strong approximation theorem. If v is a real place of K at which B is indefinite, notice that $B^1 B_v^1$ is dense in $\widehat{B}^1$. Then the map

$$\widehat{\mathcal{O}}^\times \setminus \widehat{B}^\times / B^\times \longrightarrow \widehat{R}^\times \setminus \mathbb{A}_K^\times / K_B^\times$$

induced by the reduced norm is shown to be a bijection.

As an immediate corollary of Eichler's theorem, indefinite rational quaternion algebras (that is, quaternion algebras over $\mathbb{Q}$ which are split at the only infinite place) have all class number one:

COROLLARY 1.30. *If B is an indefinite quaternion algebra over $\mathbb{Q}$, then the class number of B is* 1. *In particular, all maximal orders in B are conjugate one to each other.*

Finally, we review the formula for the number of optimal embeddings of quadratic orders into Eichler orders in a not totally definite quaternion algebra B over K. Let S be an order in a quadratic field extension L of K, and let $\mathcal{O}$ be an Eichler order in B. For every finite prime $\mathfrak{p}$ of K, write $v_\mathfrak{p}(S, \mathcal{O})$ for the number of optimal embeddings of $S_\mathfrak{p}$ into $\mathcal{O}_\mathfrak{p}$ modulo conjugation by $\mathcal{O}_\mathfrak{p}^\times$.

THEOREM 1.31. *Let B be a not totally definite quaternion algebra over K, and S be an order in a quadratic field extension L of K. Let $\mathcal{O}$ be an Eichler order in B, and let $\mathcal{O}_i$, $i = 1, \ldots, h_B$, be the left orders of a set of representatives in* $\mathrm{Pic}_r(\mathcal{O})$. *If $v(S, \mathcal{O}_i)$ denotes the number of optimal embeddings of S into $\mathcal{O}_i$ modulo conjugation by $\mathcal{O}_i^\times$, then*

$$\sum_{i=1}^{h_B} v(S, \mathcal{O}_i) = h(S) \prod_{\mathfrak{p}} v_\mathfrak{p}(S, \mathcal{O}_i), \tag{1.8}$$

where the product is over all the non-archimedean places and $h(S)$ is the class number of S.

Even though the formula (1.8) is rather cumbersome in general, notice that it becomes quite amenable when there is a unique conjugacy class of Eichler orders. In this thesis we mainly work with rational quaternion algebras, that is to say, over $K = \mathbb{Q}$, where this condition holds. Let us briefly describe the previous general theory in this particular setting.

Let B be a rational quaternion algebra. First of all, we know by Theorem 1.24 that $\mathrm{Ram}(B)$ is a finite set of places of $\mathbb{Q}$ of even cardinality. The *reduced discriminant* of B is then defined as the positive integer

$$\mathrm{disc}(B) := \prod_{\substack{p \in \mathrm{Ram}(B), \\ p \text{ finite}}} p.$$

Up to isomorphism, there is a unique rational quaternion algebra of reduced discriminant D for each square-free positive integer D. Let B_D denote any representative in this isomorphism class. Following our previous notations, we write $B_{D,v} := B_D \otimes_\mathbb{Q} \mathbb{Q}_v$ for the localisation of B_D at each place v of $\mathbb{Q}$. According to whether $B_{D,\infty}$ is division (i.e. isomorphic to $\mathbb{H}$) or not, B_D is said to be *definite* or *indefinite*, respectively. Equivalently, B_D is definite if D is the product of an odd number of primes, and indefinite otherwise.

If $B_D = (\frac{a,b}{\mathbb{Q}})$ for some $a, b \in \mathbb{Q}^\times$, the reduced discriminant D can be easily computed from a and b. Indeed, the local Hasse invariants of B_D at finite odd primes p are easily computed in terms of the Legendre symbol $(\frac{\cdot}{p})$ (see [**Vig80**, p. 37]), whereas the local Hasse invariant at the real place ∞ is -1 if and only if both a and b are negative. By (1.7), the local Hasse invariant at 2 is then determined and one deduces the set of ramified places of B_D.

On the other hand, since $B_{D,p}$ is split for every finite prime p not dividing D, observe that Hasse's criterion from Theorem 1.25 becomes very simple for rational quaternion algebras:

COROLLARY 1.32. *Let B_D be a rational quaternion algebra of reduced discriminant D, and let $F/\mathbb{Q}$ be a quadratic field. If F is real and B_D is definite, then F does not split B_D. Otherwise, F splits B_D if and only if every prime $p \mid D$ is non-split in F.*

Concerning the integral theory of orders and ideals (with respect to $\mathbb{Z}$), we have already seen in Corollary 1.30 that if B_D is indefinite, then all the maximal orders are conjugate. When B_D is definite, we refer the reader to [**Vig80**, Section III.5] for class number formulas.

Lastly, the question of whether a quadratic order embeds into an order $\mathcal{O}$ in B_D or not, and if so, a formula for the number of optimal embeddings, is also a local issue by virtue of Theorem 1.31. Indeed, by combining Theorem 1.31 with Theorems 1.21 and 1.22, we deduce the following result, where if S is an order in a quadratic field $K/\mathbb{Q}$ and ℓ is a rational prime,

$$\left\{\frac{S}{\ell}\right\} := \begin{cases} 1 & \text{if } \ell \text{ divides the conductor of } S, \\ \left(\frac{K}{\ell}\right) & \text{otherwise} \end{cases}$$

is the Eichler symbol (cf. (1.3)).

COROLLARY 1.33. *Let B_D be a rational quaternion algebra of reduced discriminant D, and $\mathcal{O}$ be an Eichler order in B_D of square-free level N. If S is an order in a quadratic field, then the number of optimal embeddings of S into $\mathcal{O}$, modulo conjugation by $\mathcal{O}^\times$, is*

$$h(S)\prod_{p|D}\left(1-\left\{\frac{S}{p}\right\}\right)\prod_{q|N}\left(1+\left\{\frac{S}{q}\right\}\right),$$

where the products are over the prime divisors of D and N, respectively, and $h(S)$ is the class number of S.

In particular, observe that if $\mathcal{O}$ is a maximal order and S is the ring of integers of a quadratic field F over $\mathbb{Q}$, then the number of optimal embeddings of S into $\mathcal{O}$ modulo conjugation by $\mathcal{O}^\times$ is $h(S)2^s$, where s is the number of prime divisors of D which are inert in F.

3. Shimura curves

Fix throughout this section an indefinite rational quaternion algebra B_D of reduced discriminant $D > 1$, and a maximal order $\mathcal{O}_D \subseteq B_D$ (which is unique up to conjugation). The reduced norm on B_D will be denoted by $\mathrm{n} : B_D \to \mathbb{Q}$ as usual. Fix also an isomorphism $\Psi : B_D \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\sim} \mathrm{M}_2(\mathbb{R})$, under which the group of units of norm 1 in $B_D^\times$ acts by conformal transformations on the complex upper half plane $\mathcal{H} := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$. Similarly, the group of units $B_D^\times$ acts naturally by linear fractional transformations on $\mathcal{H}^\pm := \mathbb{P}^1(\mathbb{C}) - \mathbb{P}^1(\mathbb{R}) = \mathbb{C} - \mathbb{R}$.

3.1. Adèlic formalism. Let $\mathbb{A}_\mathbb{Q}$ and $\mathbb{A}_f := \mathbb{A}_{\mathbb{Q},f}$ denote the ring of $\mathbb{Q}$-adèles and finite $\mathbb{Q}$-adèles, respectively. Write $\widehat{\mathbb{Z}} := \prod_v \mathbb{Z}_v$ for the profinite completion of the ring of integers, and $\widehat{\mathcal{O}}_D := \mathcal{O}_D \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$. For a compact open subgroup $U \subseteq \widehat{\mathcal{O}}_D^\times$, consider the topological space of double cosets

$$X_U := B_D^\times \backslash (\mathcal{H}^\pm \times (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times / U), \tag{1.9}$$

where $B_D^\times$ acts simultaneously on the left on both $\mathcal{H}^\pm$ and $(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$, and U acts on the right on $(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$: that is, for $z \in \mathcal{H}^\pm$, $\beta = (\beta_v)_v \in (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$, $b \in B_D^\times$ and $u = (u_v)_v \in U$,

$$b \cdot (z, \beta) \cdot u = (bz, b\beta u) = (bz, (b\beta_v u_v)_v).$$

After the work of Shimura and Deligne (see, e.g., [**Shi63, Shi67, Del71, Mil04**]), X_U admits a canonical model which is an algebraic curve over $\mathbb{Q}$. By a slight abuse of notation, we still denote this canonical model by X_U.

DEFINITION 1.34. *For every compact open subgroup $U \subseteq \widehat{\mathcal{O}}_D^\times$, we will refer to $X_U/\mathbb{Q}$ as the* Shimura curve associated with U.

Notice that the Shimura curve X_U need not be geometrically connected: in general, $X_U \times_{\mathbb{Q}} \mathbb{C}$ is the disjoint union of $|\widehat{\mathbb{Z}}^\times/\mathrm{n}(U)|$ compact connected complex curves. Indeed, let us define the double coset space

$$\mathcal{C}_\infty(U) := B_{D,+}^\times \backslash (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times / U, \tag{1.10}$$

where $B_{D,+}^\times := \{b \in B_D^\times : \mathrm{n}(b) > 0\}$. By means of the natural homeomorphism[3]

$$B_D^\times \backslash \mathcal{H}^\pm \times (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times \longrightarrow B_{D,+}^\times \backslash \mathcal{H} \times (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times,$$

we see from the very definition of X_U that there is a natural projection

$$\mathrm{pr}_U : X_U \times_{\mathbb{Q}} \mathbb{C} \longrightarrow B_{D,+}^\times \backslash (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times / U = \mathcal{C}_\infty(U).$$

Using that B_D is indefinite, the reduced norm induces an isomorphism

$$\mathcal{C}_\infty(U) = B_{D,+}^\times \backslash (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times / U \xrightarrow{\simeq} \mathbb{Q}^{>0} \backslash \mathbb{A}_f^\times / \mathrm{n}(U) \simeq \widehat{\mathbb{Z}}^\times / \mathrm{n}(U), \tag{1.11}$$

which shows that $\mathcal{C}_\infty(U)$ is actually a finite set, whose cardinality is precisely $|\widehat{\mathbb{Z}}^\times/\mathrm{n}(U)|$. The connected components of $X_U \times_{\mathbb{Q}} \mathbb{C}$ are therefore the (finitely many) fibres of pr_U (see [**Mil04**, Lemmas 5.12, 5.13]), thus we deduce that the set $\pi_0(X_U \times_{\mathbb{Q}} \mathbb{C})$ of geometric connected components of X_U is in bijection with the (finite) set $\mathcal{C}_\infty(U)$.

For every $\beta \in (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$, let us write $[\beta] \in \mathcal{C}_\infty(U)$ for its image in $\mathcal{C}_\infty(U)$. The stabiliser of $[\beta]$ with respect to the left action of $B_{D,+}^\times$ is then easily seen to be

$$\Gamma_\beta := B_{D,+}^\times \cap \beta U \beta^{-1}.$$

By using the isomorphism Ψ, the groups Γ_β should be regarded as cocompact subgroups of $\mathrm{GL}_2^+(\mathbb{R})$ (we can even consider their images in $\mathrm{PGL}_2(\mathbb{R})$), and therefore act by linear fractional transformations on $\mathcal{H}$. The quotients $\Gamma_\beta \backslash \mathcal{H}$ are hence compact connected Riemann surfaces. Letting β vary over a set of representatives in $\mathcal{C}_\infty(U)$, one obtains the decomposition of $X_U \times_{\mathbb{Q}} \mathbb{C}$ as a disjoint union of its connected components:

$$X_U \times_{\mathbb{Q}} \mathbb{C} \quad = \quad \bigsqcup_{[\beta] \in \mathcal{C}_\infty(U)} \mathrm{pr}_U^{-1}[\beta] \quad \simeq \quad \bigsqcup_{[\beta] \in \mathcal{C}_\infty(U)} \Gamma_\beta \backslash \mathcal{H}. \tag{1.12}$$

On the arithmetic side, even though the curve X_U is defined over $\mathbb{Q}$, its geometric connected components may not be so. However, they are always defined over an abelian extension of $\mathbb{Q}$. Indeed, write as usual $\mathbb{Q}^{ab}$ for the maximal abelian extension of $\mathbb{Q}$. The choice of the model $X_U/\mathbb{Q}$ defines an action of $\mathrm{Aut}(\mathbb{C})$ on $X_U(\mathbb{C}) = (X_U \times_{\mathbb{Q}} \mathbb{C})(\mathbb{C})$, which is compatible with the action of $\mathrm{Aut}(\mathbb{C})$ on the set of geometric connected components

$$\mathcal{C}_\infty(U) \simeq \widehat{\mathbb{Z}}/\mathrm{n}(U)$$

of X_U through its quotient $\mathrm{Gal}\,(\mathbb{Q}^{ab}/\mathbb{Q}) \simeq \widehat{\mathbb{Z}}^\times$ under the map

$$\begin{array}{ccccc} X_U \times_{\mathbb{Q}} \mathbb{C} \simeq B_{D,+}^\times \backslash \mathcal{H} \times (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times / U & \longrightarrow & \mathbb{Q}^{>0} \backslash \mathbb{A}_f^\times / \mathrm{n}(U) \simeq \widehat{\mathbb{Z}}^\times / \mathrm{n}(U) \\ [z, b] & \longmapsto & [\mathrm{n}(b)]. \end{array}$$

Using the previous notation, the geometric connected component of X_U corresponding to $[\beta]$ is therefore defined over the finite abelian extension $K_\beta/\mathbb{Q}$ corresponding, by class field theory, to the subgroup

$$\mathrm{Stab}_{\widehat{\mathbb{Z}}^\times}([\mathrm{n}(\beta)]) = \{g \in \widehat{\mathbb{Z}}^\times : [g\mathrm{n}(\beta)] = [\mathrm{n}(\beta)]\} \subseteq \widehat{\mathbb{Z}}^\times \simeq \mathrm{Gal}\,(\mathbb{Q}^{ab}/\mathbb{Q}).$$

[3]We could have defined X_U in (1.9) as the topological space of double cosets $B_{D,+}^\times \backslash \mathcal{H} \times (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times / U$.

When we let U vary, the algebraic curves X_U fit together into a projective system indexed by the compact open subgroups U of $(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$, as there is a natural projection $X_{U'} \to X_U$ whenever $U' \subseteq U$. This projective system is endowed with a natural action of $(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$ by right multiplication: if $b \in (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$, right multiplication by b induces an isomorphism of algebraic curves

$$\rho_U(b) : X_U \longrightarrow X_{b^{-1}Ub}. \tag{1.13}$$

Notice that for every $b \in \mathrm{Norm}_{(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times}(U)$, the isomorphism $\rho_U(b)$ is actually an automorphism of X_U. This leads to consider the group of automorphisms

$$\mathrm{Aut}^{\mathrm{mod}}(X_U) := \mathrm{Norm}_{(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times}(U)/\mathbb{Q}^\times U. \tag{1.14}$$

Moreover, one has $\mathrm{Aut}^{\mathrm{mod}}(X_U) \subseteq \mathrm{Aut}_{\mathbb{Q}}(X_U)$ (cf. [**Mil04**, Theorem 13.6]).

Definition 1.35. *An automorphism of X_U is called* modular *if it is of the form $\rho_U(b)$ for some $b \in \mathrm{Norm}_{(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times}(U)$. We call $\mathrm{Aut}^{\mathrm{mod}}(X_U)$ the* group of modular automorphisms *of X_U, regarded as a subgroup of $\mathrm{Aut}_{\mathbb{Q}}(X_U)$.*

As we will recall below, the group $\mathrm{Aut}^{\mathrm{mod}}(X_D)$ of modular automorphisms of the usual Shimura curve $X_D/\mathbb{Q}$ associated to the maximal order $\mathcal{O}_D$ is the so-called *Atkin-Lehner group*, or group of *Atkin-Lehner involutions*. Besides, in Chapter 2 we will determine the group of modular automorphisms of the covering $X_{D,\ell} \to X_D$ of Shimura curves associated to an odd prime $\ell \mid D$.

3.2. Moduli interpretation. We now discuss briefly the moduli interpretation of Shimura curves X_U introduced above. Further details and references can be found in [**Shi63, Shi67, BC91**], for example. Let us assume that our fixed maximal order $\mathcal{O}_D$ in B_D (which is unique up to conjugation) is stable under the canonical involution $b \mapsto \bar{b}$ on B_D. We can choose $\mathcal{O}_D$ in such a way, as we can do it locally at all places.

Let $* : B_D \to B_D$ be a positive (anti-)involution. By the Noether-Skolem Theorem, $*$ is conjugate to the canonical involution. That is to say, there exists $\mu \in B_D^\times$ (determined by $*$ up to multiplication by $\mathbb{Q}^\times$) such that

$$b^* = \mu^{-1}\bar{b}\mu \quad \text{for all } b \in B_D.$$

Moreover, the positiveness of $*$ implies that $\mathrm{tr}(\mu) = 0$ and $\mathrm{n}(\mu) \in \mathbb{Q}^{>0}$ (see [**Rot03**]), hence μ satisfies a quadratic equation of the form $\mu^2 + \delta = 0$ for some $\delta > 0$. Noticing that $\mathbb{Q}(\sqrt{-D})$ splits B_D, observe that we can choose $\mu \in \mathcal{O}_D$ such that $\mu^2 + D = 0$. We will assume henceforth that $*$ is the positive (anti-)involution associated to such an element μ, and write $*_\mu$ to emphasise it. Having fixed these choices at the outset, the triple $(B_D, \mathcal{O}_D, *_\mu)$ is sometimes referred to as a *quaternionic datum*.

In order to state the moduli problem represented by the Shimura curve X_U, first over $\mathbb{C}$, we shall define the notion of level U structure on an abelian surface with quaternionic multiplication. So let S be a $\mathbb{C}$-scheme, and A be an abelian scheme over S of relative dimension 2 endowed with an action of $\mathcal{O}_D$, say

$$\iota : \mathcal{O}_D \longrightarrow \mathrm{End}_S(A).$$

If $U = U(N)$ is the group of units in $\widehat{\mathcal{O}}_D$ which are congruent to 1 modulo N, then a level $U(N)$ structure on (A, ι) is an $\mathcal{O}_D$-linear isomorphism

$$\nu : A[N] \xrightarrow{\simeq} \mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{Z}/N\mathbb{Z}. \tag{1.15}$$

Here, $A[N]$ denotes the N-torsion subgroup (regarded as a group S-scheme) of A as usual, endowed with an action of $\mathcal{O}_D$ induced naturally by ι, and notice that $\mathcal{O}_D$ acts also on $\mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{Z}/N\mathbb{Z}$ through the natural action on $\mathcal{O}_D$.

For a general U, choose first an integer N such that $U(N) \subseteq U$. Then a level U structure on (A, ι) consists, by definition, in giving (locally for the étale topology) a class $\bar{\nu}$ modulo U of

isomorphisms ν as in (1.15). One can check that this definition does not depend on the choice of the integer N.

Besides, assume that we have a triple $(A, \iota, \bar{\nu})$ as above. Then a $*$-*polarisation* on A, or a polarisation compatible with $*$, is a polarisation λ on A such that, for all geometric points s of S, the Rosati involution $'$ associated to λ on $\mathrm{End}^0(A_s)$ satisfies $\iota(\gamma)' = \iota(\gamma^*)$ for all $\gamma \in \mathcal{O}_D$. Equivalently, one may ask that the diagram

$$\begin{array}{ccc} A & \xrightarrow{\lambda} & A^\vee \\ {\scriptstyle \iota(\gamma^*)}\downarrow & & \downarrow{\scriptstyle \iota(\gamma)^\vee} \\ A & \xrightarrow{\lambda} & A^\vee \end{array}$$

commutes for every $\gamma \in \mathcal{O}_D$.

THEOREM 1.36. *The curve $X_U/\mathbb{C}$ represents, if U is* small enough*, the functor*

$$\mathcal{F}_U : \mathrm{Schemes}_{\mathbb{C}} \longrightarrow \mathrm{Sets} \tag{1.16}$$

sending a $\mathbb{C}$-scheme S to the collection $\mathcal{F}_U(S)$ of isomorphism classes of triples $(A, \iota, \bar{\nu})$, where:

i) *A/S is an abelian scheme of relative dimension 2, endowed with a principal $*$-polarisation,*
ii) *$\iota : \mathcal{O}_D \hookrightarrow \mathrm{End}_S(A)$ is an action of $\mathcal{O}_D$ on A, and*
iii) *$\bar{\nu}$ is a level U structure on A.*

REMARK 1.37. The condition on U to be *small enough* is to ensure that the level U structure is rigid enough to avoid non-trivial automorphisms. It suffices, for example, that U be a subgroup of the group $U(N)$ of units in $\widehat{\mathcal{O}}_D$ that are congruent to 1 modulo an integer $N \geq 3$.

REMARK 1.38. When $S = \mathrm{Spec}(k)$ with k an algebraically closed field, giving a level U structure is the same as giving a class modulo U of $\mathcal{O}_D$-linear isomorphisms

$$T_f(A) \xrightarrow{\simeq} \mathcal{O}_D \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}} = \widehat{\mathcal{O}}_D,$$

where $T_f(A)$ is the product of all the Tate modules $T_\ell(A)$ of A for all prime numbers ℓ. Further, one can work in the category of abelian surfaces up to isogeny, and in this case giving a level U structure amounts to giving a class modulo U of $\mathcal{O}_D$-linear isomorphisms

$$V_f(A) \xrightarrow{\simeq} \mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{A}_f,$$

where $V_f(A)$ is the restricted product of all the $\mathbb{Q}_\ell$-vector spaces $V_\ell(A) := T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ with respect to $T_f(A)$.

The moduli problem described by the functor $\mathcal{F}_U$ from (1.16) is in fact defined and representable over $\mathbb{Q}$, thus it affords a $\mathbb{Q}$-structure on X_U (as we announced above). This $\mathbb{Q}$-structure is recovered as the generic fibre of a proper smooth curve over $\mathbb{Z}[1/DN]$ (where N is an integer such that $U(N) \subseteq U$).

Concerning the $*$-polarisation on the triples $(A, \iota, \bar{\nu})$, we first observe that one can equivalently ask for a *weak* polarisation instead of a principal polarisation. That is to say, a $\mathbb{Q}$-equivalence class[4] of polarisations. However, in order to simplify matters, we will omit the $*$-polarisation attached to a triple $(A, \iota, \bar{\nu})$ in the above moduli problem because of the following result due to Milne (see [**Mil79**]):

PROPOSITION 1.39 (Milne). *Let S be a scheme in characteristic zero, and $(A, \iota, \bar{\nu}) \in \mathcal{F}_U(S)$. Then there exists a unique principal $*$-polarisation on A.*

[4]Two polarisations $\lambda, \lambda' : A \to A^\vee$ on A are said to be $\mathbb{Q}$-equivalent if there exist positive integers m, n such that $m\lambda = n\lambda'$.

The moduli problem in Theorem 1.36 can be extended to a moduli problem over arbitrary schemes over $\mathbb{Z}$, giving rise to a smooth model of X_U over $\mathbb{Z}$ (and even over $\mathbb{Z}[1/DN]$ if the integer $N \geq 1$ is chosen such that $U(N) \subseteq U$), known as Morita's model of X_U (see [**Mor81**]). If p is a prime at which U is *maximal*, meaning that $U_p = \mathcal{O}_{D,p}^\times$, then the moduli problem can also be extended to arbitrary $\mathbb{Z}_p$-schemes as explained for example in [**BC91**, Chapter III], giving rise to a model over $\mathbb{Z}_p$ of X_U. At primes of bad reduction, these models are described by Čerednik-Drinfeld theory. We elaborate more on this topic in Chapter 3.

3.3. The Shimura curve X_D. When we take U to be $\widehat{\mathcal{O}}_D^\times$, the curve $X_D := X_{\widehat{\mathcal{O}}_D^\times}$ is the usual Shimura curve associated with the indefinite rational quaternion algebra B_D (recall that $D > 1$). Its canonical model over $\mathbb{Q}$, which we still denote by $X_D/\mathbb{Q}$, is the coarse moduli scheme over $\mathbb{Q}$ classifying abelian surfaces with quaternionic multiplication (QM) by $\mathcal{O}_D$, also known as *fake elliptic curves*. That is to say, pairs (A, ι) where A is an abelian surface and $\iota : \mathcal{O}_D \hookrightarrow \mathrm{End}(A)$ is a monomorphism of rings (see [**Shi63, Shi67**]). As discussed above, we omit the polarisation on A compatible with the choice of a positive anti-involution $*_\mu$ making $(B_D, \mathcal{O}_D, *_\mu)$ a quaternionic datum.

The curve X_D is projective and smooth, and it depends neither on the choice of $\mathcal{O}_D$ nor of Ψ, which are unique up to conjugation. By strong approximation, the set $\mathcal{C}_\infty(\widehat{\mathcal{O}}_D^\times)$ is trivial (alternatively, use in (1.11) that $\mathbb{Q}$ has class number one), hence $X_D/\mathbb{Q}$ is geometrically connected. Furthermore, from (1.12), we have an isomorphism of compact Riemann surfaces

$$X_D(\mathbb{C}) \simeq \mathcal{O}^1 \setminus \mathcal{H},$$

where $\mathcal{O}^1 := \{\gamma \in \mathcal{O}^\times : \mathrm{n}(\gamma) = 1\}$ shall be regarded as a subgroup of $\mathrm{GL}_2(\mathbb{R})$ under the embedding $B_D^\times \hookrightarrow \mathrm{GL}_2(\mathbb{R})$ induced by our fixed isomorphism $\Psi : B_D \otimes_{\mathbb{Q}} \mathbb{R} \to \mathrm{M}_2(\mathbb{R})$.

The natural complex uniformisation map

$$\Phi : \mathcal{H} \longrightarrow \mathcal{O}^1 \setminus \mathcal{H} \simeq X_D(\mathbb{C}) \tag{1.17}$$

was described in terms of moduli by Shimura. Namely, the image under Φ of an arbitrary $z \in \mathcal{H}$ is the closed point in $X_D(\mathbb{C})$ corresponding to the isomorphism class $[(A_z, \iota_z)]$ of the abelian surface with QM by $\mathcal{O}_D$ defined as

$$A_z := \mathbb{C}^2/\Lambda_z, \quad \text{where} \quad \Lambda_z := \mathcal{O}_D \begin{pmatrix} z \\ 1 \end{pmatrix} \subset \mathbb{C}^2,$$

together with the natural monomorphism $\iota_z : \mathcal{O}_D \hookrightarrow \mathrm{End}(A_z)$.

Let us now say a few words about the existence of points on X_D rational over various fields. First of all, let us sketch a proof of a particular case of a theorem of Shimura stating the non-existence of real points on Shimura varieties (see [**Shi75**, Theorem 0]):

Theorem 1.40 (Shimura). *The curve X_D has no real points, that is, $X_D(\mathbb{R}) = \emptyset$.*

Proof. Using the complex uniformisation Φ from (1.17), the real structure on X_D is such that

$$\overline{\Phi(z)} = \Phi(\varepsilon \bar{z}),$$

where $z \mapsto \bar{z}$ denotes the complex conjugation and $\varepsilon \in \mathcal{O}_D^\times$ is any unit of reduced norm -1. Then a real point on X_D would be a point $P \in X_D(\mathbb{C})$ such that $\bar{P} = P$. If $P = \Phi(z)$ for some $z \in \mathcal{H}$, this is the same as saying that $z = \gamma\varepsilon\bar{z}$ for some $\gamma \in \mathcal{O}_D^1$, or equivalently, that

$$z = \beta\bar{z} \quad \text{for some } \beta \in \mathcal{O}_D^\times, \quad \mathrm{n}(\beta) = -1.$$

By means of our fixed identification $\Psi : B_D \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\sim} \mathrm{M}_2(\mathbb{R})$, write

$$\Psi(\beta) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$$

for the linear fractional transformation through which the element β acts on $\mathcal{H}^\pm$. Then the above equality implies that $az + b = c|z|^2 + d\bar{z}$. By comparing the imaginary parts, we obtain

$\mathrm{tr}(\beta) = a + d = 0$ and therefore β satisfies the quadratic equation $\beta^2 = 1$. Since B_D is indefinite, we deduce that $\beta = \pm 1$, but this contradicts the fact that $\mathrm{n}(\beta) = -1$. This shows that X_D does not have real points. □

A fortiori, it follows that the set $X_D(\mathbb{Q})$ of $\mathbb{Q}$-rational points on X_D is empty as well. As a consequence, the sets $X_U(\mathbb{R})$ and $X_U(\mathbb{Q})$ are therefore empty for every compact open subgroup $U \subseteq \widehat{\mathcal{O}}_D^\times$: otherwise, the natural projection $X_U \to X_D$ would produce a real, resp. rational, point on X_D.

More in general, the existence of points on X_D rational over local fields is well understood. Indeed, besides the above theorem, the existence of points on X_D rational over finite extensions K of $\mathbb{Q}_p$, for any given rational prime p, was precisely characterised by Jordan and Livné [**JL85**]. If $p \nmid D$, the Shimura curve X_D has good reduction at p, and a criterion for the existence of points in $X_D(K)$ follows from the Eichler-Selberg Trace Formula. In contrast, the primes $p \mid D$ are exactly the primes of bad reduction for X_D, and a criterion for the existence of points in $X_D(K)$ requires the theory of Čerednik and Drinfeld. We refer the reader to *ibid.* for an accurate exposition.

On the other hand, the existence of rational points on X_D over number fields is far more challenging. The question of whether the set $X_D(K)$ is empty or not for a general number field K is widely open. After the work of Mazur on rational points on the modular curves $X_1(N)$ in his celebrated article [**Maz77**], which started a research line that has been intensively and successfully explored by many others, the general philosophy is that rational points on (modular and) Shimura curves should correspond only to (cusps or) CM-points, except for a few exceptional cases. Because of their importance, we will introduce and describe briefly CM-points on Shimura curves below (see Section 3.5).

3.4. Atkin-Lehner involutions and quotients. The group of modular automorphisms $\mathrm{Aut}^{\mathrm{mod}}(X_D)$ of X_D is isomorphic to the group

$$W_D := \mathrm{Norm}_{B_D^\times}(\mathcal{O}_D)/\mathbb{Q}^\times \mathcal{O}_D^\times \simeq (\mathbb{Z}/2\mathbb{Z})^{2r},$$

where $2r$ is the number of prime factors of D (see Proposition 1.28 above, or [**Vig80**, Chap. III, Exercises 5.4, 5.5], [**Mic81**, Proposition 1]). The above isomorphism provides a one-to-one correspondence between the automorphisms in $W_D \subseteq \mathrm{Aut}_{\mathbb{Q}}(X_D)$, all of them being rational involutions, and the positive divisors of D. In fact, the class in $\mathrm{Norm}_{B_D^\times}(\mathcal{O}_D)/\mathbb{Q}^\times \mathcal{O}_D^\times$ corresponding to a positive divisor m of D is represented by any generator $w_m \in \mathcal{O}_D$ of the unique two-sided ideal of reduced norm m in $\mathcal{O}_D$.

Definition 1.41. *The group W_D is called the* Atkin-Lehner group *of X_D (or of $\mathcal{O}_D$). For each positive divisor m of D, we write $\omega_m = [w_m]$ for the involution in W_D corresponding to m, and call it the* Atkin-Lehner involution *associated with m.*

It is plain that all the Atkin-Lehner involutions commute one with each other, and furthermore

$$\omega_m \omega_{m'} = \omega_{\frac{mm'}{\gcd(m,m')^2}}, \quad \text{for all integers } m, m' | D, m, m' > 0.$$

An easy exercise shows that, in the above adèlic formalism, the Atkin-Lehner involution ω_q associated to each prime divisor q of D corresponds to the modular automorphism

$$\rho_{\widehat{\mathcal{O}}_D^\times}(\mathrm{w}_q) := \rho_{\widehat{\mathcal{O}}_D^\times}(1, \dots, 1, \mathrm{w}_q, 1, 1, \dots),$$

where w_q is any element in $\mathrm{Norm}_{B_{D,q}^\times}(\mathcal{O}_{D,q}^\times) \cap \mathcal{O}_{D,q}$ such that $\mathrm{val}_q(\mathrm{n}(\mathrm{w}_q)) = 1$. In particular, after identifying $\mathcal{O}_{D,q}$ with a matrix subring of $\mathrm{M}_2(\mathbb{Z}_{q^2})$ as in (1.5), we can choose

$$\mathrm{w}_q = \begin{pmatrix} 0 & 1 \\ q & 0 \end{pmatrix}.$$

And once we have defined the involutions ω_q for primes $q \mid D$, we can define the Atkin-Lehner involution ω_m associated with a positive divisor m of D just as the composition of the involutions ω_q with q varying over the prime factors of m.

REMARK 1.42. Usually, the group of modular automorphisms $\mathrm{Aut}^{\mathrm{mod}}(X_D) \simeq W_D$ of the Shimura curve X_D is actually the full group of automorphisms $\mathrm{Aut}(X_D)$ of $X_D \times_{\mathbb{Q}} \mathbb{C}$. The question of determining which Shimura curves admit *exceptional automorphisms* (i.e., automorphisms that are not Atkin-Lehner involutions) was addressed by Rotger in [**Rot02**] (see also [**KR08**] for the case of Shimura curves with non-trivial level). The question was motivated by previous work of Ogg [**Ogg77**] and Kenku and Momose [**KM88**], from which it is known that modular curves $X_0(N)$ of squarefree level N do not admit exceptional automorphisms, provided that $N \neq 37, 63$.

The moduli interpretation of the Atkin-Lehner involutions acting on the coarse moduli scheme X_D can be easily described by using the complex uniformisation (1.17) of X_D (cf. [**Jor81**, pp. 11-13]). Indeed, if we represent the Atkin-Lehner involution ω_m associated with a positive divisor $m \mid D$ by a generator $w_m \in \mathcal{O}_D$ of the unique two-sided $\mathcal{O}_D$-ideal of reduced norm m as above, and $P \in X_D(\bar{\mathbb{Q}})$ corresponds to the isomorphism class $[(A, \iota)]$ of an abelian surface (A, ι) with QM by $\mathcal{O}_D$, then $\omega_m(P)$ corresponds to $[(A, \iota_m)]$, where

$$\iota_m : \mathcal{O}_D \hookrightarrow \mathrm{End}(A), \quad \gamma \longmapsto \iota_m(\gamma) := \iota(w_m^{-1}\gamma w_m).$$

That is to say, ω_m acts on the moduli problem associated with X_D by preserving the underlying abelian surfaces and twisting the $\mathcal{O}_D$-action on them.

We denote the quotient of X_D by the action of ω_m by

$$X_D^{(m)} := X_D/\langle \omega_m \rangle,$$

and write $\pi_m : X_D \to X_D^{(m)}$ for the natural projection map.

DEFINITION 1.43. *For each positive divisor m of D, the curve $X_D^{(m)}/\mathbb{Q}$ is called the* Atkin-Lehner quotient of X_D by ω_m.

Curves $X_D^{(m)}$ admit a moduli interpretation, inherited from that of X_D, as we next describe following [**Rot04b**].

DEFINITION 1.44. *Let $\delta, m \geq 1$ be integers, with $m \mid D$. We say that $\mathcal{O}_D$ admits a* twist of degree δ and norm m *if there exist elements $\mu, \chi \in \mathcal{O}_D$ such that $\mu^2 = -D\delta$, $\chi^2 = m$ and $\mu\chi = -\chi\mu$. In other words, if*

$$B_D = \mathbb{Q} + \mathbb{Q}\mu + \mathbb{Q}\chi + \mathbb{Q}\mu\chi = \left(\frac{-D\delta, m}{\mathbb{Q}}\right).$$

If $\delta = 1$, we say that $\mathcal{O}_D$ admits a principal twist. *Fixed an element $\mu \in \mathcal{O}_D$, $\mu^2 + D\delta = 0$, we say that the pair $(\mathcal{O}_D, \mu)$ admits a* twist of norm $m \mid D$ *if there exists $\chi \in \mathcal{O}_D$ satisfying the above conditions.*

Note that $\mathcal{O}_D$ does not necessarily admit twists of a fixed degree $\delta \geq 1$. For later use in this thesis, however, we do point out the following observation:

LEMMA 1.45. *Assume $D = pm$ is odd, with p a prime such that $(\frac{m}{p}) = -1$. There exists an integer $\delta \geq 1$ such that $\mathcal{O}_D$ admits a twist of degree δ and norm m.*

PROOF. An easy computation of Hilbert symbols shows (using Čebotarev's Theorem) that there exist infinitely many primes δ such that $B_D \simeq (\frac{-D\delta, m}{\mathbb{Q}})$. Hence, we can choose $\mu, \chi \in B_D$ such that $\mu^2 + D\delta = 0$, $\chi^2 = m$ and $\mu\chi = -\chi\mu$. Furthermore, since $\mathbb{Z}[\mu, \chi]$ is an integral order in B_D and any maximal order is conjugated to $\mathcal{O}_D$, the elements μ and χ can be taken to lie in $\mathcal{O}_D$. □

Now fix a positive divisor m of D, and let us assume that $\mathcal{O}_D$ admits a twist of degree δ and norm $m \mid D$, for some integer $\delta \geq 1$. Then choose elements $\mu, \chi \in \mathcal{O}_D$ with $\mu^2 + D\delta = 0$, $\chi^2 = m$ and $\mu\chi = -\chi\mu$. Without loss of generality, we can assume that X_D is the Shimura curve attached to the quaternionic datum $(B_D, \mathcal{O}_D, *_\mu)$, where $*_\mu$ denotes the positive (anti-)involution associated with μ. Notice that since $\mathrm{n}(\chi) = -m$ and the set of elements of norm $\pm m$ in $\mathcal{O}_D$ is a homogenous

space under the action of $\mathcal{O}_D^\times$, we have $\chi = w_m\alpha$ for some $\alpha \in \mathcal{O}_D^\times$ of reduced norm -1. That is to say, $\chi \in \mathcal{O}_D \cap \mathrm{Norm}_{B_D^\times}(\mathcal{O}_D)$ induces the Atkin-Lehner involution ω_m.

Let us write $\mathcal{H}_m$ for the Hilbert modular surface classifying isomorphism classes of abelian surfaces with real multiplication by the ring of integers R_m of $\mathbb{Q}(\sqrt{m})$, or in other words, of pairs (A, i) where

- A is a (weakly polarised) abelian surface, and
- $i : R_m \hookrightarrow \mathrm{End}(A)$ is a ring monomorphism.

As we did for X_D, we omit the polarisation on A in order to simplify the discussion.

The element χ determines an embedding $\vartheta_\chi : R_m \hookrightarrow \mathcal{O}_D$ of R_m into $\mathcal{O}_D$, and this embedding induces a forgetful map

$$\pi_{R_m} : X_D \longrightarrow \mathcal{H}_m,$$

given in terms of moduli by the rule

$$[(A, \iota)] \longmapsto [(A, \iota_{|R_m})],$$

where $\iota_{|R_m} := \iota \circ \vartheta_\chi$. That is to say, the image of a closed point in X_D represented by a fake elliptic curve (A, ι) is the closed point in $\mathcal{H}_m$ obtained by forgetting the quaternionic structure on $\mathrm{End}(A)$ and just keeping the real multiplication given by the restriction of ι to R_m. The next statement is easily obtained by following the same arguments of the proof of [**Rot04a**, Theorem 4.4]:

PROPOSITION 1.46. *The map π_{R_m} is a quasi-finite map that factors over $\mathbb{Q}$ into the natural projection π_m of X_D onto its quotient $X_D^{(m)}$ and a birrational morphism*

$$b_{R_m} : X_D^{(m)} \dashrightarrow \pi_{R_m}(X_D) \subseteq \mathcal{H}_m$$

into the image of X_D by π_{R_m} in $\mathcal{H}_m$. Moreover, $b_{R_m}^{-1}$ is defined on the whole $\pi_{R_m}(X_D)$ except for a finite set of CM-points.

As a consequence, the Atkin-Lehner quotient $X_D^{(m)}/\mathbb{Q}$ is a solution to the coarse moduli problem of classifying abelian surfaces (A, i) with real multiplication by R_m and admitting quaternionic multiplication by $\mathcal{O}_D$ (these are sometimes called abelian surfaces with *potential quaternionic multiplication*). This means that $i : R_m \hookrightarrow \mathrm{End}(A)$ is the restriction to R_m of some ring monomorphism $\iota : \mathcal{O}_D \hookrightarrow \mathrm{End}(A)$, but notice that an isomorphism of pairs $(A, i) \simeq (A', i')$ may not extend to an isomorphism between the corresponding pairs (A, ι) and (A', ι').

3.5. CM-points on X_D and $X_D^{(m)}$. Shimura curves and their Atkin-Lehner quotients are supplied with special families of algebraic points which play a fundamental role in their arithmetic: the so-called *CM-points*. Fix as above a Shimura curve X_D, together with its complex uniformisation Φ. Recall also that $B_{D,+}^\times$ acts by linear fractional transformations on $\mathcal{H}$ through our fixed isomorphism $\Psi : B_D \otimes_{\mathbb{Q}} \mathbb{R} \to \mathrm{M}_2(\mathbb{R})$.

If $z \in \mathcal{H}$ is an arbitrary point, then its stabiliser $\mathrm{Stab}_{B_{D,+}^\times}(z)$ with respect to the action of $B_{D,+}^\times$ on $\mathcal{H}$ is either $\mathbb{Q}^\times$ or the group of units $K^\times$ of some imaginary quadratic field K. The former case is the generic situation.

DEFINITION 1.47. *If $z \in \mathcal{H}$ is such that $\mathrm{Stab}_{B_{D,+}^\times}(z) = K^\times$ for some imaginary quadratic field K, then z has* complex multiplication (CM) by K. *The set of points in $X_D(\mathbb{C})$ with complex multiplication by K is then defined naturally as*

$$\mathrm{CM}(K) := \{\Phi(z) : z \in \mathcal{H} \text{ has CM by } K\} \subseteq X_D(\mathbb{C}).$$

Notice that if $z \in \mathcal{H}$ has CM by an imaginary quadratic field K, then K necessarily splits the quaternion algebra B_D. Conversely, given a splitting imaginary quadratic subfield of $B_D^\times$, there is a common fixed point in $\mathcal{H}$ by all the elements in $K^\times$. This leads to a one-to-one correspondence between the set of points in $\mathcal{H}$ with CM by an imaginary quadratic field K and the set of quadratic subfields in B_D isomorphic to K.

In order to be more precise in the above bijection, a $\mathbb{Q}$-linear embedding $\vartheta : K \hookrightarrow B_D$ is said to be *normalised* if

$$\Psi(\vartheta(x)) \cdot \begin{pmatrix} z_\vartheta \\ 1 \end{pmatrix} = x \cdot \begin{pmatrix} z_\vartheta \\ 1 \end{pmatrix} \quad \text{for all} \quad x \in K^\times,$$

where $z_\vartheta \in \mathcal{H}$ denotes the unique common fixed point of $\vartheta(K^\times)$. Then we have one-to-one correspondences

$$\{z \in \mathcal{H} \text{ with CM by } K\} \longleftrightarrow \{\text{normalised } \mathbb{Q}\text{-linear embeddings } \vartheta : K \hookrightarrow B_D\} \tag{1.18}$$

and

$$\mathrm{CM}(K) \longleftrightarrow \frac{\{\text{normalised } \mathbb{Q}\text{-linear embeddings } \vartheta : K \hookrightarrow B_D\}}{\text{conjugation by elements in } \mathcal{O}_D^\times}. \tag{1.19}$$

Fix an imaginary quadratic field K splitting B_D. Then the (non-empty) set $\mathrm{CM}(K)$ is better understood by refining our definition of CM points on $\mathcal{H}$ in terms of orders. If $R \subseteq K$ is an order, we set

$$D(R) := \prod_{p \mid D, \{\frac{R}{p}\} = -1} p. \tag{1.20}$$

Since K splits B_D, notice that $D(R)$ is the product of the prime divisors of D which do not ramify in K and do not divide the conductor of R.

A point $z \in \mathcal{H}$ is said to have CM by an order $R \subseteq K$ if

$$\mathrm{Stab}_{\mathcal{O}_{D,+}}(z) \simeq R - \{0\}.$$

Similarly as above, we define the set of points in $X_D(\mathbb{C})$ with CM by R as the set

$$\mathrm{CM}(R) := \{\Phi(z) : z \in \mathcal{H} \text{ has CM by } R\} \subseteq X_D(\mathbb{C}),$$

and we obviously have

$$\mathrm{CM}(K) = \bigcup_{\substack{R \subseteq K \\ \text{order}}} \mathrm{CM}(R).$$

Now the bijections in (1.18) and (1.19) give rise directly to one-to-one correspondences

$$\{z \in \mathcal{H} \text{ with CM by } R\} \longleftrightarrow \{\text{normalised } R\text{-optimal } \mathbb{Q}\text{-linear embeddings } \vartheta : K \hookrightarrow B_D\} \tag{1.21}$$

and

$$\mathrm{CM}(R) \longleftrightarrow \frac{\{\text{normalised } R\text{-optimal } \mathbb{Q}\text{-linear embeddings } \vartheta : K \hookrightarrow B_D\}}{\text{conjugation by elements in } \mathcal{O}_D^\times}. \tag{1.22}$$

In view of (1.22), Corollary 1.33 implies directly the following:

Proposition 1.48. *Let K be an imaginary quadratic field and $R \subseteq K$ be an order. Then the set $\mathrm{CM}(R)$ is not empty if and only if $D/D(R)$ divides $\mathrm{disc}(R)$, the discriminant of R. In this case, if s denotes the number of prime divisors of $D(R)$, then*

$$|\,\mathrm{CM}(R)| = 2^s h(R),$$

where $h(R)$ is the class number of R.

The moduli interpretation of CM-points in $X_D(\mathbb{C})$ is easily described by applying the definitions, as it is shown in [**Jor81**, pp. 16-17]. Indeed, if (A, ι) is a QM-abelian surface let

$$\mathrm{End}(A, \iota) := \mathrm{End}_{\mathcal{O}_D}(A) := \{f \in \mathrm{End}(A) : f \circ \iota(\gamma) = \iota(\gamma) \circ f \text{ for all } \gamma \in \mathcal{O}_D\} \subseteq \mathrm{End}(A)$$

be the ring of endomorphisms of the pair (A, ι), and set

$$\mathrm{End}^0(A, \iota) := \mathrm{End}(A, \iota) \otimes_{\mathbb{Z}} \mathbb{Q} \subseteq \mathrm{End}^0(A).$$

We say that (A, ι) has CM by an order R in an imaginary quadratic field K if $\mathrm{End}(A, \iota) \simeq R$, and more generally we say that (A, ι) has CM by K if $\mathrm{End}^0(A, \iota) \simeq K$.

If we write $[(A,\iota)] = \Phi(z)$ for some $z \in \mathcal{H}$, then it follows immediately from the definitions that

$$\mathrm{End}(A,\iota) = \mathrm{Stab}_{\mathcal{O}_{D,+}}(z) \cup \{0\} \quad \text{and} \quad \mathrm{End}^0(A,\iota) = \mathrm{Stab}_{B_{D,+}^\times}(z) \cup \{0\},$$

thus the notion of complex multiplication for pairs (A,ι) and for points in $X_D(\mathbb{C})$ is consistent.

If (A,ι) is a QM-abelian surface, then observe that $\mathrm{End}(A) = \mathrm{End}(A,\iota) \otimes_{\mathbb{Z}} \mathcal{O}_D$, and similarly

$$\mathrm{End}^0(A) = \mathrm{End}^0(A,\iota) \otimes_{\mathbb{Q}} B_D.$$

Hence if $P = [(A,\iota)] \in \mathrm{CM}(K)$, then $\mathrm{End}^0(A) \simeq K \otimes_{\mathbb{Q}} B_D \simeq \mathrm{M}_2(K)$. Conversely, if $P = [(A,\iota)] \in X_D(\mathbb{C})$ is such that $\mathrm{End}^0(A) \simeq \mathrm{M}_2(K)$, then $P \in \mathrm{CM}(K)$. From this we deduce the following:

PROPOSITION 1.49. *A QM-abelian surface (A,ι) has complex multiplication by an imaginary quadratic field K if and only if $A \sim E \times E$, where E is an elliptic curve with complex multiplication by K.*

As shown in the foundational work of Shimura in [**Shi67**], the canonical model of X_D over $\mathbb{Q}$ obtained by extending the classification problem over $\mathbb{C}$ to a moduli problem over $\mathbb{Q}$ is distinguished by the number fields generated by the CM points. Observe that the complex uniformisation Φ is a transcendental map, hence *a priori* it is not expected at all that it takes on algebraic values when evaluated on algebraic arguments.

Following the exposition in [**GR06**, Section 5], which builds on previous work of Shimura [**Shi67**] and Jordan [**Jor81**, Ch. III], we review some rationality properties of CM points on X_D. Fix an order R of conductor $f \geq 1$ in an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-d})$ splitting B_D, and assume $\mathrm{CM}(R)$ is non-empty. Let also H_R be the ring class field of R, that is to say, the abelian extension of K unramified outside f such that $\mathrm{Gal}\,(H_R/K) \simeq \mathrm{Pic}(R)$; its degree $h(R) := [H_R : K]$ is the class number of R. Further, if $I(R)$ denotes the group of fractional invertible ideals of R, then we write $\sigma_{\mathfrak{a}} \in \mathrm{Gal}\,(H_R/K)$ for the automorphism attached to $\mathfrak{a} \in I(R)$ by the Artin symbol.

The next theorem is a particular case of [**Shi67**, Main Theorem II]:

THEOREM 1.50. *Let $P \in \mathrm{CM}(R)$, and let $\mathbb{Q}(P)$ be the number field generated by the coordinates of P. Then:*

i) *$H_R = K \cdot \mathbb{Q}(P)$.*
ii) *Let $\vartheta : K \hookrightarrow B_D$ be an R-optimal embedding such that $P = \Phi(z_\vartheta)$, and let $\mathfrak{a} \in I(R)$. There is an element $\beta \in \mathcal{O}_D$, with $\mathrm{n}(\beta) > 0$, such that $\vartheta(\mathfrak{a})\mathcal{O}_D = \beta\mathcal{O}_D$, and for any such β it holds*

$$^{\sigma_{\mathfrak{a}}}P = \Phi(\beta^{-1} z_\vartheta).$$

Statement in ii) is known as *Shimura's reciprocity law*. Besides, by i) we know that H_R is an extension of $\mathbb{Q}(P)$ of degree at most 2 (the degree is exactly 2 if and only if K is not contained in $\mathbb{Q}(P)$). The precise determination of H_R is described in Theorem 1.51 below (see [**GR06**, Section 5] for a proof, covering also the case of Shimura curves of non-trivial level), where $D(R)$ is defined as in (1.20).

THEOREM 1.51. *If $P \in \mathrm{CM}(R)$, then the following holds.*

i) *If $D(R) \neq 1$, then $H_R = \mathbb{Q}(P)$ (i.e., $K \subseteq \mathbb{Q}(P)$).*
ii) *If $D(R) = 1$, then $[H_R : \mathbb{Q}(P)] = 2$ and $\mathbb{Q}(P) \subset H_R$ is the subfield fixed by*

$$\sigma := c \cdot \sigma_{\mathfrak{a}} \in \mathrm{Gal}\,(H_R/\mathbb{Q})$$

for some $\mathfrak{a} \in I(R)$ such that $B_D \simeq \left(\frac{-d, \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a})}{\mathbb{Q}}\right)$, where c denotes the complex conjugation.

From this result, notice that if $D(R) = 1$ and $h(R)$ is either 1 or 2, then X_D admits rational points over some imaginary quadratic field. Another consequence of the previous theorem is that we can also describe the rationality of CM-points on Atkin-Lehner quotients of X_D.

Given a positive divisor $m > 1$ of D, a point $Q \in X_D^{(m)}(\bar{\mathbb{Q}})$ is said to be a CM-point if $\pi_m^{-1}(Q)$ consists of CM-points on X_D, where recall that $\pi_m : X_D \to X_D^{(m)}$ denotes the natural projection

map. As proved in [**Ogg83**, Section 1], fixed points by Atkin-Lehner involutions are CM-points, not necessarily by a maximal quadratic order:

PROPOSITION 1.52. *Let $\mathcal{F}_{\omega_m}$ be the set of fixed points on X_D of the Atkin-Lehner involution ω_m associated to a positive divisor $m > 1$ of D. Then*

$$\mathcal{F}_{\omega_m} = \begin{cases} \mathrm{CM}(\mathbb{Z}[\sqrt{-1}]) \cup \mathrm{CM}(\mathbb{Z}[\sqrt{-2}]) & \text{if } m = 2, \\ \mathrm{CM}(\mathbb{Z}[\sqrt{-m}]) \cup \mathrm{CM}(\mathbb{Z}[(1+\sqrt{-m})/2]) & \text{if } m = 3, \\ \mathrm{CM}(\mathbb{Z}[\sqrt{-m}]) & \text{otherwise.} \end{cases}$$

Finally, combining the above results one can prove the following statement about the rationality of CM points on Atkin-Lehner quotients of X_D (cf. [**GR06**, Corollary 5.14]):

PROPOSITION 1.53. *Let $P \in \mathrm{CM}(R) \subseteq X_D(\bar{\mathbb{Q}})$, and let $Q = \pi_m(P)$ be its image in $X_D^{(m)}(\bar{\mathbb{Q}})$ for some positive divisor $m > 1$ of D. Define $m' := \gcd(m, D/D(R)) = \gcd(m, \mathrm{disc}(R))$, and let $\mathfrak{b}$ be the invertible ideal of R such that $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{b}) = m'$. Then the following holds.*

i) *If $D(R) \neq 1$, then $\mathbb{Q}(Q)$ is the field*

$$\begin{cases} H_R^{\sigma_{\mathfrak{b}}} & \text{if } m/m' = 1, \\ H_R^{c\cdot\sigma_{\mathfrak{b}}\sigma_{\mathfrak{a}}} & \text{if } m/m' = D(R), \text{ for some } \mathfrak{a} \in I(R) \text{ such that } B_D \simeq (\frac{-d, \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a})}{\mathbb{Q}}), \\ H_R & \text{otherwise.} \end{cases}$$

ii) *If $D(R) = 1$, then $\mathbb{Q}(Q)$ is the field*

$$\begin{cases} H_R^{\langle c\cdot\sigma_{\mathfrak{a}}, \sigma_{\mathfrak{b}}\rangle} & \text{if } m/m' = 1, \\ H_R^{c\cdot\sigma_{\mathfrak{a}}} & \text{otherwise,} \end{cases}$$

for some $\mathfrak{a} \in I(R)$ such that $B_D \simeq (\frac{-d, \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a})}{\mathbb{Q}})$.

4. Obstructions to the existence of rational points

One of the aims of this thesis is to study the existence of points on Shimura curves and their Atkin-Lehner quotients rational over number fields, and further to show that these curves are good candidates for testing cohomological obstructions to the Hasse principle. Hence this goal can be framed in the more general problem of studying the existence of K-rational points on a variety X over a number field K (by this we mean a proper scheme over $\mathrm{Spec}(K)$).

We write $X(K)$ for the set of K-rational points on X, which scheme-theoretically is defined to be the set $\mathrm{Hom}(\mathrm{Spec}(K), X)$ of morphisms of K-schemes. If v is a place of K, then there is a natural inclusion $X(K) \hookrightarrow X(K_v)$, which plainly implies that $X(K)$ is empty whenever there is some place v of K such that $X(K_v) = \emptyset$. When the converse is also true, that is to say, when it holds that

$$X(K) \neq \emptyset \iff X(K_v) \neq \emptyset \text{ for all places } v \text{ of } K,$$

then X is said to satisfy the *Hasse principle*, or *local-global principle*. By properness, we can interpret this principle through the natural inclusion

$$X(K) \hookrightarrow X(\mathbb{A}_K) = \prod_v X(K_v)$$

of $X(K)$ into the set of adèlic points $X(\mathbb{A}_K)$ of X. This local-global principle thus represents a first obstruction to the existence of (global) rational points on varieties, in the sense that we can predict the non-existence of K-rational points on X by showing that the set $X(\mathbb{A}_K)$ is empty (i.e., that X fails to have local points at some place of K).

By a Theorem of Hasse and Minkowski ([**Ser73**, Ch. IV, Thm. 8]), the Hasse principle holds for every curve of genus zero over a number field. Equivalently, this can be rephrased by saying that a homogeneous quadratic form over a number field has a non-trivial global solution if and only if it has a local non-trivial solution at every place. However, the Hasse principle does not

hold in general, and a lot of effort has been devoted to define and explore new obstructions to the Hasse principle since the first counterexamples were discovered.

EXAMPLE 1.54. The first celebrated counterexamples to the Hasse principle over $\mathbb{Q}$ were the curve of Lind [**Lin40**] and Reichardt [**Rei42**], given by the affine equation $2y^2 = 1 - 17x^4$, and Selmer's cubic $3x^3 + 4y^3 = 5$ ([**Sel51**]). Both of these curves have rational points over $\mathbb{Q}_p$ for every rational place p (including $\mathbb{Q}_\infty = \mathbb{R}$), but fail to have $\mathbb{Q}$-rational points.

In this section we review two obstructions to the Hasse principle for a variety X over a number field K, namely the *Brauer-Manin obstruction* and the *descent obstruction*.

4.1. The Brauer-Manin obstruction. Let k be a global field. The *Brauer group* $\mathrm{Br}(k)$ of k is defined as the set of Morita-equivalence classes of finite-dimensional central simple algebras over k, with group law induced by the tensor product of k-algebras. One can also think of $\mathrm{Br}(k)$ as the set of equivalence classes of finite-dimensional central division algebras over k, and it fits into a short exact sequence

$$0 \longrightarrow \mathrm{Br}(k) \longrightarrow \bigoplus_v \mathrm{Br}(k_v) \xrightarrow{\sum \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z} \longrightarrow 0,$$

where the sum is over all the places v of k, $\mathrm{Br}(k_v)$ is the local Brauer group of k_v and

$$\mathrm{inv}_v : \mathrm{Br}(k_v) \xrightarrow{\simeq} \mathbb{Q}/\mathbb{Z} \tag{1.23}$$

is the local invariant at v (see [**Pie82**, Section 17.10]). Notice that the short exact sequence in (1.6) is the two-torsion part of the above one.

Besides, the Brauer group $\mathrm{Br}(k)$ admits a cohomological interpretation, as there is an isomorphism

$$\mathrm{Br}(k) \simeq \mathrm{H}^2(G_k, k^s) =: \mathrm{H}^2(k, \mathbb{G}_m), \tag{1.24}$$

where k^s is a separable closure of k, $G_k := \mathrm{Gal}\,(k^s/k)$ and $\mathbb{G}_m$ denotes the multiplicative group scheme; for any $\mathbb{Q}$-algebra R, $\mathbb{G}(R) = R^\times$. The interested reader may consult [**Pie82**, Chapter 14], for example, for a proof of (1.24) using crossed product algebras.

When the cohomological point of view provided by (1.24) is considered, $\mathrm{Br}(k)$ is often referred to as the *Brauer-Grothendieck group of* k. It is in this setting where invoking the machinery of étale cohomology one can easily generalise the notion of Brauer groups to arbitrary schemes.

DEFINITION 1.55. *For an arbitrary scheme X, the* Brauer group of X *is by definition the group*

$$\mathrm{Br}(X) := \mathrm{H}^2_{\text{ét}}(X, \mathbb{G}_m).$$

If R is a commutative ring, we write $\mathrm{Br}(R) := \mathrm{Br}(\mathrm{Spec}(R))$.

REMARK 1.56. If k is a global field, observe that the previous definition yields

$$\mathrm{Br}(k) = \mathrm{Br}(\mathrm{Spec}(k)) = \mathrm{H}^2_{\text{ét}}(\mathrm{Spec}(k), \mathbb{G}_m) \simeq \mathrm{H}^2(k, \mathbb{G}_m),$$

thus we recover the Galois cohomological interpretation of $\mathrm{Br}(k)$ as in (1.24).

The functoriality of $\mathrm{H}^2_{\text{ét}}$ makes Br into a contravariant functor from the category of schemes to the category of abelian groups. Hence, if $X \to Y$ is a morphism of schemes, then there is an induced group homomorphism $\mathrm{Br}(Y) \to \mathrm{Br}(X)$. If X is a regular integral noetherian scheme and $k(X)$ denotes its function field, then one can prove that the induced morphism $\mathrm{Br}(X) \to \mathrm{Br}(k(X))$ is injective. In particular, this shows that $\mathrm{Br}(X)$ is a torsion abelian group, since $\mathrm{Br}(k(X))$ is a Galois cohomology group. However, it is not true in general that the Brauer group of an arbitrary scheme is torsion.

There is a construction using Azumaya algebras on a scheme X which leads to an alternative definition $\mathrm{Br}_{Az}(X)$ of Brauer group. The group $\mathrm{Br}_{Az}(X)$ is torsion and abelian, and there is an injective group homomorphism $\mathrm{Br}_{Az}(X) \to \mathrm{Br}(X)$. Although it is not the case in general, this

homomorphism is in fact an isomorphism if X is regular and quasi-projective over $\mathrm{Spec}(R)$ for some noetherian ring.

From now on we assume for simplicity that X is a projective, smooth variety over a number field K. Assume that $x \in X(K)$ is a K-rational point on X, which we can regard as a homomorphism $x : \mathrm{Spec}(K) \to X$. By functoriality, we obtain a group homomorphism

$$\mathrm{Br}(X) \longrightarrow \mathrm{Br}(K), \quad A \longmapsto A(x).$$

If v is any place of K and $x_v \in X(K_v)$ is a local point, we can do the same and obtain a group homomorphism

$$\mathrm{Br}(X) \longrightarrow \mathrm{Br}(K_v), \quad A \longmapsto A(x_v).$$

The key point of these homomorphisms towards the study of the adèlic points on X is that given an arbitrary $(x_v)_v \in X(\mathbb{A}_K)$, it holds that $A(x_v) = 0$ for almost all places v (see [**Poo13**, Proposition 8.2.1]). This gives rise to a well-defined pairing

$$\mathrm{Br}(X) \times X(\mathbb{A}_K) \longrightarrow \mathbb{Q}/\mathbb{Z}, \qquad (A, (x_v)_v) \longmapsto \langle A, (x_v)_v \rangle := \sum_v \mathrm{inv}_v(A(x_v)), \tag{1.25}$$

where $\mathrm{inv}_v : \mathrm{Br}(K_v) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$ are the local invariants as in (1.23).

For each element $A \in \mathrm{Br}(X)$, we have a commutative diagram

$$\begin{array}{ccccccccc} & & X(K) & \longrightarrow & X(\mathbb{A}_K) & & & & \\ & & \downarrow & & \downarrow & & & & \\ 0 & \longrightarrow & \mathrm{Br}(K) & \longrightarrow & \bigoplus_v \mathrm{Br}(K_v) & \xrightarrow{\sum_v \mathrm{inv}_v} & \mathbb{Q}/\mathbb{Z} & \longrightarrow & 0, \end{array}$$

where the vertical arrows map x and $(x_v)_v$ to $A(x) \in \mathrm{Br}(K)$ and $(A(x_v))_v \in \bigoplus_v \mathrm{Br}(K_v)$, respectively. By the commutativity of the diagram, if $x \in X(K) \subseteq X(\mathbb{A}_K)$ and $(x_v)_v$ is the image of x in $X(\mathbb{A}_K)$, then $\langle A, (x_v)_v \rangle = 0$. Since A was arbitrary, we have

$$x \in X(K) \Rightarrow \langle A, (x_v)_v \rangle = 0 \text{ for every } A \in \mathrm{Br}(X).$$

This argument using the pairing (1.25) leads to the definition of the Brauer set of the K-variety X. For each element $A \in \mathrm{Br}(X)$ write

$$X(\mathbb{A}_K)^A := \{(x_v)_v \in X(\mathbb{A}_K) : \langle A, (x_v)_v \rangle = 0\} = \ker(\langle A, \cdot \rangle : X(\mathbb{A}_K) \to \mathbb{Q}/\mathbb{Z}).$$

Definition 1.57. *The* Brauer set *of X is defined to be*

$$X(\mathbb{A}_K)^{\mathrm{Br}} := \bigcap_{A \in \mathrm{Br}(X)} X(\mathbb{A}_K)^A.$$

More generally, for a subset $\mathrm{B} \subseteq \mathrm{Br}(X)$ we can define in the same way

$$X(\mathbb{A}_K)^{\mathrm{B}} := \bigcap_{A \in \mathrm{B}} X(\mathbb{A}_K)^A \supseteq X(\mathbb{A}_K)^{\mathrm{Br}}.$$

Directly from the definitions, observe that

$$X(K) \subseteq X(\mathbb{A}_K)^{\mathrm{Br}} \subseteq X(\mathbb{A}_K)^{\mathrm{B}} \subseteq X(\mathbb{A}_K)$$

for every $\mathrm{B} \subseteq \mathrm{Br}(X)$. If $X(\mathbb{A}_K)^{\mathrm{B}} = \emptyset$ for some $\mathrm{B} \subseteq \mathrm{Br}(X)$, but $X(\mathbb{A}_K) \neq \emptyset$, then we say that *there is a Brauer-Manin obstruction to the local-global principle for X*. More generally, a counterexample to the Hasse principle X over K is said to be *accounted for by the Brauer-Manin obstruction* if $X(\mathbb{A}_K)^{\mathrm{Br}} = \emptyset$.

At this point, the question of whether the Brauer-Manin obstruction is the *best* obstruction to the local-global principle that one can find naturally arises. Given a class of smooth, projective and geometrically integral varieties over K, it is said that *the Brauer-Manin obstruction to the local-global principle is the only one* if the implication

$$X(\mathbb{A}_K)^{\mathrm{Br}} \neq \emptyset \Rightarrow X(K) \neq \emptyset$$

holds for any variety X in the class. In this language, a conjecture attributed to Poonen predicts that the Brauer-Manin obstruction to the local-global principle is the only one for the class of smooth, projective and geometrically integral curves over number fields (see [**Poo06**]).

From a computational point of view, since the problem of finding obstructions to the Hasse principle is closely related to Hilbert's 10th Problem and undecidability, it is natural to wonder if it is possible to effectively compute the Brauer-Manin obstruction. In this regard, Colliot-Thélène, Kanevsky and Sansuc (see [**CT86, CTKS87**]) gave an algorithm to compute, in an effective way, the Brauer-Manin obstruction of a cubic diagonal surface over $\mathbb{Q}$. Computations with this algorithm lead them to conjecture that the Brauer-Manin obstruction should be the only one for this family of varieties. In the same direction, another conjecture attributed to Colliot-Thélène expects that this should be also the case for the class of smooth, proper, geometrically integral and rationally connected varieties over number fields (see [**PV04**, Conjecture 3.2]).

As an example of a family of varieties for which it is known that the Brauer-Manin obstruction is the only obstruction to the Hasse principle, let us mention that a theorem of Colliot-Thélène, Sansuc and Swinnerton-Dyer (see [**Sko01**, Theorem 7.2.1]) states that this is the case for the family of smooth projective models of Châtelet surfaces. In [**Sko01**, Section 7.2], Skorobogatov describes an explicit family of Châtelet surfaces over $\mathbb{Q}$ violating Hasse principle, which are variations of a previous counterexample due to Iskovskih [**Isk71**].

Despite of these conjectures, however, there are examples of varieties violating the Hasse principle for which this failure is not accounted for by the Brauer-Manin obstruction. For example, Skorobogatov constructed in [**Sko99**] a bielliptic surface X over $\mathbb{Q}$ which is a counterexample to the Hasse principle that cannot be explained by the Brauer-Manin obstruction. For this case, Skorobogatov uses étale-Brauer obstruction to explain the emptiness of $X(\mathbb{Q})$.

4.2. The descent obstruction. Let k be a field and G be an algebraic group over k, that is to say, a k-variety endowed with a group structure defined over k. We denote by $\mathbf{G}$ the algebraic group G equipped with the right action of itself by translation, and say that it is the *trivial k-torsor under G*. More generally, a *(right) k-torsor under G* (or a *principal G-homogeneous space*) is a k-variety X equipped with a right action of G such that $X_{k^s} := X \times_k k^s$ (equipped with its right G_{k^s}-action) is isomorphic to $\mathbf{G}_{k^s}$. A *morphism of k-torsors* under G is a G-equivariant morphism of k-schemes.

On the one hand, notice that if X is a k-torsor under G, then $X(k^s)$ is a transitive faithful $G(k^s)$-set, which explains why k-torsors are also called principal homogeneous spaces. On the other hand, it follows from the definitions that there is a one-to-one bijection

$$\frac{\{k\text{-torsors under } G\}}{k\text{-isomorphism}} \;\leftrightarrow\; \{\text{twists of } \mathbf{G}\}$$

between the k-isomorphism classes of k-torsors under G and the set of twists of the trivial k-torsor $\mathbf{G}$. This bijection leads to an identification

$$\frac{\{k\text{-torsors under } G\}}{k\text{-isomorphism}} \simeq \mathrm{H}^1(G_k, G(k^s)) =: \mathrm{H}^1(k, G), \tag{1.26}$$

where $\mathrm{H}^1(k, G)$ is the first Galois cohomology set of k with values in G.

Intuitively, k torsors under G are analogous to cosets of G in some larger group, or to translates of a vector subspace in some larger vector space. In order to trivialise a torsor T, one must choose a point in T to be translated back to the identity of G, but such a point might not be rational over the ground field. Indeed, the following is a standard criterion:

PROPOSITION 1.58. *Let G be an algebraic group over a field k, and let X be a k-torsor under G. Then the following are equivalent:*

i) *X is isomorphic to the trivial torsor $\mathbf{G}$,*
ii) *$X(k) \neq \emptyset$,*
iii) *X corresponds to the neutral element of $\mathrm{H}^1(k, G)$.*

The notion of k-torsor can be generalised to torsors over an arbitrary base scheme S, which in some sense can be thought of as families of k-torsors parametrised by S:

DEFINITION 1.59. *Let G be a group scheme over S, such that the structure morphism $G \to S$ is faithfully flat and locally of finite presentation (*fppf*, for short*[5]*). An S-*torsor under G *is an fppf S-scheme X equipped with a right G-action $X \times_S G \to X$ such that one of the following equivalent condition holds:*

i) *There exists an fppf base change $S' \to S$ such that $X_{S'}$ with its right $G_{S'}$-action is isomorphic over S' to $G_{S'}$ with the right-translation $G_{S'}$-action.*
ii) *The morphism*

$$X \times_S G \longrightarrow X \times_S X, \quad (x, g) \longmapsto (x, xg)$$

is an isomorphism.

From (1.26), the set of k-isomorphism classes of k-torsors under an algebraic group G over k are classified by the first Galois cohomology set $\mathrm{H}^1(k, G)$, which is identified with the first étale cohomology set $\mathrm{H}^1_{\text{ét}}(\mathrm{Spec}(k), G)$. In turn, the latter can be identified with the first fppf cohomology set $\mathrm{H}^1_{\text{fppf}}(\mathrm{Spec}(k), G)$ (cf. [**Poo13**, Chapter 6]). It is in this language of fppf cohomology that torsors under group schemes G over arbitrary base schemes S admit also a cohomological interpretation. Indeed, one needs to introduce the notion of *S-torsor sheaves under G*, which include S-torsors under G and are classified by the first pointed fppf cohomology set $\check{\mathrm{H}}^1_{\text{fppf}}(S, G)$. Under some mild conditions (see *loc. cit.*) that we may assume henceforth, there is an identification

$$\frac{\{S\text{-torsors under } G\}}{S\text{-isomorphism}} \simeq \frac{\{S\text{-torsor sheaves under } G\}}{S\text{-isomorphism}},$$

thus S-torsors under G are classified by the (pointed) cohomology set $\check{\mathrm{H}}^1_{\text{fppf}}(S, G)$.

From now on, suppose that X is a k-variety. For an affine algebraic group G over k, by an X-torsor under G we mean a right fppf X-torsor under the base extension G_X. For simplicity, write $\mathrm{H}^1(X, G)$ for the pointed cohomology set $\check{\mathrm{H}}^1_{\text{fppf}}(X, G)$.

Let $f : Z \to X$ be an X-torsor under G, and let $\zeta \in \mathrm{H}^1(X, G)$ be the corresponding cohomology class. For every k-rational point $x \in X(k)$, the fibre $Z_x \to x$ defines a k-torsor under G, and thus defines a Galois cohomology class $\zeta(x) \in \mathrm{H}^1(k, G)$. In other words, since x can be regarded as a morphism of schemes $x : \mathrm{Spec}(k) \to X$, by functoriality x defines a morphism in cohomology

$$\mathrm{H}^1(X, G) \longrightarrow \mathrm{H}^1(k, G), \quad \zeta \longmapsto \zeta(x).$$

Summing up, the torsor $f : Z \to X$ gives rise to an *evaluation map*

$$X(k) \longrightarrow \mathrm{H}^1(k, G), \quad x \longmapsto \zeta(x),$$

which makes more precise our above claim that torsors over an arbitrary base can be thought of as families of k-torsors parametrised by the base. Moreover, this evaluation map allows to describe the set $X(k)$ of k-rational points on X as a disjoint union by classifying k-rational points x according to the value of $\zeta(x)$. That is to say,

$$X(k) = \bigsqcup_{\tau \in \mathrm{H}^1(k,G)} \{x \in X(k) : \zeta(x) = \tau\}.$$

The key point of this decomposition is that each of the sets appearing in it can be interpreted in terms of *twisted torsors*:

THEOREM 1.60. *Let k be a field and X be a k-variety. Suppose that $f : Z \to X$ is an X-torsor under a smooth affine algebraic group G over k, and denote by $\zeta \in \mathrm{H}^1(X, G)$ its corresponding cohomology class. For each $\tau \in \mathrm{H}^1(k, G)$, one can define a "twisted torsor" ${}^\tau f : {}^\tau Z \to X$ such that*

$$ {}^\tau f({}^\tau Z(k)) = \{x \in X(k) : \zeta(x) = \tau\}. \tag{1.27}$$

[5]The abbreviation *fppf* is borrowed from the french terminology 'fidèlement plat et de présentation fini'.

In particular,

$$X(k) = \bigsqcup_{\tau \in \mathrm{H}^1(k,G)} {}^{\tau}f({}^{\tau}Z(k)). \tag{1.28}$$

PROOF. We sketch a proof assuming G is commutative. For the case where G is non-commutative, the construction of ${}^{\tau}Z$ is more technical and we refer the reader to [**Poo13**, Theorem 8.4.1].

Assume therefore that G is commutative. First we relate $f(Z(k))$ with the trivial element of $\mathrm{H}^1(k,G)$. By Proposition 1.58, the fibre of $f : Z \to X$ above a rational point $x \in X(k)$ contains a k-point if and only if it is trivial as a k-torsor under G, i.e. if and only if the class of the k-torsor $Z_x \to x$ is the trivial element of $\mathrm{H}^1(k,G)$. Hence,

$$\{x \in X(k) : \zeta(x) = 0\} = f(Z(k)).$$

Now, for a given $\tau \in \mathrm{H}^1(k,G)$ let $\tau_X \in \mathrm{H}^1(X,G)$ be its image under the map $\mathrm{H}^1(k,G) \to \mathrm{H}^1(X,G)$ induced by the structure morphism $X \to \mathrm{Spec}(k)$. Thus τ_X corresponds to an X-torsor "with constant fibres". Since we have assumed that G is commutative, we can consider a cocycle representing $\zeta - \tau_X \in \mathrm{H}^1(X,G)$, which gives rise to a torsor ${}^{\tau}f : {}^{\tau}Z \to X$ under G (because G is affine). Then, if $x \in X(k)$ we have $(\zeta - \tau_X)(x) = \zeta(x) - \tau$ and

$$\{x \in X(k) : \zeta(x) = \tau\} = \{x \in X(k) : \zeta(x) - \tau = 0\} = {}^{\tau}f({}^{\tau}Z(k))$$

arguing as before. Taking the union over all $\tau \in \mathrm{H}^1(k,G)$ we are done. □

From now on we assume that K is a number field, X is a K-variety, G is an affine algebraic group over K and $f : Z \to X$ is an X-torsor under G. Let also S be a finite set of places of K.

For each place v of K, fix an embedding $K \hookrightarrow K_v$. Then we obtain an induced map in fppf cohomology

$$\mathrm{H}^1(K,G) \longrightarrow \mathrm{H}^1(K_v,G), \quad \tau \longmapsto \tau_v$$

which coincides with the restriction map of Galois cohomology given by the natural inclusion

$$\mathrm{Gal}\,(\bar{K}_v/K_v) \hookrightarrow \mathrm{Gal}\,(\bar{K}/K).$$

In this situation, many of the twisted torsors ${}^{\tau}f$ do not contribute in the decomposition of the set $X(K)$ as in (1.28). The relevant cohomology classes are detected by the *Selmer set*:

DEFINITION 1.61. *The* Selmer set *of the torsor $f : Z \to X$, with respect to S, is*

$$\mathrm{Sel}_{Z,S}(K,G) := \{\tau \in \mathrm{H}^1(K,G) : {}^{\tau}Z(K_v) \neq \emptyset \text{ for all } v \notin S\} \subset \mathrm{H}^1(K,G).$$

It is clear from the definition that $\mathrm{Sel}_{Z,S}(K,G) \supseteq \{\tau \in \mathrm{H}^1(K,G) : {}^{\tau}Z(K) \neq \emptyset\}$, thus we have

$$X(K) = \bigsqcup_{\tau \in \mathrm{Sel}_{Z,S}(K,G)} {}^{\tau}f({}^{\tau}Z(K)), \tag{1.29}$$

and notice that this is true for any finite set S of places of K. The importance of the Selmer set hence follows from the next result (see [**Poo13**, Theorem 8.4.4]):

THEOREM 1.62. *If K is a number field and X is proper over K, then $\mathrm{Sel}_{Z,S}(K,G)$ is finite.*

Under our running assumptions, the set $\mathrm{Sel}_{Z,S}(K,G)$ is therefore finite, which implies that the decomposition (1.29) is in fact a finite union. This makes especially interesting the descent obstruction, which we now explain.

Recall that the set $X(\mathbb{A}_K)$ of adèlic points on X can be identified (because of properness) with $\prod_v X(K_v)$, where v runs over all the places of K, thus we can consider the diagonal embedding

$$X(K) \hookrightarrow X(\mathbb{A}_K) = \prod_v X(K_v), \quad x \longmapsto (x_v)_v.$$

The idea behind the descent obstruction is that the torsor $f : Z \to X$ imposes restrictions on the image of this embedding. More precisely, using the evaluation map the commutative diagram

$$\begin{array}{ccc} X(K) & \longrightarrow & X(\mathbb{A}_K) \\ \downarrow & & \downarrow \\ \mathrm{H}^1(K,G) & \longrightarrow & \prod_v \mathrm{H}^1(K_v,G) \end{array} \tag{1.30}$$

shows that $X(K)$ is contained in the subset of $X(\mathbb{A}_K)$ defined by

$$X(\mathbb{A}_K)^f := \left\{ (x_v)_v \in X(\mathbb{A}_K) \text{ whose image in } \prod_v \mathrm{H}^1(K_v,G) \text{ arises from } \mathrm{H}^1(K,G) \right\}.$$

Moreover, it can be shown that $X(\mathbb{A}_K)^f$ is closed in $X(\mathbb{A}_K)$ and

$$X(\mathbb{A}_K)^f = \bigcup_{\tau \in \mathrm{H}^1(K,G)} {}^\tau f({}^\tau Z(\mathbb{A}_K)) = \bigcup_{\tau \in \mathrm{Sel}_{Z,\emptyset}(K,G)} {}^\tau f({}^\tau Z(\mathbb{A}_K)), \tag{1.31}$$

By construction, it is clear that

$$X(K) \subseteq X(\mathbb{A}_K)^f \subseteq X(\mathbb{A}_K),$$

thus $X(\mathbb{A}_K)^f$ represents an obstruction for the existence of K-rational points on K, which can be finer than the local-global obstruction. If we repeat the argument for all the X-torsors under some affine algebraic group G over K, so that all the obstructions sum up, we can define

$$X(\mathbb{A}_K)^{\mathrm{descent}} := \bigcap_{\substack{G \text{ affine} \\ f:Z \to X \text{ under } G}} X(\mathbb{A}_K)^f,$$

and again by construction

$$X(K) \subseteq X(\mathbb{A}_k)^{\mathrm{descent}} \subseteq X(\mathbb{A}_K).$$

Definition 1.63. *We say that there is a* descent obstruction to the local-global principle *for* X *if* $X(\mathbb{A}_K) \neq \emptyset$ *but* $X(\mathbb{A}_K)^{\mathrm{descent}} = \emptyset$.

So far, we have introduced two (cohomological) obstructions to the existence of K-rational points on a variety X over K, namely the Brauer-Manin and the descent obstruction. These obstructions can be combined to define new obstructions, such as the *étale-Brauer* obstruction or the *étale-descent* obstruction (see [**Sko09**]). In turn, the wealth of obstructions that arise in this way can be compared among them and used to explain counterexamples to the Hasse principle. Important work in this direction has been carried out by Harari [**Har02**], Stoll [**Sto07**], Demarche [**Dem09**] and Skorobogatov [**Sko09**], among others (the interested reader may consult [**Sko01**] and [**Poo13**] for detailed expositions and further references).

We close this section with an adapted statement of the main theorem of descent theory of Colliot-Thélène and Sansuc. Suppose as usual that X is a projective, smooth variety over a number field K, and write $\overline{X}$ for the base extension $X \times_K \bar{K}$. With analogous notations, a commutative algebraic group G over K is said to be of *multiplicative type* if $\overline{G} = G \times_K \bar{K}$ is a subgroup of $\mathbb{G}_m^n$ for some integer $n \geq 1$. Then, the module of characters $\widehat{G} = \mathrm{Hom}(\overline{G}, \mathrm{Pic}(\overline{X}))$ of G is an abelian group of finite type acted on by $\mathrm{Gal}\,(\bar{K}/K)$. Indeed, the assignment $G \mapsto \widehat{G}$ gives an anti-equivalence of categories between the category of K-groups of multiplicative type and the category of continuous $\mathrm{Gal}\,(\bar{K}/K)$-modules which are of finite type as abelian groups.

It turns out that torsors under groups of multiplicative type are the nicest ones. An X-torsor under the multiplicative group $\mathbb{G}_m$ can be regarded as a line bundle over X with the zero section removed, so these objects are parametrised by $\mathrm{Pic}(X) = \mathrm{H}^1(X, \mathbb{G}_m)$. From the general theory briefly sketched above, X-torsors under a commutative group G are classified by the étale cohomology group $\mathrm{H}^1(X,G)$. And in this context, the canonical cup-pairing

$$\mathrm{H}^1(\overline{X}, \overline{G}) \times \widehat{G} \longrightarrow \mathrm{H}^1(\overline{X}, \mathbb{G}_m) = \mathrm{Pic}(\overline{X})$$

provides a map $\mathrm{H}^1(\overline{X},\overline{G}) \to \mathrm{Hom}(\widehat{G},\mathrm{Pic}(\overline{X}))$. By composing with the natural map $\mathrm{H}^1(X,G) \to \mathrm{H}^1(\overline{X},\overline{G})$ we thus obtain a map

$$\mathrm{H}^1(X,G) \longrightarrow \mathrm{Hom}_{\mathrm{Gal}\,(\bar{K}/K)}(\widehat{G},\mathrm{Pic}(\overline{X})).$$

The image of the class of a torsor $f : Y \to X$ under G by this map is called the *type* of the torsor, and we denote it by $\mathrm{type}(Y,f)$. A nice and useful description of $\mathrm{H}^1(X,G)$, for G a K-group of multiplicative type, is provided by the exact sequence of Colliot-Thélène and Sansuc, which for projective K-varieties takes the form

$$0 \to \mathrm{H}^1(K,G) \to \mathrm{H}^1(X,G) \xrightarrow{\chi} \mathrm{Hom}_{\mathrm{Gal}\,(\bar{K}/K)}(\widehat{G},\mathrm{Pic}(\overline{X})) \to \mathrm{H}^2(K,G) \to \mathrm{H}^2(X,G), \tag{1.32}$$

where χ maps the class of an X torsor under G to its type, up to sign (see [**Sko01**, Thm. 2.3.6] for details).

Finally, the *algebraic part of the Brauer group* of X is defined to be the subgroup

$$\mathrm{Br}_1(X) := \ker(\mathrm{Br}(X) \to \mathrm{Br}(\overline{X}))$$

of $\mathrm{Br}(X)$, where $\mathrm{Br}(X) \to \mathrm{Br}(\overline{X})$ is induced by the natural map $\overline{X} \to X$. Then the *algebraic Brauer set* is the subset $X(\mathbb{A}_K)^{\mathrm{Br}_1(X)}$ of $X(\mathbb{A}_K)$ cut out by the Brauer-Manin relations imposed by $\mathrm{Br}_1(X)$. In particular, we have $X(\mathbb{A}_K)^{\mathrm{Br}} \subseteq X(\mathbb{A}_K)^{\mathrm{Br}_1(X)}$.

With all these ingredients, the main theorem of descent theory of Colliot-Thélène and Sansuc ensures that the obstruction to the local-global principle defined by torsors under groups of multiplicative type coincides with the algebraic Brauer-Manin obstruction. In our setting, this result can be stated as follows (see [**Sko01**, Thm. 6.1.2] for the general statement):

THEOREM 1.64 (Colliot-Thélène and Sansuc). *Let X be a projective variety over a number field K. Then we have*

$$X(\mathbb{A}_K)^{\mathrm{Br}_1(X)} = \bigcap_{\lambda : M \hookrightarrow \mathrm{Pic}(\overline{X})} \bigcup_{type(Y,f)=\lambda} f(Y(\mathbb{A}_K)),$$

where $\lambda : M \hookrightarrow \mathrm{Pic}(\overline{X})$ runs over the $\mathrm{Gal}\,(\bar{K}/K)$-submodules of $\mathrm{Pic}(\overline{X})$ of finite type.

We want to point out two interesting remarks about this result. First, the theorem shows that the algebraic Brauer-Manin obstruction is equivalent to the combination of obstructions of two different kinds: the obstruction for the existence of torsors $f : Y \to X$ of a given type λ, and the descent obstruction defined by torsors of type λ, for all possible λ's. And secondly, by (1.32) we have that all torsors of a given type can be obtained from one such torsor by *twisting*. Hence, fixed a type λ and a torsor $f_0 : Y_0 \to X$ of type λ, the union of the sets $f(Y(\mathbb{A}_K))$ over all the torsors $f : Y \to X$ of type λ is just the union of the sets ${}^{\tau}f_0({}^{\tau}Y_0(\mathbb{A}_K))$, letting τ range over all the cohomology classes in $\mathrm{H}^1(K,G)$. Therefore, if given a torsor $f : Y \to X$ under G of a certain type, one shows that every twisted form of f (including f itself) fails to have adèlic points, then according to Theorem 1.64 it holds that $X(\mathbb{A}_K)^{\mathrm{Br}_1(X)} = \emptyset$, hence also $X(\mathbb{A}_K)^{\mathrm{Br}} = \emptyset$, and the absence of K-rational points on X is explained by the (algebraic) Brauer-Manin obstruction.

5. Admissible curves, Drinfeld's upper half plane and Mumford uniformisation

Finally, the last section of this preliminary chapter is devoted to introduce some definitions and results concerning *admissible curves* over a discrete valuation ring, and to recall how admissible curves over $\mathbb{Z}_p$ are obtained as quotients of Drinfeld's upper half plane by Schottky subgroups of $\mathrm{PGL}_2(\mathbb{Q}_p)$, after the work of Mumford.

The notions of this section will be used in Chapter 3 to study the existence of local points on certain Shimura curves at primes of bad reduction.

5.1. Admissible curves and their dual graphs. Let R be a discrete valuation ring, with perfect residue field k and uniformiser π. Let also R^{ur} be a strict henselisation of R, and $\bar{k} := R^{\mathrm{ur}}/\pi R^{\mathrm{ur}}$.

DEFINITION 1.65. *A curve C/R (that is to say, $C/\operatorname{Spec}(R)$) is called* admissible *if:*

a) *it is proper and flat over R, and its generic fibre is a non-singular curve;*
b) *its special fibre C_0/k has reduced normal crossings, and all its components are rational;*
c) *if x is a double point on C_0, there exists an integer e (uniquely determined) such that $C \times_R R^{\mathrm{ur}}$ is locally isomorphic, at x, to the scheme $\operatorname{Spec}(R^{\mathrm{ur}}[X,Y]/(XY-\pi^e))$.*

The special fibre of an admissible curve can be described using *graphs with lengths* as we now recall. A graph $\mathcal{G}$ consists of a set of vertices $\mathrm{Ver}(\mathcal{G})$ and a set of edges $\mathrm{Ed}(\mathcal{G})$. Every edge $y \in \mathrm{Ed}(\mathcal{G})$ has an *opposite* edge $\bar{y} \in \mathrm{Ed}(\mathcal{G})$, an *origin* vertex $o(y)$ and an *end* vertex $t(y)$, both in $\mathrm{Ver}(\mathcal{G})$. One has $\bar{\bar{y}} = y$ and $o(\bar{y}) = t(y)$. We allow the possibility that $y = \bar{y}$. Furthermore, $\mathcal{G}$ is a *graph with lengths* if there is a positive integer attached to each pair $\{y, \bar{y}\}$. That is, if we are given a map $\ell_{\mathcal{G}} : \mathrm{Ed}(\mathcal{G}) \to \mathbb{N} - \{0\}$ such that $\ell_{\mathcal{G}}(y) = \ell_{\mathcal{G}}(\bar{y})$. A graph $\mathcal{G}$ is easily represented by a diagram in which marked points correspond to vertices and lines joining the marked points correspond to pairs of edges $\{y, \bar{y}\}$. If $\mathcal{G}$ is a graph with lengths, every line representing a pair $\{y, \bar{y}\}$ is decorated with the integer $\ell_{\mathcal{G}}(y) = \ell_{\mathcal{G}}(\bar{y})$.

A morphism of graphs $f : \mathcal{G} \to \mathcal{G}'$ consists of a pair of maps $f_V : \mathrm{Ver}(\mathcal{G}) \to \mathrm{Ver}(\mathcal{G})$ and $f_E : \mathrm{Ed}(\mathcal{G}) \to \mathrm{Ed}(\mathcal{G}')$ such that $o(f_E(y)) = f_V(o(y))$ and $f_E(\bar{y}) = \overline{f_E(y)}$ for every $y \in \mathrm{Ed}(\mathcal{G})$. If both $\mathcal{G}$ and $\mathcal{G}'$ are graphs with lengths and f_E preserves lengths, then f is said to be a morphism of graphs with lengths. If $\mathcal{G}$ is a graph (with lengths), we denote by $\mathrm{End}(\mathcal{G})$ the set of endomorphisms of $\mathcal{G}$, that is to say, the morphisms of graphs (with lengths) from $\mathcal{G}$ to itself.

Let $f : \mathcal{G} \to \mathcal{G}'$ be a morphism of graphs with lengths, and fix two endomorphisms $F \in \mathrm{End}(\mathcal{G})$, $F' \in \mathrm{End}(\mathcal{G}')$. Then we write $f : (\mathcal{G}, F) \to (\mathcal{G}', F')$, and say that f is a morphism of pairs, if $F' \circ f = f \circ F$. When this is the case, we say f is an isomorphism of pairs if it induces an isomorphism of graphs with lengths from $\mathcal{G}$ to $\mathcal{G}'$.

DEFINITION 1.66. *Let C/R be an admissible curve, with special fibre C_0/k. The* dual graph of *C/R, which we shall denote by $\mathcal{G}(C/R)$, is defined as follows:*

i) *the vertices of $\mathcal{G}(C/R)$ are in bijection with the components of C_0;*
ii) *the edges of $\mathcal{G}(C/R)$ correspond to the branches of C_0 through each double point of C_0, so that if $y \in \mathrm{Ed}(\mathcal{G}(C/R))$ passes through the double point x, then $\bar{y}$ is the other branch of C_0 passing through x, $o(y)$ corresponds to the component of C_0 containing x and $t(y) = o(\bar{y})$.*
iii) *the length of an edge $y \in \mathrm{Ed}(\mathcal{G}(C/R))$ passing through the double point x of C_0 is the integer e from Definition 1.65, c).*

Every isomorphism $f : C/R \to C'/R$ of admissible curves induces an isomorphism of graphs with lengths $f_{\mathcal{G}} : \mathcal{G}(C/R) \to \mathcal{G}(C'/R)$. In particular, if k is finite, then the Frobenius automorphism $C_0 \times_k \bar{k} \to C_0 \times_k \bar{k}$ induces an automorphism of graphs $F(C/R) : \mathcal{G}(C/R) \to \mathcal{G}(C/R)$, which preserves lengths because the lifting of Frobenius from $\bar{k}$ to R^{ur} preserves π.

Having recalled the notions of admissible curves and their dual graphs, it will be crucial for us the fact that admissibility is preserved by base change and resolution of singularities. Furthermore, the effect of these operations in the dual graphs is rather easy to describe.

DEFINITION 1.67. *Let $\mathcal{G}$ be a graph with lengths, and $i \geq 1$ an integer. We define $\mathcal{G}^i$ to be the graph with lengths whose underlying graph is the same as $\mathcal{G}$, but whose length function is given by $\ell_{\mathcal{G}^i}(y) = i\ell_{\mathcal{G}}(y)$, for $y \in \mathrm{Ed}(\mathcal{G}^i) = \mathrm{Ed}(\mathcal{G})$. Besides, we define $\widetilde{\mathcal{G}}$ to be the graph with lengths obtained from $\mathcal{G}$ by replacing each pair $\{y, \bar{y}\}$ such that $y \neq \bar{y}$, with $y \in \mathrm{Ed}(\mathcal{G})$, by a chain of $\ell_{\mathcal{G}}(y)$ edges of trivial length.*

From the very definition, notice that there is a natural bijection between $\mathrm{End}(\mathcal{G})$ and $\mathrm{End}(\mathcal{G}^i)$. And as for $\widetilde{\mathcal{G}}$, observe on the one hand that every edge $y \in \mathrm{Ed}(\widetilde{\mathcal{G}})$ such that $y \neq \bar{y}$ has trivial length. On the other hand, there is also a natural map $\mathrm{End}(\mathcal{G}) \to \mathrm{End}(\widetilde{\mathcal{G}}), f \mapsto \tilde{f}$.

The next proposition describes the effect of base change and resolution of singularities of an admissible curve in its dual graph (cf. [**JL85**, pp. 242, 243]):

PROPOSITION 1.68. *Let C/R be an admissible curve.*

1) *Let R' be a finite discrete valuation ring extension of R, with uniformiser π' and residue field k'. Let e and f be the ramification and residual degree of R'/R, respectively, and write $C' := C \times_R R'$ for the base change and $j : C' \to C$ for the natural projection. Then C'/R' is admissible, and j induces a natural isomorphism of graphs with lengths $j_* : \mathcal{G}(C'/R') \xrightarrow{\simeq} \mathcal{G}(C/R)^e$. Further, if k is finite, then*

$$j_* : (\mathcal{G}(C'/R'), F(C'/R')) \xrightarrow{\simeq} (\mathcal{G}(C/R)^e, F(C/R)^f)$$

is an isomorphism of pairs.

2) *The curve $\widetilde{C}/R$ obtained from C/R by resolving singularities is again an admissible curve, and the canonical map $p : \widetilde{C}/R \to C/R$ induces a natural identification $p_* : \mathcal{G}(\widetilde{C}/R) \xrightarrow{\simeq} \widetilde{\mathcal{G}(C/R)}$. Further, if k is finite, then*

$$p_* : (\mathcal{G}(\widetilde{C}/R), F(\widetilde{C}/R)) \xrightarrow{\simeq} (\widetilde{\mathcal{G}(C/R)}, \widetilde{F(C/R)})$$

is an isomorphism of pairs.

Finally, we will also need that twists of admissible curves are again admissible curves. Suppose X/R is a curve and $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$ is a Galois étale cover, and let

$$\xi \in \mathrm{H}^1(\mathrm{Gal}\,(S/R), \mathrm{Aut}(X \times_R S/S))$$

be the cohomology class of a 1-cocycle $\tilde{\xi} : \mathrm{Gal}\,(S/R) \to \mathrm{Aut}(X \times_R S/S)$. Then the torsor

$$\mathscr{X}^\xi : \mathrm{Schemes}_R \longrightarrow \mathrm{Sets} \qquad \mathscr{X}^\xi(Y/R) = \sim \backslash (X \times_R S)(Y),$$

where $(x, s) \sim (1 \times \sigma)\tilde{\xi}(\sigma)(x, t)$ for every $\sigma \in \mathrm{Gal}\,(S/R)$, is represented by a unique scheme X^ξ/R, up to R-isomorphism: the so-called *twist of X/R by ξ* (cf. [**Mil80**, Ch. III, §4]). There is an S-isomorphism $X^\xi \times_R S \simeq X \times_R S$, and the set $X^\xi(R)$ of R-points of X^ξ is in bijection with the set

$$\{x \in X(S) : \tilde{\xi}(\sigma)(x) = \sigma(x) \text{ for every } \sigma \in \mathrm{Gal}\,(S/R)\}.$$

PROPOSITION 1.69. *Let C/R be an admissible curve, $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$ be a Galois étale cover and $\xi \in \mathrm{H}^1(\mathrm{Gal}\,(S/R), \mathrm{Aut}(C \times_R S/S))$ as before. Then C^ξ/R is admissible, and $\mathcal{G}(C^\xi/R) \simeq \mathcal{G}(C/R)$. Further, if k is finite and $\sigma \in \mathrm{Gal}\,(S/R)$ is a Frobenius element, then there is an isomorphism of pairs*

$$(\mathcal{G}(C^\xi/R), F(C^\xi/R)) \simeq (\mathcal{G}(C/R), \tilde{\xi}(\sigma)_{\mathcal{G}}^{-1} \circ F(C/R)).$$

5.2. Drinfeld's p-adic upper half plane and Mumford uniformisation. To close this chapter, we shortly review Drinfeld's p-adic upper half plane $\mathcal{H}_p$ in order to state Mumford's uniformisation theorem. The reader may consult [**Tei98**] for a detailed account on the geometry of $\mathcal{H}_p$, or also [**Dar03**, Section 5.1] for a brief summary, from which we borrow some notations.

Let p be a prime, and let $\mathbb{C}_p$ be the completion of an algebraic closure $\bar{\mathbb{Q}}_p$ of the field $\mathbb{Q}_p$ of p-adic numbers. We let $|\cdot|_p$ denote the p-adic norm on $\mathbb{C}_p$, normalised so that $|p|_p = p^{-1}$. The space

$$\mathcal{H}_p := \mathbb{P}^1(\mathbb{C}_p) - \mathbb{P}^1(\mathbb{Q}_p)$$

endowed with its p-adic topology has a natural structure of a rigid analytic space, and it is equipped with an action of $\mathrm{PGL}_2(\mathbb{Q}_p)$. Namely, identifying $\mathbb{P}^1(\mathbb{C}_p)$ with the $\mathbb{C}_p^\times$-homothety classes of non-zero $\mathbb{Q}_p$-linear maps from $\mathbb{Q}_p^2$ into $\mathbb{C}_p$, $\mathbb{P}^1(\mathbb{Q}_p)$ corresponds to those maps having $\mathbb{Q}_p$-rank one, thus $\mathcal{H}_p$ is identified with the collection of $\mathbb{C}_p^\times$-homothety classes of $\mathbb{Q}_p$-linear injective maps from $\mathbb{Q}_p^2$ into $\mathbb{C}_p$. If we let $\mathrm{PGL}_2(\mathbb{Q}_p)$ act naturally on $\mathbb{Q}_p^2$, we obtain an induced action of $\mathrm{PGL}_2(\mathbb{Q}_p)$ on $\mathcal{H}_p$.

The rigid analytic structure on $\mathcal{H}_p$ is defined by distinguishing the so-called *affinoid* subsets of $\mathcal{H}_p$. If $\mathrm{red} : \mathbb{P}^1(\mathbb{C}_p) \to \mathbb{P}^1(\bar{\mathbb{F}}_p)$ denotes the reduction modulo the maximal ideal of the ring of integers of $\mathbb{C}_p$, then a first example of a standard affinoid is the set

$$\mathcal{A} := \mathrm{red}^{-1}(\mathbb{P}^1(\bar{\mathbb{F}}_p) - \mathbb{P}^1(\mathbb{F}_p)) = \{\tau \in \mathcal{H}_p : |\tau - t|_p \geq 1 \text{ for } t = 0, \ldots, p-1, |\tau|_p \geq 1\} \subset \mathcal{H}_p.$$

This affinoid can be enlarged by adjoining the following *annuli* of $\mathcal{H}_p$:

$$W_t := \{\tau \in \mathcal{H}_p : p^{-1} < |\tau - t|_p < 1\}, \text{ for } t = 0, \ldots, p-1, \text{ and } W_\infty := \{\tau \in \mathcal{H}_p : 1 < |\tau|_p < p\}.$$

These regions give rise to more general affinoids on the p-adic upper half plane by introducing a combinatorial structure on $\mathcal{H}_p$, the *Bruhat-Tits tree*.

The Bruhat-Tits tree associated with $\mathrm{PGL}_2(\mathbb{Q}_p)$, denoted by $\mathcal{T}_p$, is a graph whose vertices are in bijection with homothety classes of $\mathbb{Z}_p$-lattices in $\mathbb{Q}_p^2$, and in which two vertices v and v' are joined by an edge if they can be represented by lattices Λ_v and $\Lambda_{v'}$ such that $p\Lambda_{v'} \subset \Lambda_v \subset \Lambda_{v'}$. This gives a symmetric relation, thus $\mathcal{T}_p$ becomes an unordered graph. Further, it is easy to see that $\mathcal{T}_p$ is indeed a tree and that all its vertices have degree $p+1$. The natural action of $\mathrm{PGL}_2(\mathbb{Q}_p)$ on the set of $\mathbb{Z}_p$-lattices of $\mathbb{Q}_p^2$ induces an action of $\mathrm{PGL}_2(\mathbb{Q}_p)$ on $\mathcal{T}_p$ by graph automorphisms.

We write $\mathrm{Ver}(\mathcal{T}_p)$ (resp. $\mathrm{Ed}(\mathcal{T}_p)$) for the set of vertices of $\mathcal{T}_p$ (resp. ordered edges). As above, by an ordered edge we mean an ordered pair of adjacent vertices $e = (v_1, v_2)$ where $v_1 = o(e)$ and $v_2 = t(e)$ are the origin and the end vertices of e, respectively. Let us denote by $v_0 \in \mathrm{Ver}(\mathcal{T}_p)$ the vertex corresponding to the standard lattice $\mathbb{Z}_p^2 \subset \mathbb{Q}_p^2$. The edges for which $t(e) = v_0$ are in one-to-one correspondence with the index p sublattices of $\mathbb{Z}_p^2$, hence they are in bijection with the set $\mathbb{P}^1(\mathbb{F}_p)$ of $\mathbb{F}_p$-rational points in $\mathbb{P}^1$. We can therefore label these edges as $e_0, e_1, \ldots, e_{p-1}, e_\infty \in \mathrm{Ed}(\mathcal{T}_p)$.

With the above notations, relative to the distinguished vertex v_0, there is a unique $\mathrm{PGL}_2(\mathbb{Q}_p)$-equivariant map

$$r : \mathcal{H}_p \longrightarrow \mathcal{T}_p \tag{1.33}$$

such that

i) $r(\tau) = v_0$ if and only if $\tau \in \mathcal{A}$,
ii) $r(\tau) = e_t$ for some $t \in \{0, 1, \ldots, p-1, \infty\}$ if and only if $\tau \in W_t$.

Because of the $\mathrm{PGL}_2(\mathbb{Q}_p)$-equivariance, notice that the preimage $\mathcal{A}_v := r^{-1}(v)$ of any vertex $v \in \mathrm{Ver}(\mathcal{T}_p)$ is therefore a translate of the standard affinoid $\mathcal{A}$. Similarly, the preimage of an arbitrary edge of $\mathcal{T}_p$ is a $\mathrm{PGL}_2(\mathbb{Q}_p)$-translate of an annulus W_t for some t. To be more precise, for any edge $e \in \mathrm{Ed}(\mathcal{T}_p)$ we write $]e[\subset \mathcal{T}_p$ for the singleton $\{e\}$, and $[e] \subset \mathcal{T}_p$ for the set $\{e, o(e), t(e)\} \subset \mathcal{T}_p$. We call $]e[$ and $[e]$ the *open* and *closed* edge attached to e, respectively, and say that the sets

$$\mathcal{A}_{[e]} := r^{-1}([e]) \quad \text{and} \quad W_{]e[} := r^{-1}(]e[)$$

are the *standard affinoid* and the *standard annulus* of $\mathcal{H}_p$ attached to e, respectively. According to the above observations, the affinoid $\mathcal{A}_{[e]}$ is the union of two $\mathrm{PGL}_2(\mathbb{Q}_p)$-translates of the standard affinoid $\mathcal{A}$ glued along the annulus $W_{]e[}$, which in turn is a translate of some standard annulus W_t. The collection of affinoids $\mathcal{A}_{[e]}$ as e varies over the edges of $\mathcal{T}_p$ defines a covering of $\mathcal{H}_p$ by standard affinoids, whose pairwise intersections are either empty or equal to $\mathcal{A}_v$ for some vertex $v \in \mathrm{Ver}(\mathcal{T}_p)$. Therefore, the incidence relations in this covering of affinoids are described by the combinatorics of $\mathcal{T}_p$.

The above properties suggest also a topology on $\mathcal{T}_p$. Namely, the one for which a subset U of $\mathcal{T}_p$ is open if for every vertex $v \in U$, the edges having v as an end vertex also belong to U. If we endow $\mathcal{T}_p$ with this topology and $\mathcal{H}_p$ with its natural p-adic topology, then the reduction map $r : \mathcal{H}_p \to \mathcal{T}_p$ is continuous. Furthermore, if $\Gamma \subseteq \mathrm{PGL}_2(\mathbb{Q}_p)$ is a discrete subgroup for which $\Gamma \setminus \mathcal{H}_p$ is compact (if this holds, we say Γ is *cocompact*), then the graph $\Gamma \setminus \mathcal{T}_p$ is finite.

Fixed an affinoid $\mathcal{A}_0$ of $\mathcal{H}_p$, a rational function having poles outside $\mathcal{A}_0$ reaches its supremum, with respect to the p-adic metric, on $\mathcal{A}_0$. Thus the space of rational functions without poles on $\mathcal{A}_0$ can be endowed with the supremum norm. This leads to the notion of *rigid analytic function*.

Indeed, a $\mathbb{C}_p$-valued function f on $\mathcal{H}_p$ is said to be *rigid analytic* if for every edge $e \in \mathrm{Ed}(\mathcal{T}_p)$, the restriction of f to the standard affinoid $\mathcal{A}_{[e]}$ attached to e is a uniform limit, with respect to the supremum norm, of rational functions on $\mathbb{P}^1(\mathbb{C}_p)$ with no poles on $\mathcal{A}_{[e]}$.

If Γ is a cocompact discrete subgroup of $\mathrm{SL}_2(\mathbb{Q}_p)$, then the quotient $\Gamma \setminus \mathcal{H}_p$ (with the natural inherited p-adic topology) is equipped with the structure of a *rigid analytic curve* over $\mathbb{Q}_p$, whose functions are the Γ-invariant rigid analytic functions on $\mathcal{H}_p$ in the above sense. By a p-adic analogue of the GAGA theorem, this curve can be identified with an algebraic curve over $\mathbb{Q}_p$, although it is not true that every curve over $\mathbb{Q}_p$ arises in this way.

In fact, Mumford [**Mum72**] constructs a formal scheme $\widehat{\mathcal{H}}_p$ over $\mathbb{Z}_p$, whose associated rigid analytic space is $\mathcal{H}_p$, endowed with a natural action of $\mathrm{PGL}_2(\mathbb{Q}_p)$. Roughly speaking, the formal scheme $\widehat{\mathcal{H}}_p$ is obtained by blowing up the (infinitely many) projective lines corresponding to the vertices of $\mathcal{T}_p$ at the intersection points, which correspond to the edges of $\mathcal{T}_p$.

For a Schottky subgroup $\Gamma \subseteq \mathrm{PGL}_2(\mathbb{Q}_p)$, one can consider the quotient $\Gamma \setminus \widehat{\mathcal{H}}_p$ in the category of formal schemes, and Mumford proves that this quotient is isomorphic to the formal completion along its closed fibre of a proper and flat scheme $\mathcal{M}_\Gamma$ over $\mathbb{Z}_p$, whose genus equals the number of generators of Γ. Further, $\mathcal{M}_\Gamma$ is a stable curve with $\mathbb{F}_p$-split degenerate special fibre. In particular, $\mathcal{M}_\Gamma/\mathbb{Z}_p$ is admissible, and its dual graph is the finite graph $\Gamma \setminus \mathcal{T}_p$ (see [**Mum72**, Theorems 3.1, 3.3]). The curve $\mathcal{M}_\Gamma/\mathbb{Z}_p$ is usually referred to as the *Mumford curve* associated with Γ, and it is also said that $\mathcal{M}_\Gamma/\mathbb{Z}_p$ is an algebraisation of $\Gamma \setminus \widehat{\mathcal{H}}_p$. Even more, Mumford proved (see [**Mum72**, Theorem 4.20]) that the converse to the above result holds true, which gives a p-adic analogue of the classic complex uniformisation theorem:

THEOREM 1.70 (Mumford). *Every stable curve over $\mathbb{Z}_p$ with non-singular generic fibre and $\mathbb{F}_p$-split degenerate closed fibre is isomorphic to $\mathcal{M}_\Gamma$ for a unique Schottky subgroup Γ of $\mathrm{PGL}_2(\mathbb{Q}_p)$.*

When $\Gamma \subseteq \mathrm{PGL}_2(\mathbb{Q}_p)$ is a discrete cocompact subgroup, but not necessarily a Schottky subgroup, the formal quotient $\Gamma \setminus \widehat{\mathcal{H}}_p$ is still algebraisable by a proper and flat scheme $\mathcal{X}_\Gamma/\mathbb{Z}_p$. Indeed, one can choose a finite index Schottky subgroup $\Gamma_1 \subseteq \Gamma$ and consider the Mumford curve $\mathcal{M}_{\Gamma_1}/\mathbb{Z}_p$ associated with Γ_1. The quotient group (Γ/Γ_1) acts effectively on $\mathcal{M}_{\Gamma_1}/\mathbb{Z}_p$, and $\mathcal{X}_\Gamma/\mathbb{Z}_p$ is the quotient of $\mathcal{M}_{\Gamma_1}/\mathbb{Z}_p$ by this action. One can prove that this construction is independent of the choice of Γ_1, and $\mathcal{X}_\Gamma/\mathbb{Z}_p$ is normal, proper and flat, with smooth generic fibre. Further, it is an admissible curve, and its special fibre is described by duality by the finite graph (with lengths) $(\Gamma \setminus \mathcal{T}_p)^*$, where the graph $(\Gamma \setminus \mathcal{T}_p)^*$ is obtained from $\Gamma \setminus \mathcal{T}_p$ by removing those edges y such that $\bar{y} = y$ (see [**Kur79**] for further details, especially Proposition 3-2).

In its simplest form, for example, the Theorem of Čerednik and Drinfeld states that for a prime p dividing D, the Shimura curve X_D is p-adically uniformised by $\mathcal{H}_p$. More precisely, due to its moduli interpretation X_D admits a proper and flat model over $\mathbb{Z}$ extending the moduli interpretation to arbitrary schemes over $\mathbb{Z}$, which is smooth over $\mathbb{Z}[1/D]$. Hence by base change we obtain a model $\mathcal{X}_D/\mathbb{Z}_p$ of $X_D \times_{\mathbb{Q}} \mathbb{Q}_p$. Then the Theorem of Čerednik and Drinfeld asserts that $\mathcal{X}_D/\mathbb{Z}_p$ is isomorphic, up to a quadratic twist, to a Mumford curve over $\mathbb{Z}_p$. We will review Čerednik-Drinfeld theory in more generality and detail in Section 2.1 of Chapter 3. The important breakthrough of the work of Drinfeld was to give an interpretation of the formal scheme $\widehat{\mathcal{H}}_p$ as a moduli space for special formal $\mathcal{O}_{D,p}$-modules. This way, the approach of Drinfeld gives a more conceptual proof of Čerednik's original result on the uniformisation of Shimura curves.

CHAPTER 2

Shimura coverings of a Shimura curve

As quoted in the Introduction, after the celebrated work of Mazur in [**Maz77**], and the subsequent progress made by Kenku [**Ken81**], Momose [**Mom84, Mom87**], Clark [**Cla09**], Bruin-Flynn-Gonzàlez-Rotger [**BFGR06**], Bilu-Parent [**BP11**] and many others, the general philosophy is that rational points on (modular and) Shimura curves should correspond only to (cusps or) fake elliptic curves, except for a few exceptional cases. One useful strategy to investigate the set of rational points on Shimura curves is to apply descent to suitable étale coverings of them. The question of the existence of rational points is then transferred to these coverings and their twists, and one hopes this problem to have a simpler resolution. Therefore, the knowledge of étale coverings of Shimura curves is a necessary requirement to use the machinery of descent in order to tackle the existence or non-existence of rational points on them.

Motivated by this philosophy, the main goal of this chapter is to determine the group of modular automorphisms of a cyclic Galois covering of Shimura curves $X_{D,\ell} \to X_D$ associated to an odd prime divisor ℓ of D. As an application, we construct cyclic étale Galois coverings of Atkin-Lehner quotients of X_D, which can be used to study the existence of rational points over number fields on these curves (see Chapter 5).

More precisely, let $X_D/\mathbb{Q}$ be the Shimura curve associated to a maximal order $\mathcal{O}_D$ in an indefinite rational quaternion algebra B_D of reduced discriminant $D > 1$. Fix an odd prime ℓ dividing D, and let $I_\ell \subseteq \mathcal{O}_{D,\ell} := \mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ be the unique two-sided $\mathcal{O}_{D,\ell}$-ideal of reduced norm $\ell\mathbb{Z}_\ell$ (that is, the unique maximal ideal of $\mathcal{O}_{D,\ell}$). Then define $\mathcal{U}_D \subseteq \widehat{\mathcal{O}}_D^\times$ to be the open compact subgroup of $\widehat{\mathcal{O}}_D^\times$ consisting of all the elements in $\widehat{\mathcal{O}}_D^\times$ that locally at ℓ are congruent to 1 modulo I_ℓ, and write $X_{D,\ell}$ for the canonical model over $\mathbb{Q}$ of the curve $X_{\mathcal{U}_D}$ defined as in Chapter 1. This Shimura curve has appeared a few times in the literature, with applications to the study of rational points on X_D over number fields (see, e.g., [**Jor81**], [**Sko05**]).

The curve $X_{D,\ell} \times_{\mathbb{Q}} \mathbb{Q}(\mu_\ell)$ is the disjoint union of $\ell - 1$ irreducible curves which are conjugate by the action of $\mathrm{Gal}\,(\mathbb{Q}(\mu_\ell)/\mathbb{Q})$ (see Section 1 below), and the natural finite flat morphism

$$X_{D,\ell} \longrightarrow X_D$$

induced by the inclusion $\mathcal{U}_D \subseteq \widehat{\mathcal{O}}_D^\times$ is a Galois covering whose automorphism group

$$\Delta := \mathrm{Aut}(X_{D,\ell}/X_D)$$

is isomorphic to the cyclic group $\mathbb{F}_{\ell^2}^\times/\{\pm 1\} \simeq \mathbb{Z}/\frac{\ell^2-1}{2}\mathbb{Z}$.

Besides, we prove in Section 3 that the Atkin-Lehner involutions $\omega_m \in W_D$ on X_D can be lifted to involutions $\hat{\omega}_m$ on the curve $X_{D,\ell}$. As it happens for the ω_m, these involutions commute one to each other, so that they form an abelian subgroup $W_{D,\ell} \simeq (\mathbb{Z}/2\mathbb{Z})^{2r}$ of $\mathrm{Aut}(X_{D,\ell})$. Both Δ and $W_{D,\ell}$ are in fact subgroups of $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$, and we prove in Section 4 that one actually has $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell}) = \Delta W_{D,\ell}$. More precisely, the first main result of this chapter can be summarised as follows:

THEOREM 2.1. *Let X_D and $X_{D,\ell}$ be as above.*

(1) *The Atkin-Lehner involutions $\omega_m \in W_D$ on X_D lift to involutions $\hat{\omega}_m$ on the curve $X_{D,\ell}$. The group $W_{D,\ell}$ generated by them is naturally a subgroup of* $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$*, and* $W_{D,\ell} \simeq (\mathbb{Z}/2\mathbb{Z})^{2r}$.

(2) *Write* $W_{D/\ell,\ell} \simeq (\mathbb{Z}/2\mathbb{Z})^{2r-1}$ *for the subgroup of* $W_{D,\ell}$ *generated by the involutions* $\hat{\omega}_m$ *associated with positive divisors* m *of* D/ℓ. *Then the group* $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ *is isomorphic to*

$$(\Delta \rtimes \langle \hat{\omega}_\ell \rangle) \times W_{D/\ell,\ell} \simeq \left(\mathbb{F}_{\ell^2}^\times/\{\pm 1\} \rtimes \mathbb{Z}/2\mathbb{Z}\right) \times (\mathbb{Z}/2\mathbb{Z})^{2r-1},$$

where $\hat{\omega}_\ell \cdot \delta \cdot \hat{\omega}_\ell = \delta^\ell$ *for any* $\delta \in \Delta$.

We leave open the question of studying whether the group $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ of modular automorphisms of $X_{D,\ell}$ is the full group $\mathrm{Aut}(X_{D,\ell})$ or not.

In his PhD thesis [**Jor81**, Chapter 5], Jordan showed that the maximal étale quotient of the covering $g : X_{D,\ell} \to X_D$ has degree $d_{\text{ét}} := (\ell^2-1)/2e$, where $e = e(D)$ is a positive integer dividing 6 which depends on the arithmetic of B_D (see (2.14) below for its definition). In Section 5 we apply Theorem 2.1 to investigate sufficient conditions for the natural map $g^{(m)} : X_{D,\ell}^{(m)} \to X_D^{(m)}$ induced by g to factor through a cyclic étale Galois covering of the Atkin-Lehner quotient $X_D^{(m)}$, where we write $X_{D,\ell}^{(m)} := X_{D,\ell}/\langle \hat{\omega}_m \rangle$ and $X_D^{(m)} := X_D/\langle \omega_m \rangle$ for the quotients of $X_{D,\ell}$ and X_D by the action of $\hat{\omega}_m$ and ω_m, respectively. In this direction, the second main result of this chapter is the following (cf. Theorem 2.21):

THEOREM 2.2. *Let* d *be a positive integer dividing* $(\ell^2-1)/2n$, *where*

$$n := \begin{cases} e & \text{if } \ell \nmid m, \\ \mathrm{lcm}(e, (\ell+1)/2) & \text{if } \ell \mid m. \end{cases}$$

The map $g^{(m)} : X_{D,\ell}^{(m)} \to X_D^{(m)}$ *factors through a cyclic étale Galois covering of degree* d *of* $X_D^{(m)}$ *if either of the following conditions holds:*

(i) ω_m *is fixed point free,*
(ii) $\ell \nmid m$, $(\frac{m}{\ell}) = 1$ *and* d *divides* $\ell - 1$,
(iii) $\ell \mid m$ *and* $(\frac{m/\ell}{\ell}) = -1$, *or*
(iv) d *divides* $(\ell^2-1)/4n$.

When the Atkin-Lehner involution ω_m is fixed point free, descent techniques were applied to the natural $X_D^{(m)}$-torsor $X_D \to X_D^{(m)}$ under the constant group scheme $\mathbb{Z}/2\mathbb{Z}$ in [**RSY05**] to prove the emptiness of $X_D^{(m)}(\mathbb{Q})$ in some cases. In Chapter 5 we show that the étale coverings of $X_D^{(m)}$ arising from the above theorem are also useful in the study of rational points on $X_D^{(m)}$.

1. The Shimura curve $X_{D,\ell}$

Fix for the rest of the chapter an indefinite rational quaternion algebra B_D of reduced discriminant $D > 1$ and a maximal order $\mathcal{O}_D \subseteq B_D$ as above. Write $D = p_1 \cdots p_{2r}$, where the p_i are pairwise distinct primes and $r \geq 1$. For every prime p_i dividing D, the local maximal order $\mathcal{O}_{D,p_i} := \mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{Z}_{p_i}$ will be regarded as a matrix ring after the choice of an isomorphism

$$\psi_{p_i} : \mathcal{O}_{D,p_i} \xrightarrow{\simeq} \left\{ \begin{pmatrix} x & y \\ p_i\,{}^\sigma y & {}^\sigma x \end{pmatrix} : x, y \in \mathbb{Z}_{p_i^2} \right\} \subseteq \mathrm{M}_2(\mathbb{Z}_{p_i^2}), \tag{2.1}$$

where $\mathbb{Z}_{p_i^2}$ is the ring of integers of the unique unramified quadratic extension $\mathbb{Q}_{p_i^2}$ of $\mathbb{Q}_{p_i}$ and $\sigma \in \mathrm{Gal}\,(\mathbb{Q}_{p_i^2}/\mathbb{Q}_{p_i})$ is the non-trivial automorphism (cf. (1.5)).

Fix also an odd prime ℓ dividing D, and consider the canonical model $X_{D,\ell}/\mathbb{Q}$ of the Shimura curve $X_{\mathcal{U}_D}$. As quoted above, the compact subgroup $\mathcal{U}_D \subseteq \widehat{\mathcal{O}}_D^\times$ is defined locally as

$$\mathcal{U}_D = \prod_v \mathcal{U}_{D,v}, \quad \text{where } \mathcal{U}_{D,v} := \begin{cases} \mathcal{O}_{D,v}^\times & \text{if } v \neq \ell, \\ 1 + I_\ell & \text{if } v = \ell. \end{cases} \tag{2.2}$$

Using the isomorphism ψ_ℓ, we make the identification

$$I_\ell = \left\{ \begin{pmatrix} \ell x & y \\ \ell\,{}^\sigma y & \ell\,{}^\sigma x \end{pmatrix} : x, y \in \mathbb{Z}_{\ell^2} \right\} \subseteq \mathcal{O}_{D,\ell}. \tag{2.3}$$

This section is devoted to studying the geometry of the Shimura curve $X_{D,\ell}$, and we start this task by describing the connected components of the complex curve $X_{D,\ell}\times_{\mathbb{Q}}\mathbb{C}$. In order to do so, we proceed as in Section 3.1 of Chapter 1. Recall that the set $\pi_0(X_{D,\ell}\times_{\mathbb{Q}}\mathbb{C})$ of geometric connected components of $X_{D,\ell}$ is in bijection with the set

$$\mathcal{C}_\infty(D,\ell):=\mathcal{C}_\infty(\mathcal{U}_D)=B_{D,+}^\times\setminus(B_D\otimes_{\mathbb{Q}}\mathbb{A}_f)^\times/\mathcal{U}_D.$$

Taking into account that $\mathrm{n}((B_D\otimes_{\mathbb{Q}}\mathbb{A}_f)^\times)=\mathbb{A}_f^\times$ and $\mathrm{n}(B_{D,+}^\times)=\mathbb{Q}^{>0}$ because B_D is indefinite (see Theorem 1.26), the reduced norm induces an isomorphism

$$\mathcal{C}_\infty(D,\ell)\ \xrightarrow{\simeq}\ \mathbb{Q}^{>0}\setminus\mathbb{A}_f^\times/\mathrm{n}(\mathcal{U}_D)\simeq\mathbb{Z}_\ell^\times/\mathrm{n}(1+I_\ell),$$

where the second isomorphism holds because $\mathcal{U}_D$ is maximal outside ℓ. Finally:

LEMMA 2.3. $\mathrm{n}(1+I_\ell)=1+\ell\mathbb{Z}_\ell$.

PROOF. If $x\in I_\ell$, then

$$n(1+x)=(1+x)(1+\bar{x})=1+\mathrm{tr}(x)+\mathrm{n}(x)\in 1+\ell\mathbb{Z}_\ell,$$

since from (2.3) we see that *both* the trace and the norm of elements in I_ℓ are divisible by ℓ. This shows that $\mathrm{n}(1+I_\ell)\subseteq 1+\ell\mathbb{Z}_\ell$.

But observe that $\ell\mathbb{Z}_{\ell^2}\subseteq I_\ell$, hence

$$\mathrm{n}(1+I_\ell)\supseteq\mathrm{n}(1+\ell\mathbb{Z}_{\ell^2})=N(1+\ell\mathbb{Z}_{\ell^2}),$$

where $N:\mathbb{Z}_{\ell^2}\to\mathbb{Z}_\ell$ is induced by the norm map $N_{\mathbb{Q}_{\ell^2}/\mathbb{Q}_\ell}:\mathbb{Q}_{\ell^2}\to\mathbb{Q}_\ell$. Since $N(1+\ell\mathbb{Z}_{\ell^2})=1+\ell\mathbb{Z}_\ell$ (see [**Ser79**, §V.2]), the lemma follows. □

Hence the set $\mathcal{C}_\infty(D,\ell)$ is isomorphic to $\mathbb{F}_\ell^\times$, and the natural projection

$$\mathrm{pr}_{\mathcal{U}_D}:X_{D,\ell}\times_{\mathbb{Q}}\mathbb{C}\longrightarrow\mathcal{C}_\infty(D,\ell)$$

induces a decomposition of $X_{D,\ell}\times_{\mathbb{Q}}\mathbb{C}$ as a disjoint union of its $\ell-1=|\mathbb{F}_\ell^\times|$ connected components. Indeed, the stabiliser of each class $[c]\in\mathcal{C}_\infty(D,\ell)$, represented by some $c\in(B_D\otimes_{\mathbb{Q}}\mathbb{A}_f)^\times$, is easily seen to be

$$\Gamma_c:=B_{D,+}^\times\cap c\mathcal{U}_Dc^{-1}.$$

Under our fixed isomorphism Ψ between $B_D\otimes_{\mathbb{Q}}\mathbb{R}$ and $\mathrm{M}_2(\mathbb{R})$, the groups Γ_c must be regarded as subgroups of $\mathrm{GL}_2^+(\mathbb{R})$. In particular, they act by linear fractional transformations on $\mathcal{H}$, and $\mathrm{pr}_{\mathcal{U}_D}$ gives rise to a decomposition of the form

$$X_{D,\ell}\times_{\mathbb{Q}}\mathbb{C}\simeq\bigsqcup_{[c]\in\mathcal{C}_\infty(D,\ell)}\Gamma_c\setminus\mathcal{H}. \tag{2.4}$$

Now it is easy to check that the complex compact Riemann surfaces $\Gamma_c\setminus\mathcal{H}$ appearing in this decomposition are all isomorphic one to each other. Actually, under the natural inclusion $\mathcal{O}_D^1\hookrightarrow\mathcal{O}_{D,\ell}^\times$, we can regard

$$\Gamma_{D,\ell}:=\mathcal{O}_D^1\cap(1+I_\ell)$$

as a subgroup of $\mathcal{O}_D^1$, acting by conformal transformations on $\mathcal{H}$. Then our claim is proved in the following lemma:

LEMMA 2.4. *Every connected component of $X_{D,\ell}\times_{\mathbb{Q}}\mathbb{C}$ is isomorphic to the compact Riemann surface*

$$V_{D,\ell}:=\Gamma_{D,\ell}\setminus\mathcal{H}.$$

PROOF. As before, we may choose a representative $c=(c_v)_v\in(B_D\otimes_{\mathbb{Q}}\mathbb{A}_f)^\times$ for each class $[c]\in\mathcal{C}_\infty(D,\ell)$. We can further assume that $c_v=1$ for all the primes $v\neq\ell$, thus $c=(1,\dots,1,c_\ell,1,\dots)$ for some $c_\ell\in B_{D,\ell}^\times$.

Since ℓ divides D, the maximal order $\mathcal{O}_{D,\ell}\subseteq B_{D,\ell}$ in the local quaternion division algebra $B_{D,\ell}$ is unique, and consists of *all* the integral elements in $B_{D,\ell}$ (see Theorem 1.19). In particular, $c_\ell\mathcal{O}_{D,\ell}c_\ell^{-1}=\mathcal{O}_{D,\ell}$. Besides, the two-sided $\mathcal{O}_{D,\ell}$-ideal I_ℓ consists of all the integral elements whose

reduced norm is divisible by ℓ, that is $I_\ell = \{\gamma \in \mathcal{O}_{D,\ell} : \mathrm{n}(\gamma) \in \ell\mathbb{Z}_\ell\}$. Since the reduced norm is invariant under conjugation, we deduce that $c_\ell I_\ell c_\ell^{-1} = I_\ell$. It follows that $c_\ell(1+I_\ell)c_\ell^{-1} = 1 + I_\ell$, hence also $c\mathcal{U}_D c^{-1} = \mathcal{U}_D$. This is independent on the choice of $[c]$, thus all the connected components of $X_{D,\ell}$ are isomorphic to

$$(B_{D,+}^\times \cap \mathcal{U}_D) \setminus \mathcal{H},$$

and the statement follows by observing that $B_{D,+}^\times \cap \mathcal{U}_D = \mathcal{O}_D^1 \cap (1 + I_\ell)$. □

Hence, the complex curve $X_{D,\ell} \times_{\mathbb{Q}} \mathbb{C}$ is the disjoint union of $\ell - 1$ compact connected curves, and each of them is isomorphic to the Riemann surface $V_{D,\ell} = \Gamma_{D,\ell} \setminus \mathcal{H}$.

From an arithmetic point of view, even though the curve $X_{D,\ell}$ is defined over $\mathbb{Q}$, its geometric connected components are only defined over $\mathbb{Q}(\mu_\ell)$. This follows again by proceeding as in Section 3.1 of Chapter 1. Indeed, the choice of $X_{D,\ell}$ as a model of $X_{\mathcal{U}_D}$ over $\mathbb{Q}$ defines an action of $\mathrm{Aut}(\mathbb{C})$ on $X_{\mathcal{U}_D}(\mathbb{C})$, which is compatible with the action of $\mathrm{Aut}(\mathbb{C})$ on the set of connected components

$$\mathcal{C}_\infty(D,\ell) \xrightarrow{\sim} B_{D,+}^\times \setminus (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times / \mathcal{U}_D \simeq \mathbb{Q}^{>0} \setminus \mathbb{A}_f^\times / \mathrm{n}(\mathcal{U}_D) \simeq \widehat{\mathbb{Z}}^\times / \mathrm{n}(\mathcal{U}_D)$$

of $X_{D,\ell} \times_{\mathbb{Q}} \mathbb{C}$ through its quotient $\mathrm{Gal}\,(\mathbb{Q}^{ab}/\mathbb{Q}) \simeq \widehat{\mathbb{Z}}^\times$ under the map

$$\begin{array}{rcl} X_{D,\ell} \times_{\mathbb{Q}} \mathbb{C} \simeq B_{D,+}^\times \setminus \mathcal{H} \times (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times / \mathcal{U}_D & \longrightarrow & \mathbb{Q}^{>0} \setminus \mathbb{A}_f^\times / \mathrm{n}(\mathcal{U}_D) \simeq \widehat{\mathbb{Z}}^\times / \mathrm{n}(\mathcal{U}_D) \\ [z,b] & \longmapsto & [\mathrm{n}(b)]. \end{array}$$

Using the previous notation, if we represent a connected component $[c] \in \mathcal{C}_\infty(D,\ell)$ by an element $c \in (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$, then the open subgroup $U_c \subseteq \widehat{\mathbb{Z}}^\times$ fixing $[\mathrm{n}(c)] \in \widehat{\mathbb{Z}}/\mathrm{n}(\mathcal{U}_D)$ is easily seen to be

$$U_c = \prod_{v \neq \ell} \mathbb{Z}_v^\times \times (1 + \ell\mathbb{Z}_\ell),$$

thus the number field contained in $\mathbb{Q}^{ab}$ fixed by the action of U_c on $\mathbb{Q}^{ab}$ is the ℓ-th cyclotomic field $\mathbb{Q}(\mu_\ell)$. From this we deduce that every geometric connected component of $X_{D,\ell}$ is defined over $\mathbb{Q}(\mu_\ell)$.

Summing up, the curve $X_{D,\ell} \times_{\mathbb{Q}} \mathbb{Q}(\mu_\ell)$ is the disjoint union of $\ell - 1$ geometrically connected curves defined over $\mathbb{Q}(\mu_\ell)$. These connected components are conjugated by the action of $\mathrm{Gal}\,(\mathbb{Q}(\mu_\ell)/\mathbb{Q})$ (this action being free and transitive), and all of them become isomorphic to the Riemann surface $V_{D,\ell}$ as complex curves.

2. The cyclic Galois covering $X_{D,\ell} \to X_D$

Once we have described the geometry of the curve $X_{D,\ell}$, next we study the natural covering of Shimura curves $X_{D,\ell} \to X_D$ induced by the inclusion $\mathcal{U}_D \subseteq \widehat{\mathcal{O}}_D^\times$. Since $\mathcal{U}_D$ is a normal subgroup of $\widehat{\mathcal{O}}_D^\times$, it is a Galois covering, and we can regard the Shimura curve $X_{\widehat{\mathcal{O}}_D^\times}$ as the quotient of $X_{\mathcal{U}_D}$ by the action of $\widehat{\mathcal{O}}_D^\times$. This means that every automorphism of the covering

$$X_{\mathcal{U}_D} = X_{D,\ell} \times_{\mathbb{Q}} \mathbb{C} \longrightarrow X_{\widehat{\mathcal{O}}_D^\times} = X_D \times_{\mathbb{Q}} \mathbb{C}$$

is of the form $\rho_{\mathcal{U}_D}(\alpha)$ for some $\alpha \in \widehat{\mathcal{O}}_D^\times$. Moreover, after the choice of canonical models $X_{D,\ell}$ and X_D over $\mathbb{Q}$ for the curves $X_{\mathcal{U}_D}$ and $X_{\widehat{\mathcal{O}}_D^\times}$, respectively, all these (modular) automorphisms are defined over $\mathbb{Q}$ (cf. Definition 1.35). Hence,

$$\mathrm{Aut}(X_{D,\ell}/X_D) := \mathrm{Aut}_{\mathbb{Q}}(X_{D,\ell}/X_D) = \mathrm{Aut}(X_{D,\ell} \times_{\mathbb{Q}} \mathbb{C}/X_D \times_{\mathbb{Q}} \mathbb{C})$$

and there is a surjective homomorphism

$$\begin{array}{rcl} \widehat{\mathcal{O}}_D^\times & \longrightarrow & \mathrm{Aut}(X_{D,\ell}/X_D) \\ \alpha & \longmapsto & \rho_{\mathcal{U}_D}(\alpha), \end{array}$$

whose kernel clearly contains the normal subgroup $\mathcal{U}_D \subseteq \widehat{\mathcal{O}}_D^\times$. Thus we have in fact a surjective homomorphism

$$\begin{aligned} \widehat{\mathcal{O}}_D^\times/\mathcal{U}_D \simeq \mathcal{O}_{D,\ell}^\times/(1+I_\ell) &\longrightarrow \mathrm{Aut}(X_{D,\ell}/X_D) \\ \alpha_\ell(1+I_\ell) &\longmapsto \rho_{\mathcal{U}_D}(\alpha_\ell) = \rho_{\mathcal{U}_D}(1,\dots,1,\alpha_\ell,1,\dots). \end{aligned}$$

Because of our assumption of ℓ being odd, $-1 \notin 1+I_\ell$ and the kernel of this last homomorphism is $\{\pm 1\}$, so that

$$\mathrm{Aut}(X_{D,\ell}/X_D) \simeq (\mathcal{O}_{D,\ell}^\times/(1+I_\ell))/\{\pm 1\}. \tag{2.5}$$

Definition 2.5. *We denote by* Δ *the* group of covering automorphisms $\mathrm{Aut}(X_{D,\ell}/X_D)$*, regarded as a subgroup of* $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$*. The elements of* Δ *will be called* diamond automorphisms*.*

As explained in [**Sko05**], the covering $X_{D,\ell} \to X_D$ is Galois and cyclic of degree $(\ell^2-1)/2$, so $\Delta \simeq \mathbb{F}_{\ell^2}^\times/\{\pm 1\}$, but for our purposes we shall study here the group Δ in more detail. Similarly as in [**Jor81**, Chapter 5], we start by defining the *Nebentypus character of* $\mathcal{O}_D$ *at* ℓ as the homomorphism

$$\varepsilon_\ell : \mathcal{O}_{D,\ell}^\times \longrightarrow \mathbb{F}_{\ell^2}^\times \tag{2.6}$$

given by the rule

$$\varepsilon_\ell(\gamma) = x \bmod \ell\mathbb{Z}_{\ell^2} \in \mathbb{F}_{\ell^2}^\times \quad \text{if} \quad \psi_\ell(\gamma) = \begin{pmatrix} x & y \\ \ell\,\sigma_y & \sigma_x \end{pmatrix} \quad \text{for some } x, y \in \mathbb{Z}_{\ell^2}.$$

The homomorphism ε_ℓ is clearly surjective, and its kernel is $1+I_\ell$. Therefore:

Lemma 2.6. *The quotient* $\mathcal{O}_{D,\ell}^\times/(1+I_\ell)$ *is isomorphic to* $\mathbb{F}_{\ell^2}^\times$*.*

In fact, every equivalence coset in $\mathcal{O}_{D,\ell}^\times/(1+I_\ell)$ is represented by an element of the form

$$\begin{pmatrix} x & 0 \\ 0 & \sigma_x \end{pmatrix} \in \mathcal{O}_{D,\ell}^\times$$

with $x \in \mathbb{Z}_{\ell^2}^\times$ uniquely determined modulo $\ell\mathbb{Z}_{\ell^2}$. Combining Lemma 2.6 with the isomorphism in (2.5), we obtain as claimed that

$$\Delta = \mathrm{Aut}(X_{D,\ell}/X_D) \simeq \mathbb{F}_{\ell^2}^\times/\{\pm 1\}.$$

In order to understand in detail the action of Δ on the Shimura curve $X_{D,\ell}$, we shall now exploit that $X_{D,\ell} \times_{\mathbb{Q}} \mathbb{C}$ is the disjoint union of $\ell-1$ copies of the Riemann surface $V_{D,\ell}$. In fact, every connected component of $X_{D,\ell} \times_{\mathbb{Q}} \mathbb{C}$ defines a covering

$$V_{D,\ell} \longrightarrow \mathcal{O}_D^1 \setminus \mathcal{H} \simeq X_D \times_{\mathbb{Q}} \mathbb{C}$$

of complex algebraic curves (equivalently, of Riemann surfaces), and the automorphism group of this covering can be identified as a subgroup of $\Delta \simeq \mathbb{F}_{\ell^2}^\times/\{\pm 1\}$ as follows. First of all, by the very definition of $\Gamma_{D,\ell}$ the natural inclusion of $\mathcal{O}_D^1$ in $\mathcal{O}_{D,\ell}^\times$ identifies $\mathcal{O}_D^1/\Gamma_{D,\ell}$ as a subgroup of $\mathcal{O}_{D,\ell}^\times/(1+I_\ell)$. Secondly, the restriction of the Nebentypus character of $\mathcal{O}_D$ at ℓ to $\mathcal{O}_D^1$ has kernel $\Gamma_{D,\ell} = \mathcal{O}_D^1 \cap (1+I_\ell)$, but it is no longer surjective[1] onto $\mathbb{F}_{\ell^2}^\times$:

Lemma 2.7. *The image of* $\mathcal{O}_D^1$ *under the Nebentypus character* ε_ℓ *is*

$$\mathbb{F}_{\ell^2}^1 := \ker(N_{\mathbb{F}_{\ell^2}/\mathbb{F}_\ell} : \mathbb{F}_{\ell^2}^\times \to \mathbb{F}_\ell^\times) = \{\bar{x} \in \mathbb{F}_{\ell^2}^\times : \bar{x}^{\ell+1} = 1\} \subseteq \mathbb{F}_{\ell^2}^\times,$$

the unique subgroup of order $\ell+1$ *of* $\mathbb{F}_{\ell^2}^\times$*. In particular,*

$$\mathcal{O}_D^1/\Gamma_{D,\ell} = \mathcal{O}_D^1/(\mathcal{O}_D^1 \cap (1+I_\ell)) \simeq \mathbb{F}_{\ell^2}^1.$$

[1]There is a mistake in [**Jor81**, p. 109], where it is implicitly stated that the restriction of ε_ℓ to $\mathcal{O}_D^1$ is still surjective, which in view of Lemma 2.7 is not true.

PROOF. Let $\gamma \in \mathcal{O}_D^1$. Under the natural inclusion $\mathcal{O}_D^1 \subseteq \mathcal{O}_{D,\ell}^\times$ and using the isomorphism ψ_ℓ, we can write $\gamma = \begin{pmatrix} x & y \\ \ell\,{}^\sigma y & {}^\sigma x \end{pmatrix}$ for some $x, y \in \mathbb{Z}_{\ell^2}$ such that $x^\sigma x - \ell y^\sigma y = 1$. In particular, if $\bar{x} \in \mathbb{F}_{\ell^2}^\times$ denotes the reduction of x modulo $\ell\mathbb{Z}_{\ell^2}$, then

$$\bar{x}^{\ell+1} = x^\sigma x \mod \ell\mathbb{Z}_{\ell^2} = x^\sigma x - \ell y^\sigma y \mod \ell\mathbb{Z}_{\ell^2} = 1 \in \mathbb{F}_{\ell^2}^\times.$$

In other words, $\varepsilon_\ell(\gamma) = \bar{x} \in \mathbb{F}_{\ell^2}^1$.

Conversely, let $\bar{x} \in \mathbb{F}_{\ell^2}^1 \subseteq \mathbb{F}_{\ell^2}^\times$, and let $x \in \mathbb{Z}_{\ell^2}^\times$ be any representative of $\bar{x}$. Since $\bar{x} \in \mathbb{F}_{\ell^2}^1$, we have

$$x^\sigma x = 1 + \ell a, \quad \text{for some } a \in \mathbb{Z}_{\ell^2}.$$

Actually, $a \in \mathbb{Z}_\ell$ because $x^\sigma x \in \mathbb{Z}_\ell$, and we claim that we can assume $a \in \mathbb{Z}_\ell^\times$. If not, ℓ divides a, and replacing x by $x + \ell x$ we have

$$(x + \ell x)({}^\sigma x + \ell^\sigma x) = 1 + \ell(2x^\sigma x + \ell x^\sigma x + a),$$

and ℓ cannot divide $2x^\sigma x$ because ℓ is odd and $x \in \mathbb{Z}_{\ell^2}^\times$. Then, since the norm map $\mathbb{Q}_{\ell^2}^\times \to \mathbb{Q}_\ell^\times$ induces a surjective homomorphism $\mathbb{Z}_{\ell^2}^\times \to \mathbb{Z}_\ell^\times$, we can write

$$1 = x^\sigma x - \ell y^\sigma y \quad \text{for some } y \in \mathbb{Z}_{\ell^2},$$

and

$$\gamma_\ell = \begin{pmatrix} x & y \\ \ell\,{}^\sigma y & {}^\sigma x \end{pmatrix} \in \mathcal{O}_{D,\ell}^\times$$

has reduced norm 1 and satisfies $\varepsilon_\ell(\gamma_\ell) = \bar{x}$. Applying [**Miy89**, Theorem 5.2.10], there exists $\gamma \in \mathcal{O}_D^1$ such that $\gamma - \gamma_\ell \in \ell\mathbb{Z}_{\ell^2}$, thus $\varepsilon_\ell(\gamma) = \bar{x}$. □

And finally, the only non-trivial element of $\mathcal{O}_D^1$ acting as the identity on $\mathcal{H}$ is -1, but $-1 \notin \Gamma_{D,\ell}$. Therefore, the automorphism group

$$\mathrm{Aut}(V_{D,\ell}/X_D) := \mathrm{Aut}(V_{D,\ell}/X_D \times_{\mathbb{Q}} \mathbb{C}) \simeq (\mathcal{O}_D^1/\Gamma_{D,\ell})/\{\pm 1\}$$

of the cyclic covering $V_{D,\ell} \to \mathcal{O}_D^1 \setminus \mathcal{H} \simeq X_D \times_{\mathbb{Q}} \mathbb{C}$ is naturally identified with the unique subgroup of Δ of order $(\ell+1)/2$. By means of the isomorphism $\Delta \simeq \mathbb{F}_{\ell^2}^\times/\{\pm 1\}$ and the above lemma, the group $\mathrm{Aut}(V_{D,\ell}/X_D)$ corresponds to the subgroup

$$\mathbb{F}_{\ell^2}^1/\{\pm 1\} \subseteq \mathbb{F}_{\ell^2}^\times/\{\pm 1\} \simeq \Delta.$$

The quotient $\mathbb{F}_{\ell^2}^\times/\mathbb{F}_{\ell^2}^1$ is cyclic of order $\ell - 1$, thus we have a short exact sequence

$$1 \longrightarrow \mathrm{Aut}(V_{D,\ell}/X_D) \longrightarrow \Delta = \mathrm{Aut}(X_{D,\ell}/X_D) \longrightarrow \mathbb{F}_\ell^\times \longrightarrow 1.$$

Actually, this short exact sequence summarises the interpretation of the action of diamond automorphisms on the set $\pi_0(X_{D,\ell} \times_{\mathbb{Q}} \mathbb{C}) = \mathcal{C}_\infty(D,\ell)$ of geometric connected components of $X_{D,\ell}$. Namely, the group $\mathrm{Aut}(V_{D,\ell}/X_D) \simeq \mathbb{F}_{\ell^2}^1/\{\pm 1\}$ of covering automorphisms of $V_{D,\ell} \to X_D$ is identified with the subgroup of diamond automorphisms in Δ acting trivially on the set $\mathcal{C}_\infty(D,\ell)$. Given two diamond automorphisms $\delta, \delta' \in \Delta$, their action on $\mathcal{C}_\infty(D,\ell)$ is the same if and only if $\delta^{-1}\delta' \in \mathbb{F}_{\ell^2}^1/\{\pm 1\}$; equivalently, if and only if δ and δ' define the same element in the quotient $\mathbb{F}_\ell^\times$.

A detailed account of the action of a modular automorphism on the set of geometric connected components of $X_{D,\ell}$ will be given in Section 4.1.

3. Atkin-Lehner involutions and their lifts to $X_{D,\ell}$

Now we turn our attention to another family of modular automorphisms of the Shimura curve $X_{D,\ell}$. For every positive divisor m of D, we shall define an involution $\hat{\omega}_m$ on $X_{D,\ell}$ lifting the usual Atkin-Lehner involution ω_m on X_D associated with m. We first construct the involutions $\hat{\omega}_q$ attached to the primes q dividing D, and show that they commute pairwise. Then we define the involution $\hat{\omega}_m$ attached to an arbitrary positive divisor m of D as the product of the involutions $\hat{\omega}_q$ as q ranges over the primes dividing m.

Let q be a prime dividing D. Recall that the usual Atkin-Lehner involution ω_q on X_D attached to q is defined adèlically as the modular automorphism $\rho_{\widehat{\mathcal{O}}_D^\times}(\mathrm{w}_q)$, where

$$\mathrm{w}_q = \begin{pmatrix} 0 & 1 \\ q & 0 \end{pmatrix} \in \mathcal{O}_{D,q} \cap B_{D,q}^\times.$$

This way, $\omega_q \in \mathrm{Aut}^{\mathrm{mod}}(X_D) = W_D$ is clearly an involution because $\mathrm{w}_q^2 = q \in \mathcal{O}_{D,q}$ and $(1,\dots,1,q,1,1,\dots) \in \mathbb{Q}^\times \widehat{\mathcal{O}}_D^\times$. Besides, the action of ω_q on the Shimura curve X_D can be interpreted in moduli-theoretic terms (see Section 3.4 of Chapter 1).

The first attempt in order to lift the involution ω_q to $X_{D,\ell}$ is to consider the modular automorphism $\rho_{\mathcal{U}_D}(\mathrm{w}_q) \in \mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$. Plainly, this automorphism lifts the involution ω_q to $X_{D,\ell}$, but now

$$\rho_{\mathcal{U}_D}(\mathrm{w}_q)^2 = \rho_{\mathcal{U}_D}(\mathrm{w}_q^2) = \rho_{\mathcal{U}_D}(1,\dots,1,q,1,\dots), \tag{2.7}$$

where the q is in the q-th position, and this automorphism is not necessarily the identity on $X_{D,\ell}$:

Lemma 2.8. *For each prime $q \neq \ell$ dividing D, we have*

$$\rho_{\mathcal{U}_D}(\mathrm{w}_q)^2 = \delta_q \in \Delta = \mathrm{Aut}(X_{D,\ell}/X_D),$$

where $\delta_q := \rho_{\mathcal{U}_D}(1,\dots,1,q^{-1},1,\dots)$, $q^{-1} \in \mathcal{O}_{D,\ell}^\times$. Besides, the automorphism $\rho_{\mathcal{U}_D}(\mathrm{w}_\ell)$ is an involution.

Proof. For the distinguished prime ℓ, it follows immediately from (2.7) that $\rho_{\mathcal{U}_D}(\mathrm{w}_\ell^2)$ acts as the identity automorphism on $X_{D,\ell}$, since $\ell \in \mathcal{O}_{D,v}^\times$ for all $v \neq \ell$ and

$$\rho_{\mathcal{U}_D}(1/\ell)\rho_{\mathcal{U}_D}(\mathrm{w}_\ell^2)\rho_{\mathcal{U}_D}(\ell,\dots,\ell,1,\ell\dots) = \rho_{\mathcal{U}_D}(1,1,\dots).$$

Now assume q is a prime dividing D/ℓ, and let

$$\kappa := (q,\dots,q,1,q,\dots,q,1,q,\dots) \in \mathcal{U}_D,$$

where the 1's are in the q-th and ℓ-th positions. Then, using (2.7) again, we see that

$$\rho_{\mathcal{U}_D}(\mathrm{w}_q)^2 = \rho_{\mathcal{U}_D}(1/q)\rho_{\mathcal{U}_D}(\mathrm{w}_q^2)\rho_{\mathcal{U}_D}(\kappa) = \rho_{\mathcal{U}_D}(1,\dots,1,q^{-1},1,\dots) = \delta_q$$

as claimed. □

As a consequence, for primes $q \neq \ell$ we see that the automorphism $\rho_{\mathcal{U}_D}(\mathrm{w}_q)$ lifting ω_q is an involution on $X_{D,\ell}$ if and only if $\delta_q = \mathrm{id}$, which is equivalent to saying that $q \equiv \pm 1 \mod \ell$. However, we can still lift the Atkin-Lehner involutions ω_q to involutions on $X_{D,\ell}$ without assuming this condition as follows.

Continue assuming that $q \neq \ell$, and choose an element $s_q \in \mathbb{Z}_{\ell^2}^\times$ such that its reduction $\bar{s}_q \in \mathbb{F}_{\ell^2}^\times$ modulo $\ell\mathbb{Z}_{\ell^2}$ satisfies $\bar{s}_q^2 = q \in \mathbb{F}_\ell^\times \subseteq \mathbb{F}_{\ell^2}^\times$. Then consider the element

$$u_q := \begin{pmatrix} s_q & 0 \\ 0 & \sigma_{s_q} \end{pmatrix} \in \mathcal{O}_{D,\ell}^\times,$$

which satisfies $u_q^2 = q \in \mathcal{O}_{D,\ell}^\times$, hence $\rho_{\mathcal{U}_D}(u_q)^2 = \delta_q^{-1}$.

Remark 2.9. The diamond automorphism $\rho_{\mathcal{U}_D}(u_q) \in \Delta$ is well defined. It is clear by construction that $\rho_{\mathcal{U}_D}(u_q)$ does not depend on the choice of s_q modulo $\ell\mathbb{Z}_{\ell^2}$. In addition, since $\rho_{\mathcal{U}_D}(1,\dots,1,-1,1,\dots)$ (with the -1 in the ℓ-th position) is the identity automorphism on $X_{D,\ell}$, $\rho_{\mathcal{U}_D}(u_q)$ remains the same if s_q is replaced by $-s_q$.

Definition 2.10. *Let q be a prime dividing D. We define the modular automorphism $\hat{\omega}_q \in \mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ by*

$$\hat{\omega}_q := \begin{cases} \rho_{\mathcal{U}_D}(\mathrm{w}_\ell) & \text{if } q = \ell, \\ \rho_{\mathcal{U}_D}(\mathrm{w}_q, u_q) = \rho_{\mathcal{U}_D}(\mathrm{w}_q)\rho_{\mathcal{U}_D}(u_q) & \text{if } q \neq \ell. \end{cases}$$

Directly from the definition and Lemma 2.8:

COROLLARY 2.11. *For every prime q dividing D, the automorphism $\hat{\omega}_q \in \mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ is an involution lifting the Atkin-Lehner involution ω_q on X_D to the curve $X_{D,\ell}$.*

Finally, we observe that the involutions $\hat{\omega}_q$, as q ranges over the prime divisors of D, commute pairwise:

LEMMA 2.12. *For primes q, q' dividing D, $\hat{\omega}_q\hat{\omega}_{q'} = \hat{\omega}_{q'}\hat{\omega}_q$.*

PROOF. The statement is obvious if $q' = q$, and it is also clear when both q and q' are different from ℓ, because u_q and $u_{q'}$ commute one with each other in $\mathcal{O}_{D,p}^\times$. Thus it remains to prove that $\hat{\omega}_q\hat{\omega}_\ell = \hat{\omega}_\ell\hat{\omega}_q$ for every prime $q \neq \ell$ dividing D, which amounts to checking that

$$\rho_{\mathcal{U}_D}(u_q)\rho_{\mathcal{U}_D}(\mathrm{w}_\ell) = \rho_{\mathcal{U}_D}(\mathrm{w}_\ell)\rho_{\mathcal{U}_D}(u_q).$$

Indeed, one easily checks from the definitions that $u_q\mathrm{w}_\ell = \mathrm{w}_\ell{}^\sigma u_q$. If q is a square in $\mathbb{F}_\ell^\times$, we can choose $s_q \in \mathbb{Z}_\ell^\times$, and therefore ${}^\sigma u_q = u_q$ and we are done. Otherwise, ${}^\sigma s_q \equiv -s_q \mod \ell\mathbb{Z}_{\ell^2}$ and the claim follows from the fact that $\rho_{\mathcal{U}_D}(1,\dots,1,-1,1,\dots) = \mathrm{id}$. □

As a consequence, we can attach an involution $\hat{\omega}_m \in \mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ lifting ω_m to an arbitrary positive divisor m of D, just by defining $\hat{\omega}_m$ as the product of the involutions $\hat{\omega}_q$ with q ranging over the prime divisors of m. We call $\hat{\omega}_m$ the *Atkin-Lehner involution on $X_{D,\ell}$ associated with m*, and write

$$W_{D,\ell} := \{\hat{\omega}_m : m \mid D, m > 0\} = \langle \hat{\omega}_q : q \mid D, q \text{ prime}\rangle \subseteq \mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell}) \tag{2.8}$$

for the abelian group consisting of these involutions, which is generated by the involutions $\hat{\omega}_q$ with $q \mid D$ prime. It is naturally a subgroup of $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ and, by the above lemma,

$$W_{D,\ell} \simeq (\mathbb{Z}/2\mathbb{Z})^{2r}.$$

Moreover, for any pair of positive divisors m, m' of D, we have the relation

$$\hat{\omega}_m\hat{\omega}_{m'} = \hat{\omega}_{\frac{mm'}{\gcd(m,m')^2}}.$$

So far, we have introduced two *natural* abelian subgroups of the group $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ of modular automorphisms of $X_{D,\ell}$. Namely, the group $\Delta = \mathrm{Aut}(X_{D,\ell}/X_D)$ of diamond automorphisms and the group $W_{D,\ell}$ of (lifted) Atkin-Lehner involutions. The above description of $W_{D,\ell}$ establishes part (1) of Theorem 2.1, and in the next section we will conclude the proof of part (2). Before that, we show how an Atkin-Lehner involution interacts with a diamond automorphism:

PROPOSITION 2.13. *Let $\delta \in \Delta$ be a diamond automorphism, and let $m \mid D$, $m > 0$. Then, the following holds in $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$:*

$$\delta\hat{\omega}_m = \begin{cases} \hat{\omega}_m\delta & \text{if } \ell \nmid m, \\ \hat{\omega}_m\delta^\ell & \text{if } \ell \mid m. \end{cases}$$

PROOF. Since Atkin-Lehner involutions on $X_{D,\ell}$ commute pairwise, it suffices to prove the statement for $m = q$ prime. Moreover, we can also assume that $\delta = \rho_{\mathcal{U}_D}(\alpha)$, where

$$\alpha = \begin{pmatrix} x & 0 \\ 0 & {}^\sigma x \end{pmatrix} \in \mathcal{O}_{D,\ell}^\times$$

for some $x \in \mathbb{Z}_{\ell^2}^\times$.

If $q \neq \ell$, then the automorphism $\delta = \rho_{\mathcal{U}_D}(\alpha)$ commutes with both $\rho_{\mathcal{U}_D}(u_q)$ and $\rho_{\mathcal{U}_D}(\mathrm{w}_q)$, thus

$$\delta\hat{\omega}_q = \rho_{\mathcal{U}_D}(\alpha)\rho_{\mathcal{U}_D}(\mathrm{w}_q)\rho_{\mathcal{U}_D}(u_q) = \rho_{\mathcal{U}_D}(\mathrm{w}_q)\rho_{\mathcal{U}_D}(u_q)\rho_{\mathcal{U}_D}(\alpha) = \hat{\omega}_q\delta.$$

And if $q = \ell$, observe that $\rho_{\mathcal{U}_D}({}^\sigma\alpha) = \rho_{\mathcal{U}_D}(\alpha^\ell) = \rho_{\mathcal{U}_D}(\alpha)^\ell$ because ${}^\sigma x \equiv x^\ell \mod \ell\mathbb{Z}_{\ell^2}$, hence the statement follows from the identity $\alpha\mathrm{w}_\ell = \mathrm{w}_\ell\,{}^\sigma\alpha$. □

4. The group $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ of modular automorphisms

At this point, we know that the group $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ of modular automorphisms of the Shimura curve $X_{D,\ell}$ contains both $\Delta = \mathrm{Aut}(X_{D,\ell}/X_D)$ and $W_{D,\ell}$ as subgroups, hence also the group

$$G := \Delta W_{D,\ell}$$

generated by them. Moreover, $\Delta \cap W_{D,\ell} = \{1\}$: otherwise, some non-trivial Atkin-Lehner involution $\hat{\omega}_m$ on $X_{D,\ell}$ would be an automorphism of the covering $X_{D,\ell} \to X_D$, and this would force the corresponding Atkin-Lehner involution ω_m on X_D to be trivial, that is to say, $m = 1$, which is a contradiction.

Proposition 2.13 implies that Δ is normal in G, and hence G is a semidirect product of its subgroups Δ and $W_{D,p}$. In particular, $|G| = (\ell^2 - 1)2^{2r-1}$.

The goal of this section is to prove part (2) of Theorem 2.1. We will first show that the inclusion $G \subseteq \mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ is actually an equality, by comparing orders, and then we will determine the structure of $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ as an abstract group.

Recall that the group $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ is defined as the quotient

$$N(\mathcal{U}_D)/\mathbb{Q}^\times \mathcal{U}_D,$$

where $N(\mathcal{U}_D) := \mathrm{Norm}_{(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times}(\mathcal{U}_D)$ is the normaliser of $\mathcal{U}_D$ in $(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$. Writing

$$\mathcal{U}_D = \prod_v \mathcal{U}_{D,v}$$

as in (2.2), observe that

$$\begin{aligned} N(\mathcal{U}_D) &= \{(b_v)_v \in (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times : b_v^{-1}\mathcal{U}_{D,v} b_v = \mathcal{U}_{D,v} \text{ for all } v\} = \\ &= (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times \cap \prod_v N_v(\mathcal{U}_{D,v}), \end{aligned}$$

where $N_v(\mathcal{U}_{D,v}) := \mathrm{Norm}_{B_{D,v}^\times}(\mathcal{U}_{D,v})$. For primes $v \nmid D$, the local quaternion algebra $B_{D,v}$ is isomorphic to $\mathrm{M}_2(\mathbb{Q}_v)$ and all its maximal orders are conjugate to $\mathrm{M}_2(\mathbb{Z}_v)$, hence the normaliser of $\mathcal{O}_{D,v}^\times$ in $B_{D,v}^\times$ is $\mathbb{Q}_v^\times \mathcal{O}_{D,v}^\times$. In contrast, for primes $v \mid D$ this normaliser is the full group of units $B_{D,v}^\times$, because $\mathcal{O}_{D,v}$ is the unique maximal order in the local quaternion algebra $B_{D,v}$. At the prime ℓ, since I_ℓ is the unique two-sided $\mathcal{O}_{D,\ell}$-ideal of reduced norm ℓ we also have $N_\ell(1 + I_\ell) = B_{D,\ell}^\times$. Summing up,

$$N(\mathcal{U}_D) = \{(b_v)_v \in (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times : b_v \in \mathbb{Q}_v^\times \mathcal{O}_{D,v}^\times \text{ for all } v \nmid D\}. \tag{2.9}$$

Now consider the surjective homomorphism

$$\varphi : N(\mathcal{U}_D) \longrightarrow \prod_{v|D} N_v(\mathcal{U}_{D,v})/\mathbb{Q}_v^\times \mathcal{U}_{D,v}, \quad (b_v)_v \longmapsto ([b_v])_{v|D},$$

which induces an exact sequence

$$1 \longrightarrow N_\varphi := \ker(\varphi) \longrightarrow N(\mathcal{U}_D) \xrightarrow{\varphi} \prod_{v|D} N_v(\mathcal{U}_{D,v})/\mathbb{Q}_v^\times \mathcal{U}_{D,v} \longrightarrow 1.$$

From (2.9) and the definition of φ, observe that $N_\varphi = \mathbb{A}_f^\times \mathcal{U}_D$, hence $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ fits in the following short exact sequence:

$$1 \longrightarrow \mathbb{A}_f^\times \mathcal{U}_D/\mathbb{Q}^\times \mathcal{U}_D \longrightarrow \mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell}) \longrightarrow \prod_{v|D} N_v(\mathcal{U}_{D,v})/\mathbb{Q}_v^\times \mathcal{U}_{D,v} \longrightarrow 1. \tag{2.10}$$

Lemma 2.14. *The quotient $\mathbb{A}_f^\times \mathcal{U}_D/\mathbb{Q}^\times \mathcal{U}_D$ is isomorphic to $\mathbb{F}_\ell^\times/\{\pm 1\}$.*

PROOF. There is a natural isomorphism

$$\mathbb{A}_f^\times \mathcal{U}_D/\mathbb{Q}^\times \mathcal{U}_D \simeq \mathbb{A}_f^\times/(\mathbb{A}_f^\times \cap \mathbb{Q}^\times \mathcal{U}_D),$$

so let us determine the intersection $\mathbb{A}_f^\times \cap \mathbb{Q}^\times \mathcal{U}_D$. If we write $S = \prod_v S_v$, where $S_v := \mathbb{Z}_v^\times$ for all primes $v \neq \ell$ and $S_\ell := 1 + \ell\mathbb{Z}_\ell$, then it is clear that

$$\mathbb{Q}^\times S \subseteq \mathbb{A}_f^\times \cap \mathbb{Q}^\times \mathcal{U}_D.$$

But the reverse inclusion also holds. Indeed, let $q(\kappa_v)_v \in \mathbb{A}_f^\times \cap \mathbb{Q}^\times \mathcal{U}_D$, with $q \in \mathbb{Q}^\times$ and $(\kappa_v)_v \in \mathcal{U}_D$. In particular, $q(\kappa_v)_v$, hence also $(\kappa_v)_v$, belongs to $\mathbb{A}_f^\times$, so that

$$\begin{aligned} &\kappa_v \in \mathcal{O}_{D,v}^\times \cap \mathbb{Q}_v^\times = \mathbb{Z}_v^\times \text{ for all } v \neq \ell, \\ &\kappa_\ell \in (1 + I_\ell) \cap \mathbb{Q}_\ell^\times = 1 + \mathbb{Z}_\ell, \end{aligned}$$

and the claim follows. Therefore, we deduce that

$$\begin{aligned} \mathbb{A}_f^\times \mathcal{U}_D/\mathbb{Q}^\times \mathcal{U}_D &\simeq \mathbb{A}_f^\times/\mathbb{Q}^\times S \simeq \widehat{\mathbb{Z}}^\times \mathbb{Q}^\times/\mathbb{Q}^\times S \simeq \widehat{\mathbb{Z}}^\times/S\{\pm 1\} \simeq \\ &\simeq (\mathbb{Z}_\ell^\times/(1 + \ell\mathbb{Z}_\ell))/\{\pm 1\} \simeq \mathbb{F}_\ell^\times/\{\pm 1\}. \end{aligned}$$

□

LEMMA 2.15. *The group $\prod_{v|D} N_v(\mathcal{U}_{D,v})/\mathbb{Q}_\ell^\times \mathcal{U}_{D,v}$ is isomorphic to the direct product of $(\mathbb{Z}/2\mathbb{Z})^{2r-1}$ and an extension of $\mathbb{Z}/2\mathbb{Z}$ by $\mathbb{Z}/(\ell+1)\mathbb{Z}$.*

PROOF. We shall distinguish the factors $N_v(\mathcal{U}_{D,v})/\mathbb{Q}_v^\times \mathcal{U}_{D,v}$ at primes $v \neq \ell$ from the one at ℓ. For the primes $v \mid D/\ell$, the quotient

$$N_v(\mathcal{U}_{D,v})/\mathbb{Q}_v^\times \mathcal{U}_{D,v} = B_{D,v}^\times/\mathbb{Q}_v^\times \mathcal{O}_{D,v}^\times$$

is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ (see the proof of Proposition 1.28, or [**Vig80**, Chap. III, Exercises 5.4, 5.5]), and we have $2r-1$ such factors.

In contrast, at the prime ℓ the quotient $B_{D,\ell}^\times/\mathbb{Q}_\ell^\times(1 + I_\ell)$ fits in the short exact sequence

$$1 \longrightarrow \mathbb{Q}_\ell^\times \mathcal{O}_{D,\ell}^\times/\mathbb{Q}_\ell^\times(1 + I_\ell) \longrightarrow B_{D,\ell}^\times/\mathbb{Q}_\ell^\times(1 + I_\ell) \longrightarrow B_{D,\ell}^\times/\mathbb{Q}_\ell^\times \mathcal{O}_{D,\ell}^\times \longrightarrow 1.$$

As before, $B_{D,\ell}^\times/\mathbb{Q}_\ell^\times \mathcal{O}_{D,\ell}^\times \simeq \mathbb{Z}/2\mathbb{Z}$, and we claim that

$$\mathbb{Q}_\ell^\times \mathcal{O}_{D,\ell}^\times/\mathbb{Q}_\ell^\times(1 + I_\ell)$$

is cyclic of order $\ell + 1$, from which the lemma follows. Indeed, using the equality

$$\mathbb{Q}_\ell^\times(1 + I_\ell) \cap \mathcal{O}_{D,\ell}^\times = \mathbb{Z}_\ell^\times(1 + I_\ell)$$

we have a natural isomorphism

$$\mathbb{Q}_\ell^\times \mathcal{O}_{D,\ell}^\times/\mathbb{Q}_\ell^\times(1 + I_\ell) \simeq \mathcal{O}_{D,\ell}^\times/\mathbb{Z}_\ell^\times(1 + I_\ell).$$

Then, by composing the Nebentypus character $\varepsilon_\ell : \mathcal{O}_{D,\ell}^\times \to \mathbb{F}_{\ell^2}^\times$ with the natural quotient homomorphism $\mathbb{F}_{\ell^2}^\times \to \mathbb{F}_{\ell^2}^\times/\mathbb{F}_\ell^\times$, the kernel of the resulting surjective homomorphism $\mathcal{O}_{D,\ell}^\times \to \mathbb{F}_{\ell^2}^\times/\mathbb{F}_\ell^\times$ is precisely $\mathbb{Z}_\ell^\times(1 + I_\ell)$, hence the claim is proved. □

As a direct consequence of Lemmas 2.14 and 2.15, we finally obtain:

PROPOSITION 2.16. *The group $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ is generated by its subgroups Δ and $W_{D,\ell}$, i.e.*

$$\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell}) = \Delta W_{D,\ell} = G.$$

PROOF. The short exact sequence in (2.10) expresses $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ as an extension of a group of order $2^{2r}(\ell + 1)$ by a cyclic group of order $(\ell - 1)/2$. In particular, the order of $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ is $(\ell^2 - 1)2^{2r-1} = |G|$ and the inclusion $G \subseteq \mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ is then an equality. □

Finally, we describe the structure of $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ as an abstract group, but instead of using the exact sequence in (2.10) we rather take advantage of our knowledge of the subgroups Δ and $W_{D,\ell}$ from the previous sections.

It follows from Proposition 2.13 that Δ is normal in $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell}) = \Delta W_{D,\ell}$, with quotient isomorphic to $W_{D,\ell}$. Then, the inclusion of $W_{D,\ell}$ in $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ makes the short exact sequence

$$1 \longrightarrow \Delta \longrightarrow \mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell}) \longrightarrow W_{D,\ell} \longrightarrow 1 \tag{2.11}$$

split, hence $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ is recovered as the semidirect product $\Delta \rtimes_\theta W_{D,\ell}$ of its subgroups Δ and $W_{D,\ell}$, where the action $\theta : W_{D,\ell} \to \mathrm{Aut}(\Delta)$ is given by

$$\theta(\hat{\omega}_m)(\delta) = \hat{\omega}_m^{-1}\delta\hat{\omega}_m = \hat{\omega}_m\delta\hat{\omega}_m = \begin{cases} \delta & \text{if } \ell \nmid m, \\ \delta^\ell & \text{if } \ell \mid m. \end{cases}$$

Write $W_{D/\ell,\ell} = \langle \hat{\omega}_q : q \text{ prime}, q \mid \frac{D}{\ell} \rangle$ for the subgroup of $W_{D,\ell}$ consisting of the Atkin-Lehner involutions $\hat{\omega}_m$ associated with the positive divisors m of D/ℓ. Then observe that

$$W_{D,\ell} = \langle \hat{\omega}_\ell \rangle \times W_{D/\ell,\ell},$$

and the action θ is trivial on $W_{D/\ell,\ell}$ because the involutions in $W_{D/\ell,\ell}$ commute with the diamond automorphisms. Therefore, we have a natural isomorphism

$$\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell}) = \Delta \rtimes_\theta W_{D,\ell} \simeq (\Delta \rtimes_\eta \langle \hat{\omega}_\ell \rangle) \times W_{D/\ell,\ell},$$

where now $\eta : \langle \hat{\omega}_\ell \rangle \to \mathrm{Aut}(\Delta)$ is determined by

$$\eta(\hat{\omega}_\ell)(\delta) = \hat{\omega}_\ell\delta\hat{\omega}_\ell = \delta^\ell, \qquad \delta \in \Delta.$$

This concludes the proof of Theorem 2.1.

Remark 2.17. Identifying $W_{D,\ell} \simeq W_D$ in the natural way, the short exact sequence (2.11) becomes

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Delta & \longrightarrow & \mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell}) & \longrightarrow & W_D & \longrightarrow & 1, \\ & & \delta & \longmapsto & \delta & & & & \\ & & & & \delta\hat{\omega}_m & \longmapsto & \omega_m & & \end{array}$$

which shows that the modular automorphisms of $X_{D,\ell}$ lifting an Atkin-Lehner involution ω_m on X_D are precisely those in the coset $\Delta\hat{\omega}_m = \hat{\omega}_m\Delta$. If q is a prime dividing D, from the adèlic definition of $\hat{\omega}_q$ we see that the automorphisms in $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ lifting $\omega_q \in W_D$ are those in $\Delta\rho_{\mathcal{U}_D}(\mathrm{w}_q) = \rho_{\mathcal{U}_D}(\mathrm{w}_q)\Delta$.

Remark 2.18. Let q be a prime dividing D, and let $\hat{\omega}_q \in W_{D,\ell}$ be the associated Atkin-Lehner involution defined as in Definition 2.10. After the previous remark, it is natural to ask whether there are other involutions in $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ lifting ω_q or not. In other words, is the choice of $\hat{\omega}_q$ unique or canonical in some sense?

As in Remark 2.17, every modular automorphism lifting ω_q is of the form $\delta\hat{\omega}_q$ for some $\delta \in \Delta$. If $q \neq \ell$, since $\hat{\omega}_q$ commutes with every diamond automorphism it is clear that $\delta\hat{\omega}_q$ is an involution if and only if $\delta^2 = 1$. If we denote by τ the unique diamond involution in Δ, then there are exactly two involutions in $\mathrm{Aut}^{\mathrm{mod}}(X_{D,p})$ lifting ω_q, namely $\hat{\omega}_q$ and $\tau\hat{\omega}_q$.

Besides, for the distinguished prime ℓ the involution $\hat{\omega}_\ell$ does not commute with the diamond automorphisms, and from the identity

$$(\delta\hat{\omega}_\ell)^2 = \delta\hat{\omega}_\ell\delta\hat{\omega}_\ell = \delta^{\ell+1}$$

we see that $\delta\hat{\omega}_\ell$ is an involution if and only if δ lies in the unique (cyclic) subgroup $\Theta \subseteq \Delta$ of order $\ell+1$. As a consequence, there are exactly $\ell+1$ involutions in $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ lifting ω_ℓ, namely the $\ell+1$ automorphisms in $\Theta\hat{\omega}_\ell$.

Nevertheless, we emphasise that the group structure of $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ as stated in Theorem 2.1 does not depend on which involutions in $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ lifting the usual Atkin-Lehner involutions on X_D we choose.

4.1. Action of modular automorphisms on the set of connected components. Let $\rho_{\mathcal{U}_D}(\alpha) \in \mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ be a modular automorphism of $X_{D,\ell}$, where $\alpha = (\alpha_v)_v \in N(\mathcal{U}_D)$. Let $[z, (\beta_v)_v] \in X_{D,\ell} \times_{\mathbb{Q}} \mathbb{C}$ be a point on the Riemann surface underlying $X_{D,\ell}$ and assume without loss of generality that $z \in \mathcal{H}$. Let also $[c] \in \mathcal{C}_\infty(D,\ell) \simeq \mathbb{F}_\ell^\times$ be the connected component of $X_{D,\ell} \times_{\mathbb{Q}} \mathbb{C}$ in which this point lies, where as usual $c \in (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$ and we regard $[c] \in \mathbb{F}_\ell^\times$ through the isomorphisms

$$\mathcal{C}_\infty(D,\ell) = B_{D,+}^\times \setminus (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times / \mathcal{U}_D \simeq \mathbb{Q}^{>0} \setminus \mathbb{A}_f^\times / \mathrm{n}(\mathcal{U}_D) \simeq \mathbb{Z}_\ell^\times / (1 + \ell\mathbb{Z}_\ell) \simeq \mathbb{F}_\ell^\times.$$

Then the connected component in which the point

$$\rho_{\mathcal{U}_D}(\alpha)([z, (\beta_v)_v]) = [z, (\beta_v \alpha_v)_v]$$

lies is given by the class of $\mathrm{n}((\beta_v\alpha_v)_v)$ in $\mathbb{Q}^{>0} \setminus \mathbb{A}_f^\times / \mathrm{n}(\mathcal{U}_D) \simeq \mathbb{F}_\ell^\times$. Since the double coset

$$B_{D,+}^\times \setminus (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times / \widehat{\mathcal{O}}_D^\times$$

is trivial, there are elements $b \in B_{D,+}^\times, (\gamma_v)_v \in \widehat{\mathcal{O}}_D^\times$ such that $(\beta_v\alpha_v)_v = b(\beta_v)_v(\gamma_v)_v$. Hence, taking classes in $B_{D,+}^\times \setminus (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times / \mathcal{U}_D$ we see that

$$[(\beta_v\alpha_v)_v] = [b(\beta_v)_v(1, \dots, 1, \gamma_\ell, 1, \dots)(\gamma_v)_{v\neq\ell}] = [(\beta_v)_v(1, \dots, 1, \gamma_\ell, 1, \dots)],$$

and using the reduced norm we deduce that $\rho_{\mathcal{U}_D}(\alpha)([z, (\beta_v)_v])$ lies in the connected component given by

$$[\mathrm{n}(\gamma_\ell)][c] \in \mathbb{F}_\ell^\times,$$

where $[\mathrm{n}(\gamma_\ell)]$ denotes the class of $\mathrm{n}(\gamma_\ell) \in \mathbb{Z}_\ell^\times$ in $\mathbb{F}_\ell^\times \simeq \mathbb{Z}_\ell^\times / (1 + \ell\mathbb{Z}_\ell)$.

Example 2.19. For a diamond automorphism $\delta \in \Delta$ represented by some $\alpha_\ell \in \mathcal{O}_{D,\ell}^\times$, that is $\delta = \rho_{\mathcal{U}_D}(1, \dots, 1, \alpha_\ell, 1, \dots)$, the previous argument shows that δ maps the connected component indexed by $[c] \in \mathbb{F}_\ell^\times$ to the one indexed by $[\mathrm{n}(\alpha_\ell)][c] \in \mathbb{F}_\ell^\times$.

Let us describe now in detail the action of Atkin-Lehner involutions on the set $\mathcal{C}_\infty(D,\ell)$. First let $q \neq \ell$ be a prime dividing D, and let $\hat{\omega}_q \in \mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ be the associated Atkin-Lehner involution on $X_{D,\ell}$. In order to determine its action on $\mathcal{C}_\infty(D,\ell)$, we need to study the modular automorphisms $\rho_{\mathcal{U}_D}(\mathrm{w}_q)$ and $\rho_{\mathcal{U}_D}(u_q)$.

The action of $\rho_{\mathcal{U}_D}(\mathrm{w}_q)$ on the points of $X_{D,\ell} \times_{\mathbb{Q}} \mathbb{C}$ is given by

$$[z, (\beta_v)_v] \longmapsto [z, (\dots, \beta_v, \dots, \beta_q \mathrm{w}_q, \dots)],$$

where again we can assume $z \in \mathcal{H}$. Now write

$$(\dots, \beta_v, \dots, \beta_q \mathrm{w}_q, \dots) = b(\beta_v)_v(\gamma_v)_v$$

for some $b \in B_{D,+}^\times$, $(\gamma_v)_v \in \widehat{\mathcal{O}}_D^\times$. The equalities at the v-th components for $v \neq q$ tell us that $\mathrm{n}(b)$ must be a power of q, and from the equality $\beta_q \mathrm{w}_q = b\beta_q\gamma_q$ we deduce that $\mathrm{n}(b) = q$. As a consequence, $\mathrm{n}(\gamma_\ell) = q^{-1}$, and by the above discussion $\rho_{\mathcal{U}_D}(\mathrm{w}_q)$ sends the connected component indexed by $[c] \in \mathbb{F}_\ell^\times$ to the one indexed by $[c][q]^{-1} \in \mathbb{F}_\ell^\times$.

As for the automorphism $\rho_{\mathcal{U}_D}(u_q)$, we shall distinguish two cases.

(i) If q is a square in $\mathbb{F}_\ell^\times$ we can choose s_q to be in $\mathbb{Z}_\ell^\times$. In this case, ${}^\sigma s_q = s_q$ and $[\mathrm{n}(u_q)] = [q]$ in $\mathbb{F}_\ell^\times$. From Example 2.19, $\rho_{\mathcal{U}_D}(u_q)$ maps the connected component indexed by $[c] \in \mathbb{F}_\ell^\times$ to the one indexed by $[c][q] \in \mathbb{F}_\ell^\times$.

(ii) If q is not a square in $\mathbb{F}_\ell^\times$ then $s_q \notin \mathbb{Z}_\ell^\times$ and ${}^\sigma s_q \equiv -s_q \bmod \ell\mathbb{Z}_{\ell^2}$, thus $[\mathrm{n}(u_q)] = -[q]$ in $\mathbb{F}_\ell^\times$. Therefore, the connected component indexed by $[c] \in \mathbb{F}_\ell^\times$ is sent by $\rho_{\mathcal{U}_D}(u_q)$ to the one indexed by $-[c][q] \in \mathbb{F}_\ell^\times$.

Therefore, when q is a square in $\mathbb{F}_\ell^\times$ the Atkin-Lehner involution $\hat{\omega}_q$ acts trivially on the set of connected components of $X_{D,\ell} \times_{\mathbb{Q}} \mathbb{C}$. Otherwise, if q is not a square modulo ℓ, then $\hat{\omega}_q$ acts on the set of connected components as multiplication by $[-1] \in \mathbb{F}_\ell^\times$.

Finally, we deal with the case of the Atkin-Lehner involution $\hat{\omega}_\ell = \rho_{\mathcal{U}_D}(\mathrm{w}_\ell)$, whose action on $X_{D,\ell} \times_{\mathbb{Q}} \mathbb{C}$ is described on points by

$$[z, (\beta_v)_v] \longmapsto [z, (\dots, \beta_v, \dots, \beta_\ell \mathrm{w}_\ell, \dots)].$$

Proceeding as before, writing

$$(\dots, \beta_v, \dots, \beta_\ell \mathrm{w}_\ell, \dots) = b(\beta_v)_v(\gamma_v)_v$$

for some $b \in B_{D,+}^\times$ and $(\gamma_v)_v \in \widehat{\mathcal{O}}_D^\times$, and looking separately the components at primes $v \neq \ell$ from the one at ℓ, one deduces that $\mathrm{n}(\gamma_\ell) = -1$. As a consequence, the Atkin-Lehner involution $\hat{\omega}_\ell$ acts on the set of connected components of the complex curve $X_{D,\ell} \times_{\mathbb{Q}} \mathbb{C}$ as the involution given by multiplication by $[-1] \in \mathbb{F}_\ell^\times$.

Summing up, for an arbitrary positive divisor m of D, the Atkin-Lehner involution $\hat{\omega}_m \in W_{D,\ell}$ acts on the set $\mathcal{C}_\infty(D, \ell) \simeq \mathbb{F}_\ell^\times$ as multiplication by

$$\varepsilon(m) := \begin{cases} \left(\frac{m}{\ell}\right) & \text{if } \ell \nmid m, \\ -\left(\frac{m/\ell}{\ell}\right) & \text{if } \ell \mid m, \end{cases} \tag{2.12}$$

where we regard the Kronecker symbol $\left(\frac{\cdot}{\ell}\right)$ as taking values in $\mathbb{F}_\ell$.

5. Cyclic étale Galois coverings of $X_D^{(m)}$

Let m be a positive divisor of D, and ω_m be the corresponding Atkin-Lehner involution on X_D. We write $X_D^{(m)}/\mathbb{Q}$ for the quotient $X_D/\langle\omega_m\rangle$ of X_D by the action of ω_m, and

$$\pi_m : X_D \longrightarrow X_D^{(m)}$$

for the natural projection map.

The cyclic Galois covering $g : X_{D,\ell} \to X_D$ can be used to prove the non-existence of rational points on the Shimura curve X_D over imaginary quadratic fields under certain congruence conditions (see [**Jor86**], [**Sko05**] and Chapter 5 below). Combined with the work of Jordan and Livné [**JL85**], such results often lead to counterexamples to the Hasse principle accounted for by the Brauer-Manin obstruction.

As an application of our study of the group $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ of modular automorphisms of $X_{D,\ell}$, now we want to obtain cyclic Galois coverings of $X_D^{(m)}$ from the intermediate coverings of $g : X_{D,\ell} \to X_D$. Even more, we will construct cyclic étale Galois coverings of $X_D^{(m)}$ that can be used to study the set of rational points $X_D^{(m)}(\mathbb{Q})$ by applying descent techniques.

Let $\hat{\omega}_m$ be the Atkin-Lehner involution on $X_{D,\ell}$ lifting ω_m, and write $X_{D,\ell}^{(m)}/\mathbb{Q}$ for the quotient $X_{D,\ell}/\langle\hat{\omega}_m\rangle$ of $X_{D,\ell}$ by the action of the lifted involution $\hat{\omega}_m$. Then the natural projection map

$$\hat{\pi}_m : X_{D,\ell} \longrightarrow X_{D,\ell}^{(m)} := X_{D,\ell}/\langle\hat{\omega}_m\rangle$$

onto the quotient gives rise to a commutative diagram

$$\begin{array}{ccc} X_{D,\ell} & \xrightarrow{g} & X_D \\ \downarrow{\scriptstyle \hat{\pi}_m} & & \downarrow{\scriptstyle \pi_m} \\ X_{D,\ell}^{(m)} & \xrightarrow{g^{(m)}} & X_D^{(m)}. \end{array} \tag{2.13}$$

For every positive divisor d of $(\ell^2 - 1)/2$, let $\Theta_d \subseteq \Delta$ denote the unique (cyclic) subgroup of Δ of index d (i.e. of order $(\ell^2 - 1)/2d$), and define $Y_d/\mathbb{Q}$ to be the intermediate curve of the covering $X_{D,\ell} \to X_D$ arising as the quotient of $X_{D,\ell}$ by the action of Θ_d. If $g_d : Y_d \to X_D$ denotes the induced covering, then $\deg(g_d) = d$. Actually, all the intermediate coverings of g arise in this way, and since Δ is cyclic it follows that all the g_d are cyclic Galois coverings. In particular, the intermediate curves Y_d are in bijection with the (cyclic) subgroups Θ_d of Δ, hence with the positive divisors of $(\ell^2 - 1)/2$.

By virtue of Proposition 2.13, the action of the Atkin-Lehner involution $\hat{\omega}_m$ on $X_{D,\ell}$ commutes with the action of each subgroup Θ_d of Δ. Therefore, $\hat{\omega}_m$ induces an involution on every intermediate curve Y_d lifting ω_m, which we still denote by $\hat{\omega}_m$. We write $Y_d^{(m)}/\mathbb{Q}$ for the quotient of Y_d by its action and

$$g_d^{(m)} : Y_d^{(m)} \longrightarrow X_D^{(m)}$$

for the natural induced covering.

5.1. The Galois property. The covering $X_{D,\ell} \to X_D^{(m)}$ obtained by composing g with π_m is Galois of degree $\ell^2 - 1$, and its automorphism group $\mathrm{Aut}(X_{D,\ell}/X_D^{(m)})$ is the group

$$\Delta\langle\hat{\omega}_m\rangle \subseteq \mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$$

generated by Δ and $\langle\hat{\omega}_m\rangle$. Therefore, the cyclic Galois coverings of $X_D^{(m)}$ induced by intermediate coverings of $g : X_{D,\ell} \to X_D$ and not factoring through X_D are in one-to-one correspondence with the normal subgroups of $\Delta\langle\hat{\omega}_m\rangle$ containing $\hat{\omega}_m$. After Theorem 2.1, the subgroups of $\Delta\langle\hat{\omega}_m\rangle$ containing $\hat{\omega}_m$ are precisely those of the form $\Theta_d\langle\hat{\omega}_m\rangle$, as d ranges through the positive divisors of $(\ell^2 - 1)/2$.

Corollary 2.20. *Let d be a positive divisor of $(\ell^2 - 1)/2$, and $g_d : Y_d \to X_D$ be the above defined covering.*

(i) *If ℓ does not divide m, then $g_d^{(m)} : Y_d^{(m)} \to X_D^{(m)}$ is a cyclic Galois covering of degree d. In particular, $g^{(m)} : X_{D,\ell}^{(m)} \to X_D^{(m)}$ is cyclic and Galois with automorphism group isomorphic to Δ.*

(ii) *If ℓ divides m, then $g_d^{(m)} : Y_d^{(m)} \to X_D^{(m)}$ is a cyclic Galois covering if and only if d divides $\ell - 1$. In particular, $g_{\ell-1}^{(m)} : Y_{\ell-1}^{(m)} \to X_D^{(m)}$ is cyclic and Galois with automorphism group isomorphic to $\Delta/(\mathbb{F}_{\ell^2}^1/\{\pm 1\}) \simeq \mathbb{F}_\ell^\times$.*

Proof. If ℓ does not divide m, it follows from Theorem 2.1 that

$$\Delta\langle\hat{\omega}_m\rangle \simeq \Delta \times \langle\hat{\omega}_m\rangle.$$

In particular, $\Delta\langle\hat{\omega}_m\rangle$ is abelian, thus all its subgroups (containing $\hat{\omega}_m$) are normal and the statement in (i) follows.

Assume now that ℓ divides m. The subgroup $\Theta_d\langle\hat{\omega}_m\rangle$ is normal in $\Delta\langle\hat{\omega}_m\rangle$ if and only if it is normalised by both Δ and $\hat{\omega}_m$. On the one hand, it is clear that $\hat{\omega}_m$ normalises $\Theta_d\langle\hat{\omega}_m\rangle$. And on the other hand, for a diamond automorphism $\delta \in \Delta$ the relation

$$\delta^{-1}\Theta_d\hat{\omega}_m\delta = \delta^{\ell-1}\Theta_d\hat{\omega}_m$$

from Proposition 2.13 implies that δ normalises $\Theta_d\langle\hat{\omega}_m\rangle$ if and only if $\delta^{\ell-1} \in \Theta_d$. Since this must happen for all $\delta \in \Delta$, the last condition is equivalent to saying that the index of Θ_d in Δ divides $\ell - 1$, hence (ii) is proved. □

5.2. The étale property. Let $e = e(D)$ be the positive integer defined by the recipe

$$e := \begin{cases} \left(1 + 2\left(\frac{B_D}{\mathbb{Q}(\sqrt{-3})}\right)\right)\left(1 + \left(\frac{B_D}{\mathbb{Q}(\sqrt{-1})}\right)\right) & \text{if } \ell > 3, \\ 1 + \left(\frac{B_D}{\mathbb{Q}(\sqrt{-1})}\right) & \text{if } \ell = 3, \end{cases} \tag{2.14}$$

where for a quadratic field F, we set $\left(\frac{B_D}{F}\right) = 1$ if F splits B_D and 0 otherwise. Notice that e divides 6, thus it clearly divides $(\ell^2 - 1)/2$. Put $d_{\text{ét}} := (\ell^2 - 1)/2e$. Jordan showed in [**Jor81**, Chapter 5] that the maximal étale quotient of $g : X_{D,\ell} \to X_D$ (the so-called *Shimura covering of X_D at ℓ*, see *loc. cit.* and [**Sko05**]) is the unique intermediate covering

$$g_{d_{\text{ét}}} : Y_{d_{\text{ét}}} \longrightarrow X_D$$

of degree $d_{\text{ét}}$. In particular, for a positive divisor d of $(\ell^2-1)/2$, the intermediate covering $g_d : Y_d \to X_D$ is étale[2] if and only if d divides $d_{\text{ét}}$.

Let d be a positive integer dividing $(\ell^2-1)/2$, and assume that $d \mid d_{\text{ét}}$, so that $g_d : Y_d \to X_D$ is a cyclic étale Galois covering of degree d. Assume moreover that the induced covering

$$g_d^{(m)} : Y_d^{(m)} \longrightarrow X_D^{(m)}$$

is Galois. By virtue of Corollary 2.20, this is equivalent to assuming that d divides $(\ell^2-1)/2n$, where

$$n := \begin{cases} e & \text{if } \ell \nmid m, \\ \operatorname{lcm}(e, (\ell+1)/2) & \text{if } \ell \mid m. \end{cases} \tag{2.15}$$

Observe that when ℓ divides m the cyclic subgroup $\Theta_{(\ell^2-1)/2n}$ of Δ contains the subgroup $\Theta_{\ell-1} \simeq \mathbb{F}_{\ell^2}^1/\{\pm 1\}$, which consists of all the diamond automorphisms in Δ that act trivially on the set of connected components of $X_{D,\ell} \times_{\mathbb{Q}} \mathbb{C}$.

THEOREM 2.21. *Let d be a positive integer dividing $(\ell^2-1)/2n$. The cyclic Galois covering $g_d^{(m)} : Y_d^{(m)} \to X_D^{(m)}$ is étale if either of the following conditions holds:*

(i) *ω_m is fixed point free,*
(ii) *$\ell \nmid m$, $(\frac{m}{\ell}) = 1$ and d divides $\ell - 1$,*
(iii) *$\ell \mid m$ and $(\frac{m/\ell}{\ell}) = -1$, or*
(iv) *d divides $(\ell^2-1)/4n$.*

PROOF. Write $g' : X_{D,\ell} \to Y_{(\ell^2-1)/2n}$. By the definition of n, the covering $g_d : Y_d \to X_D$ is étale, and the induced covering $g_d^{(m)} : Y_d^{(m)} \to X_D^{(m)}$ is Galois. When ω_m is fixed point free, the projection map $\pi_m : X_D \to X_D^{(m)}$ is étale, hence the commutative diagram

$$\begin{array}{ccc} Y_d & \xrightarrow{\text{ét}} & X_D \\ \downarrow & & \downarrow{\scriptstyle \text{ét}} \\ Y_d^{(m)} & \longrightarrow & X_D^{(m)} \end{array}$$

implies that $g_d^{(m)} : Y_d^{(m)} \to X_D^{(m)}$ is étale as well.

Now we show that $g_d^{(m)}$ is also étale if either (ii), (iii) or (iv) holds. If ω_m is fixed point free, then (i) applies, so we can assume that ω_m has fixed points. Let $Q \in X_D(\bar{\mathbb{Q}})$ be a fixed point of ω_m, and let $P \in X_{D,\ell}(\bar{\mathbb{Q}})$ be any point such that $g(P) = Q$. Then,

$$g(\hat{\omega}_m(P)) = \omega_m(g(P)) = \omega_m(Q) = Q,$$

thus $\hat{\omega}_m$ acts on the fibre $g^{-1}(Q)$. Since $g : X_{D,\ell} \to X_D$ is Galois, there exists a diamond automorphism $\delta_Q \in \Delta$, which depends only on Q, such that

$$\hat{\omega}_m(P) = \delta_Q(P) \quad \text{for every} \quad P \in g^{-1}(Q). \tag{2.16}$$

In particular, $\delta_Q^2(P) = \hat{\omega}_m^2(P) = P$ for every $P \in g^{-1}(Q)$. It follows that

$$\delta_Q^2 \in \Theta_{(\ell^2-1)/2n} \subseteq \Theta_d,$$

and hence δ_Q^2 induces the trivial automorphism of the covering $g_d : Y_d \to X_D$. Otherwise, the relation $\delta_Q'^2(g'(P)) = g'(P)$ in $Y_{(\ell^2-1)/2n}$, where δ_Q' is the class of δ_Q in $\Delta/\Theta_{(\ell^2-1)/2n}$, would prevent the action of $\Delta/\Theta_{(\ell^2-1)/2n}$ from being transitive on $g_{(\ell^2-1)/2n}^{-1}(Q)$, and this would contradict the fact that $g_{(\ell^2-1)/2n}$ is an étale Galois covering. Assume d divides $(\ell^2-1)/4n$. Then

$$\Theta_{(\ell^2-1)/2n} \subseteq \Theta_{(\ell^2-1)/4n} \subseteq \Theta_d,$$

thus it actually holds $\delta_Q \in \Theta_d$. Repeating the argument for all the fixed points $Q \in X_D(\bar{\mathbb{Q}})$ of ω_m, we deduce that all the corresponding diamond automorphisms δ_Q satisfying (2.16) belong to

[2]In a more technical parlance, $g_d : Y_d \to X_D$ is an X_D-torsor under the constant group scheme $\mathbb{Z}/d\mathbb{Z}$.

Θ_d. Therefore, every fibre of $g_d : Y_d \to X_D$ above a point $Q \in X_D(\bar{\mathbb{Q}})$ with $\omega_m(Q) = Q$ consists of exactly $d = \deg(g_d)$ points $P_1, \ldots, P_d$ which are all fixed by $\hat{\omega}_m$. In particular, the covering $g_d^{(m)} : Y_d^{(m)} \to X_D^{(m)}$ is étale when (iv) holds.

As for conditions (ii) and (iii), first observe that by the discussion in Section 4.1 the assumptions $(\frac{m}{\ell}) = 1$ and $(\frac{m/\ell}{\ell}) = -1$, respectively, are equivalent to saying that $\hat{\omega}_m$ acts trivially on the set of connected components $\mathcal{C}_\infty(D, \ell)$. Besides, the extra hypothesis $d \mid (\ell - 1)$ in (ii) and the definition of n in (iii) imply that $\Theta_{\ell-1} \subseteq \Theta_d$ in both cases.

Hence, under condition (ii) or (iii), repeating the above argument the equality (2.16) implies that δ_Q acts trivially on the set of connected components of $X_{D,\ell} \times_{\mathbb{Q}} \mathbb{C}$, since a diamond automorphism cannot fix only one connected component of $X_{D,\ell} \times_{\mathbb{Q}} \mathbb{C}$. This means that $\delta_Q \in \Theta_{\ell-1} \subseteq \Theta_d$, thus $g_d^{(m)}$ is an étale covering. □

6. Moduli interpretations

The Shimura curve X_D is the coarse moduli scheme over $\mathbb{Q}$ classifying abelian surfaces with quaternionic multiplication by $\mathcal{O}_D$. That is, a point $P \in X_D(\bar{\mathbb{Q}})$ corresponds to the $\bar{\mathbb{Q}}$-isomorphism class

$$[(A, \iota)] = \{(A', \iota')/\bar{\mathbb{Q}} : (A', \iota') \simeq (A, \iota)\}$$

of some QM-abelian surface $(A, \iota)/\bar{\mathbb{Q}}$. Recall that giving an isomorphism $(A', \iota') \simeq (A, \iota)$ amounts to giving an isomorphism $f : A' \to A$ between the underlying abelian surfaces such that

$$f \circ \iota'(\beta) = \iota(\beta) \circ f \quad \text{for all } \beta \in \mathcal{O}_D.$$

Now consider our distinguished prime ℓ dividing D, and the associated Shimura curve $X_{D,\ell}$. This curve admits a natural moduli interpretation as a covering of X_D, by adding a suitable level structure at ℓ, as we now describe.

Let (A, ι) be an abelian surface with QM by $\mathcal{O}_D$. The ℓ-torsion subgroup $A[\ell]$ of A contains a unique proper non-trivial $\mathcal{O}_D$-submodule (cf. [**Jor81**, p. 83]): indeed, if $I(\ell) \subseteq \mathcal{O}_D$ denotes the unique two-sided $\mathcal{O}_D$-ideal of reduced norm ℓ, then the only proper non-trivial $\mathcal{O}_D$-submodule of $A[\ell]$ is

$$A[I(\ell)] := \{x \in A : \iota(\beta)(x) = 0 \text{ for all } \beta \in I(\ell)\}.$$

One has isomorphisms

$$A[I(\ell)] \simeq \mathcal{O}_D/I(\ell) \simeq \mathcal{O}_{D,\ell}/I_\ell \simeq \mathbb{F}_{\ell^2},$$

hence $A[I(\ell)]$ is a free $\mathcal{O}_D/I(\ell)$-module of rank one; in particular, its order is ℓ^2.

Definition 2.22. *The torsion $\mathcal{O}_D$-module $C_\ell := A[I(\ell)]$ is called* canonical torsion subgroup of A at ℓ.

More generally, the *canonical torsion subgroup of A at m*, for each positive divisor m of D, is defined as

$$C_m := A[I(m)]] \subseteq A[m],$$

where $I(m)$ is the unique two-sided $\mathcal{O}_D$-ideal of reduced norm m. There is a natural isomorphism between C_m and $\mathcal{O}_D/I(m)$, and the order of C_m is m^2. Because of their uniqueness, notice that the canonical torsion subgroups of A are rational over the same fields over which A is.

The Shimura curve $X_{D,\ell}$ is the coarse moduli space over $\mathbb{Q}$ for triplets (A, ι, x_ℓ), where (A, ι) is a QM-abelian surface and x_ℓ is a generator of its canonical torsion subgroup C_ℓ as an $\mathcal{O}_D/I(\ell)$-module via ι. This way, a point $Q \in X_{D,\ell}(\bar{\mathbb{Q}})$ corresponds to the isomorphism class

$$[(A, \iota, x_\ell)] = \{(A', \iota', x'_\ell)/\bar{\mathbb{Q}} : (A', \iota', x'_\ell) \simeq (A, \iota, x_\ell)\}$$

of some triplet $(A, \iota, x_\ell)/\bar{\mathbb{Q}}$, where now an isomorphism of triplets $(A', \iota', x'_\ell) \simeq (A, \iota, x_\ell)$ means an isomorphism of QM-abelian surfaces $(A', \iota') \to (A, \iota)$ sending x'_ℓ to x_ℓ. Taking into account the

moduli interpretations of both X_D and $X_{D,\ell}$, the cyclic covering $X_{D,\ell} \to X_D$ becomes the forgetful map

$$[(A, \iota, x_\ell)] \longmapsto [(A, \iota)]. \tag{2.17}$$

In other words, the fibre of a point $P = [(A, \iota)] \in X_D(\bar{\mathbb{Q}})$ under (2.17) describes all the non-isomorphic choices of a generator for the canonical torsion subgroup C_ℓ as an $\mathcal{O}_D$-module.

The action of the automorphism group Δ of this cyclic Galois covering can also be described in terms of the above moduli problem. From the isomorphism of $\mathcal{O}_D$-modules

$$C_\ell \simeq \mathcal{O}_D/I(\ell) \simeq \mathcal{O}_{D,\ell}/I_\ell \simeq \mathbb{F}_{\ell^2},$$

we have an isomorphism

$$(\mathcal{O}_D/I(\ell))^\times \simeq \mathcal{O}_{D,\ell}^\times/(1+I_\ell) \xrightarrow{\simeq} \mathrm{Aut}(C_\ell) \simeq \mathbb{F}_{\ell^2}^\times, \quad [\alpha] \longmapsto \iota(\alpha), \tag{2.18}$$

and as a consequence $\Delta \simeq \mathrm{Aut}(C_\ell)/\{\pm 1\}$. Given an arbitrary diamond automorphism $\delta \in \Delta$, we let $\alpha_\delta \in \mathcal{O}_D$, $\alpha_\delta \notin I(\ell)$, be any element such that $\iota(\alpha_\delta) \in \mathrm{Aut}(C_\ell)$ corresponds to δ under the previous isomorphisms. Then, the action of δ on the curve $X_{D,\ell}$ is described in moduli-theoretic terms by the rule

$$P = [(A, \iota, x_\ell)] \longmapsto \delta(P) := [(A, \iota, \iota(\alpha_\delta)(x_\ell))].$$

Since the triplets (A, ι, x_ℓ) and $(A, \iota, -x_\ell)$ are clearly isomorphic, this description of δ acting on the moduli problem associated with $X_{D,\ell}$ does not depend on the choice of the element α_δ.

Concerning the action of the Atkin-Lehner involutions, let us first recall the interpretation of ω_m on X_D for a fixed positive divisor m of D. The Atkin-Lehner group W_D is defined globally as the quotient

$$\mathrm{Norm}_{B_{D,+}^\times}(\mathcal{O}_D)/\mathbb{Q}^\times\mathcal{O}_D^\times,$$

and we can choose as a representative of $\omega_m \in W_D$ any generator $w_m \in \mathcal{O}_D$ of the two-sided ideal $I(m)$, with $\mathrm{n}(w_m) = m$. Then, the action of ω_m on the moduli problem associated with X_D is described by the rule (cf. Section 3.4 of Chapter 1)

$$P = [(A, \iota)] \longmapsto \omega_m(P) = [(A, \iota_m)]. \tag{2.19}$$

Now assume that (A, ι, x_ℓ) is an abelian surface with QM by $\mathcal{O}_D$ together with a generator x_ℓ of C_ℓ. Since w_m normalises the maximal order $\mathcal{O}_D$ and $I(\ell)$ is the unique two-sided ideal of reduced norm ℓ, we deduce that

$$w_m^{-1} I(\ell) w_m = I(\ell). \tag{2.20}$$

Therefore, the canonical torsion subgroup C_ℓ of A at ℓ is the same for the pairs (A, ι) and (A, ι_m). Moreover, (2.20) also implies that for any $\beta \in \mathcal{O}_D$ we have

$$\iota_m(\beta)(x_\ell) = 0 \iff w_m^{-1}\beta w_m \in I(\ell) \iff \beta \in I(\ell).$$

In other words, x_ℓ is still a generator for the canonical torsion subgroup C_ℓ regarded as an $\mathcal{O}_D/I(\ell)$-module via the *twisted* quaternionic action ι_m. Then, by using the moduli interpretation of $X_{D,\ell}$ the rule

$$[(A, \iota, x_\ell)] \longmapsto [(A, \iota_m, x_\ell)]$$

defines an automorphism

$$\tilde{\omega}_m : X_{D,\ell} \longrightarrow X_{D,\ell}.$$

By standard moduli considerations, $\tilde{\omega}_m$ is defined over $\mathbb{Q}$, and it is clear by construction that $\tilde{\omega}_m$ lifts the Atkin-Lehner involution ω_m on X_D. In contrast to $\hat{\omega}_m$, observe that $\tilde{\omega}_m$ is not necessarily an involution: an isomorphism of pairs between (A, ι) and $\omega_m^2(A, \iota)$ does not need to fix x_ℓ.

However, from the fact that both $\hat{\omega}_m$ and $\tilde{\omega}_m$ lift the Atkin-Lehner involution ω_m, it follows that they differ by a diamond automorphism, that is to say,

$$\delta_m := \hat{\omega}_m \tilde{\omega}_m^{-1} \in \Delta.$$

In particular, $\tilde{\omega}_m = \delta_m^{-1}\hat{\omega}_m \in \mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$. The Atkin-Lehner involution $\hat{\omega}_m$ on $X_{D,\ell}$ admits then the following moduli-theoretic description:

$$\hat{\omega}_m : [(A,\iota,x_p)] \longmapsto [(A,\iota_m,\iota_m(\alpha_{\delta_m})(x_p))] = \delta_m([(A,\iota_m,x_p)]).$$

That is, the involution $\hat{\omega}_m$ acts on a triplet (A,ι,x_ℓ) by twisting the quaternionic multiplication and then applying a suitable diamond automorphism.

6.1. Analogies with classical modular curves. The cyclic covering of Shimura curves $X_{D,\ell} \to X_D$ associated with the prime ℓ bears a strong resemblance to the covering of classical (affine) modular curves $Y_1(\ell) \to Y_0(\ell)$. Here

$$Y_0(\ell) = \Gamma_0(\ell) \setminus \mathcal{H} \quad \text{and} \quad Y_1(\ell) = \Gamma_1(\ell) \setminus \mathcal{H}$$

are the (non-compact) complex Riemann surfaces obtained as quotients of the upper half plane $\mathcal{H}$ by the usual congruence subgroups

$$\Gamma_0(\ell) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \ell \mid c \right\}, \quad \Gamma_1(\ell) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \ell \mid c,\ a,b \equiv 1 \pmod{\ell} \right\}$$

of $\mathrm{SL}_2(\mathbb{Z})$, respectively. The moduli space for the congruence subgroup $\Gamma_0(\ell)$ is the set of isomorphism classes of pairs (E,C), where E is an elliptic curve and C is a subgroup of E of order ℓ. Similarly, the moduli space for $\Gamma_1(\ell)$ is the set of isomorphism classes of elliptic curves (E,Q) together with a point Q of order ℓ. Then, the natural covering

$$Y_1(\ell) \longrightarrow Y_0(\ell)$$

induced by the inclusion $\Gamma_1(\ell) \subseteq \Gamma_0(\ell)$ is described in moduli-theoretic terms by the rule

$$[(E,Q)] \longmapsto [(E,\langle Q \rangle)].$$

After compactifying the curves $Y_0(\ell)$ and $Y_1(\ell)$, the maximal étale intermediate covering of the resulting natural map $X_1(\ell) \to X_0(\ell)$ is referred to as its *Shimura covering* in the literature (see [**Maz77**, pp. 67, 99]).

The moduli problems associated with $Y_0(\ell)$ and $Y_1(\ell)$ can be posed over an arbitrary base ring R, and for $\ell > 3$ the corresponding moduli functors are representable by a smooth affine curve over $\mathbb{Z}$, leading to models over $\mathbb{Q}$ for the curves $Y_0(\ell)$ and $Y_1(\ell)$. However, special care must be taken in the case of $Y_1(\ell)$, because it can be endowed with two different $\mathbb{Q}$-structures. This fact relies on the difference between *naive* and *arithmetic* level ℓ structures on an elliptic curve in the language of Katz [**Kat76**, Chapter II] (see also [**DI95**, Variant 8.2.2, p. 70]).

Given an elliptic curve E over a base ring R, let $E[\ell]$ be the (scheme-theoretic) ℓ-torsion subgroup of E. Then $E[\ell]$ is a finite and flat commutative group-scheme over R of rank ℓ^2, and the Weil pairing

$$e_\ell : E[\ell] \times E[\ell] \longrightarrow \mu_\ell$$

identifies $E[\ell]$ with its own Cartier dual, where μ_ℓ denotes the group-scheme of ℓ-th roots of unity. A *naive level ℓ structure* on E/R is then an isomorphism of R-schemes

$$\alpha : \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z} \xrightarrow{\simeq} E[\ell],$$

and note that the existence of such an isomorphism implies that ℓ is invertible in R. The determinant of α is by definition the ℓ-th root of unity

$$\det(\alpha) := e_\ell(\alpha(1,0),\alpha(0,1)).$$

Following Katz, a pair (E,α) as above is called a *naive level ℓ curve*, or a $\Gamma(\ell)^{naive}$*-curve*. Besides, an *arithmetic level ℓ structure* on E/R is an isomorphism of R-schemes

$$\beta : \mu_\ell \times \mathbb{Z}/\ell\mathbb{Z} \xrightarrow{\simeq} E[\ell]$$

under which e_ℓ becomes the standard symplectic autoduality of $\mu_\ell \times \mathbb{Z}/\ell\mathbb{Z}$, i.e. such that

$$e_\ell(\beta(\zeta_1,n_1),\beta(\zeta_2,n_2)) = \zeta_1^{n_2}/\zeta_2^{n_1} \quad \text{for all } \zeta_1,\zeta_2 \in \mu_\ell,\ n_1,n_2 \in \mathbb{Z}/\ell\mathbb{Z}.$$

A pair (E, β) as above is referred to as an *arithmetic level ℓ curve*, or as a $\Gamma(\ell)^{arith}$*-curve*.

When ℓ is invertible in R, a naive level ℓ structure α determines both an ℓ-th root of unity $\det(\alpha)$ and an arithmetic level ℓ structure β_α described by the rule

$$\beta_\alpha(\det(\alpha)^m, n) = \alpha(m, n).$$

In fact, there is a bijection

$$\begin{array}{rcl} \{\text{naive level } \ell \text{ structures on } E/R\} & \longrightarrow & \mu_\ell(R) \times \{\text{arith. level } \ell \text{ structures on } E/R\} \\ \alpha & \longmapsto & (\det(\alpha), \beta_\alpha). \end{array}$$

Also, an arithmetic level ℓ structure β can be regarded as a pair of inclusions

$$\beta_1 : \mu_\ell \hookrightarrow E[\ell], \quad \beta_2 : \mathbb{Z}/\ell\mathbb{Z} \hookrightarrow E[\ell]$$

satisfying the compatibility condition $e_\ell(\beta_1(\zeta), \beta_2(n)) = \zeta^n$. Then, it makes sense to define a $\Gamma_1(\ell)^{arith}$-structure on E/R to be an inclusion

$$i : \mu_\ell \longrightarrow E[\ell],$$

and a $\Gamma_1(\ell)^{naive}$-structure on E/R to be an inclusion

$$j : \mathbb{Z}/\ell\mathbb{Z} \longrightarrow E[\ell]$$

(Katz uses the terms $\Gamma_{00}(\ell)^{arith}$*-structures* and $\Gamma_{00}(\ell)^{naive}$*-structures* in [**Kat76**]).

For odd primes ℓ, the contravariant functor from the category of rings to the category of sets

$$\mathcal{F}(\ell)^{arith} : \text{Rings} \longrightarrow \text{Sets}$$

defined as

$$\begin{array}{rcl} R & \rightsquigarrow & \mathcal{F}(\ell)^{arith}(R) := \text{set of isomorphism classes of } \Gamma(\ell)^{arith}\text{-structures over } R, \\ f : R \to S & \rightsquigarrow & \mathcal{F}(\ell)^{arith}(f) : \mathcal{F}(\ell)^{arith}(S) \to \mathcal{F}(p)^{arith}(R) \text{ (base-change)} \end{array}$$

is represented by a smooth affine curve $\mathcal{Y}(\ell)^{arith}$ over $\mathbb{Z}$, with geometrically irreducible fibres, and the similarly defined functor $\mathcal{F}(\ell)^{naive}$ is represented by $\mathbb{Z}[1/\ell, \zeta_\ell] \otimes_{\mathbb{Z}} \mathcal{Y}(\ell)^{arith}$.

For primes $\ell > 3$, the analogous functors $\mathcal{F}_1(\ell)^{arith}$ and $\mathcal{F}_1(\ell)^{naive}$ are both represented by smooth affine curves $\mathcal{Y}_1(\ell)^{arith}$ and $\mathcal{Y}_1(\ell)^{naive}$ over $\mathbb{Z}$, with geometrically irreducible fibres. However, although $\mathcal{Y}_1(\ell)^{arith}$ and $\mathcal{Y}_1(\ell)^{naive}$ are isomorphic as affine schemes over $\mathbb{Z}[\zeta_\ell]$, they are not isomorphic as affine $\mathbb{Z}$-schemes. In particular, the models $\mathcal{Y}_1(\ell)^{arith} \otimes_{\mathbb{Z}} \mathbb{Q}$ and $\mathcal{Y}_1(\ell)^{naive} \otimes_{\mathbb{Z}} \mathbb{Q}$ of the modular curve $Y_1(\ell)$ are not isomorphic, hence they induce different $\mathbb{Q}$-structures on $Y_1(\ell)$, even though $\mathcal{Y}_1(\ell)^{arith} \otimes_{\mathbb{Z}} \mathbb{Q}(\mu_\ell)$ and $\mathcal{Y}_1(\ell)^{naive} \otimes_{\mathbb{Z}} \mathbb{Q}(\mu_\ell)$ are isomorphic as $\mathbb{Q}(\mu_\ell)$-models of $Y_1(\ell)$.

The same moduli-theoretic method becomes a subtler one for the case of $Y_0(\ell)$, because of the torsion in $\Gamma_0(\ell)$. Alternatively, one can proceed as in [**DI95**, p. 71]. Let us write $\mathcal{F}_1(\ell)$ (resp. $\mathcal{Y}_1(\ell)$) for the *arithmetic* instance of the above functor (resp. of the above affine $\mathbb{Z}$-scheme). For each integer d not divisible by ℓ, the natural transformation $\mathcal{F}_1(\ell) \to \mathcal{F}_1(\ell)$ defined by

$$(E, i : \mu_\ell \hookrightarrow E[\ell]) \longmapsto (E, i^d)$$

induces an automorphism of $\mathcal{Y}_1(\ell)$, depending only on d modulo ℓ, which we denote by $\langle d \rangle$. Then, the map $d \mapsto \langle d \rangle$ induces a homomorphism

$$\mathbb{F}_\ell^\times \longrightarrow \text{Aut}(\mathcal{Y}_1(\ell)),$$

i.e. an action of $\mathbb{F}_\ell^\times$ on $\mathcal{Y}_1(\ell)$. Then, one can define $\mathcal{Y}_0(\ell)$ to be the quotient scheme of $\mathcal{Y}_1(\ell)$ by the action of $\mathbb{F}_\ell^\times$ by automorphisms. Then $\mathcal{Y}_0(\ell)$ is a smooth scheme over $\mathbb{Z}[1/\ell]$, and the natural projection $\mathcal{Y}_1(\ell) \to \mathcal{Y}_0(\ell)$ is finite and flat, but not necessarily étale. Moreover, the functor corresponding to the moduli problem associated to $Y_0(\ell)$ is represented by $\mathcal{Y}_0(\ell)$, so that $\mathcal{Y}_0(\ell) \otimes_{\mathbb{Z}[1/\ell]} \mathbb{Q}$ is a model over $\mathbb{Q}$ for $Y_0(\ell)$. The automorphisms $\langle d \rangle$ are described in terms of moduli by the rule

$$(E, Q) \longmapsto (E, d \cdot Q)$$

and they act as covering automorphisms on $\mathcal{Y}_1(\ell) \to \mathcal{Y}_0(\ell)$. These automorphisms are often referred to as *diamond automorphisms* in the literature, thus the analogy with the moduli interpretation of the covering automorphisms of $X_{D,\ell} \to X_D$ justifies our terminology for the elements $\delta \in \Delta$.

Attached to the prime ℓ, there is also an Atkin-Lehner involution

$$\omega_\ell : \mathcal{Y}_1(\ell) \longrightarrow \mathcal{Y}_1(\ell)$$

acting on $\mathcal{Y}_1(\ell)$ and admitting the following moduli-theoretic interpretation. Suppose (E, Q) is an elliptic curve together with a point $Q \in E[\ell]$ of exact order ℓ, and let

$$\pi : E \longrightarrow E/\langle Q \rangle$$

be the natural quotient map. After the choice of a primitive ℓ-th root of unity ζ_ℓ, there is a unique point $Q' \in E[\ell]$ modulo $\langle Q \rangle$ such that $e_\ell(Q, Q') = \zeta_\ell$. Then $\pi(Q')$ is a point of exact order ℓ in $E/\langle Q \rangle$, and the action of ω_ℓ is described by the rule

$$\omega_\ell : [(E, Q)] \ \longmapsto \ [(E/\langle Q \rangle, \pi(Q'))].$$

Next we give an alternative moduli interpretation of the Atkin-Lehner involutions of X_D which illustrates better the analogy between their lifts to $X_{D,\ell}$ and the involution ω_ℓ acting on $Y_1(\ell)$.

Let m be a positive divisor of D, and $\omega_m : X_D \to X_D$ be the associated Atkin-Lehner involution on X_D. As before, choose a generator $w_m \in \mathcal{O}_D$ of the two-sided $\mathcal{O}_D$-ideal $I(m)$ of reduced norm m, with $\mathrm{n}(w_m) = m$, as a representative of $\omega_m \in W_D$. If (A, ι) is an abelian surface with QM by $\mathcal{O}_D$, then the kernel of the endomorphism

$$\iota(w_m) : A \longrightarrow A$$

is precisely C_m, the canonical torsion subgroup of A at m, hence $\iota(w_m)$ induces an isomorphism of pairs between $(A/C_m, \iota'_m)$ and (A, ι_m), where here

$$\iota'_m : \mathcal{O}_D \ \hookrightarrow \ \mathrm{End}(A/C_m), \quad \beta \ \longmapsto \ \iota(w_m^{-2}\beta w_m^2).$$

Remark 2.23. Observe that $w_m^2 \in \mathbb{Q}^\times \mathcal{O}_D^\times$, thus

$$\iota(w_m^{-2}\beta w_m^2) = \iota(u^{-1}\beta u) = \iota(u)^{-1}\iota(\beta)\iota(u)$$

for some $u \in \mathcal{O}_D^\times$, and notice that $\iota(u)$ is an automorphism of A. If $\mathrm{tr}(w_m) = 0$, i.e. $w_m^2 = -m$, then $\iota'_m(\beta)$ is just the endomorphism $A/C_m \to A/C_m$ induced by $\iota(\beta)$.

Therefore, the Atkin-Lehner involution ω_m on X_D can also be interpreted on the moduli-theoretic side by the rule

$$\omega_m : [(A, \iota)] \ \longmapsto \ [(A/C_m, \iota'_m)].$$

Now using the natural isomorphism of pairs

$$(A/C_m, \iota'_m) \ \xrightarrow{\simeq} \ (A, \iota_m)$$

given by $\iota(w_m)$, the automorphism $\tilde{\omega}_m$ on $X_{D,\ell}$ can be expressed by the rule

$$\tilde{\omega}_m : [(A, \iota, x_\ell)] \ \longmapsto \ [(A/C_m, \iota'_m, y_{\ell,m} + C_m)] \quad (= [(A, \iota_m, x_\ell)]),$$

where $y_{\ell,m} \in A$ is any point such that $\iota(w_m)(y_{\ell,m}) = x_\ell$. The point $y_{\ell,m} + C_m$ is well-defined, and it is an easy exercise to check that $y_{\ell,m} + C_m$ is an ℓ-torsion point in A/C_m generating $(A/C_m)[I(\ell)]$ via ι'_m. Finally, the lifted Atkin-Lehner involution $\hat{\omega}_m$ acts by the recipe

$$\hat{\omega}_m : [(A, \iota, x_\ell)] \ \longmapsto \ \delta_m([(A/C_m, \iota'_m, y_{\ell,m} + C_m)]) = [(A/C_m, \iota'_m, \iota'_m(\alpha_{\delta_m})(y_{\ell,m} + C_m))],$$

where $\delta_m \in \Delta$ is the diamond automorphism introduced before. This alternative description for $\hat{\omega}_m$ makes apparent the strong resemblance to the Atkin-Lehner involution ω_ℓ on the modular curve $Y_1(\ell)$, but there is a remarkable difference: the canonical torsion subgroup $C_m \subseteq A[m]$ plays the role of the order ℓ subgroup $\langle Q \rangle \subseteq E[\ell]$, but C_m is the kernel of the endomorphism $\iota(w_m) : A \to A$, whereas the subgroup $\langle Q \rangle \subseteq E[\ell]$ is not the kernel of any endomorphism of E.

CHAPTER 3

Local points on Shimura coverings at bad reduction primes

Let $X_D/\mathbb{Q}$ be the Shimura curve associated to a maximal order $\mathcal{O}_D$ in an indefinite rational quaternion algebra B_D of reduced discriminant D, and fix an odd prime $\ell > 3$ dividing D. This chapter is devoted to the study of the existence of local points at primes of bad reduction on the intermediate curves of the cyclic Galois covering $X_{D,\ell} \to X_D$ described in Chapter 2 and their Atkin-Lehner quotients.

Writing $\mathcal{U}_D$ for the compact open subgroup of $\widehat{\mathcal{O}}_D^\times$ defining the Shimura curve $X_{D,\ell}$, recall that there is a unique intermediate cyclic Galois covering

$$Y_d \longrightarrow X_D$$

for each positive divisor d of $(\ell^2-1)/2$. Namely, the curve $Y_d/\mathbb{Q}$ is the Shimura curve corresponding to the unique intermediate compact open subgroup $\mathcal{U}_D \subseteq U_d \subseteq \widehat{\mathcal{O}}_D^\times$ of index d in $\widehat{\mathcal{O}}_D^\times$. Equivalently, under the choice of an isomorphism $\widehat{\mathcal{O}}_D^\times/\mathcal{U}_D \simeq \mathbb{F}_{\ell^2}^\times$, the curve Y_d corresponds to the unique subgroup $H_d \subseteq \mathbb{F}_{\ell^2}^\times$ of index d. In Chapter 2 we have studied the geometry of these coverings and the group of modular automorphisms of the Shimura curves Y_d, which is described as a semidirect product of the group of covering automorphisms of $Y_d \to X_D$ with the group of lifted Atkin-Lehner involutions from X_D to Y_d. In particular, if ω_m denotes the Atkin-Lehner involution on X_D attached to a positive divisor m of D and $\hat{\omega}_m$ is the corresponding lifted involution on Y_d, then we have an induced covering

$$Y_d^{(m)} := Y_d/\langle\hat{\omega}_m\rangle \longrightarrow X_D^{(m)} := X_D/\langle\omega_m\rangle.$$

The purpose of this chapter is to study the existence of local points at primes p dividing D/ℓ on the curves Y_d and their Atkin-Lehner quotients. Curves Y_d have bad reduction at these primes, and we therefore require the theory of Čerednik and Drinfeld on the p-adic uniformisation of Shimura curves to describe the formal completion along the closed fibre of the $\mathbb{Z}_p$-integral models of the curves $Y_d \times_{\mathbb{Q}} \mathbb{Q}_p$ as quotients of Drinfeld's p-adic upper half plane in the category of formal schemes. After a brief review of the geometry and the arithmetic of the intermediate curves of the covering $X_{D,\ell} \to X_D$ in Section 1, we devote Section 2 to present this theory, following mainly [**BC91**] and with special emphasis on the algebraisation of these formal schemes.

In order to state the main results of the chapter, to be proved in Sections 3 and 4, fix a positive divisor d of $(\ell^2-1)/2$, write as above H_d for the unique index d subgroup of $\mathbb{F}_{\ell^2}^\times$ and set also $t_d := |H_d| = (\ell^2-1)/d$. Even in the cases where Y_d is not geometrically connected, so that its geometric connected components are defined over a non-trivial cyclic extension of $\mathbb{Q}$ (cf. Section 1.2 below), it may be the case that the geometric connected components of $Y_d \times_{\mathbb{Q}} \mathbb{Q}_p$ are defined over $\mathbb{Q}_p$. When this happens, we say that Y_d *decomposes completely over* $\mathbb{Q}_p$. If this does not occur, one can prove the non-existence of rational points over $\mathbb{Q}_p$ (and in fact, over infinitely many extensions $K/\mathbb{Q}_p$) on Y_d by elementary Galois-theoretic arguments. We refer the reader to Section 3.1 for the details. In contrast, when Y_d decomposes completely over $\mathbb{Q}_p$, we need to invoke Čerednik-Drinfeld theory to describe a $\mathbb{Z}_p$-integral model $\mathcal{Y}_d$ of $Y_d \times_{\mathbb{Q}} \mathbb{Q}_p$ as a finite disjoint union of quadratic twists of Mumford curves. Namely, if $c_\infty(d)$ is the number of geometric connected components of Y_d, there is a discrete cocompact subgroup $\Gamma_d \subseteq \mathrm{GL}_2(\mathbb{Q}_p)$ (obtained from the definite quaternion algebra whose local invariants at p and ∞ are the opposite from those of B_D)

such that

$$\mathcal{Y}_d \simeq \coprod_{i=1}^{c_\infty(d)} \mathcal{Y}_{\Gamma_d}, \tag{3.1}$$

where $\mathcal{Y}_{\Gamma_d}/\mathbb{Z}_p$ is a quadratic twist of the Mumford curve[1] $\mathcal{M}_{\Gamma_{d,+}}/\mathbb{Z}_p$ associated with an index two subgroup $\Gamma_{d,+}$ of Γ_d.

In particular, $\mathcal{Y}_{\Gamma_d}$ is an admissible curve over $\mathbb{Z}_p$ in the sense of Definition 1.65, and the existence of $\mathbb{Q}_p$-rational points on $\mathcal{Y}_{\Gamma_d}$ (hence on Y_d) can be tackled via Hensel's lemma by studying the combinatorics of its dual graph. In Section 3 we prove the following statement (cf. Proposition 3.32 and Corollary 3.34):

THEOREM 3.1. *Assume that Y_d decomposes completely over $\mathbb{Q}_p$. Let $K/\mathbb{Q}_p$ be a finite extension, and write $f_K := f(K/\mathbb{Q}_p)$, $e_K := e(K/\mathbb{Q}_p)$. Then:*

a) *If f_K is even, then $Y_d(K) \neq \emptyset$.*
b) *If f_K is odd and e_K is even, then $Y_d(K) \neq \emptyset$ if and only if one of the following conditions holds:*
   i) *$\mathbb{Q}(\sqrt{-p})$ splits $B_{D/p}$ and $4 \mid t_d$,*
   ii) *$p = 2$, $4 \mid t_d$, $\mathbb{Q}(\sqrt{-1})$ splits $B_{D/p}$ and H_d contains a root of $x^2 + 2x + 2 = 0$, or*
   iii) *$p = 3$, $6 \mid t_d$, $\mathbb{Q}(\sqrt{-3})$ splits $B_{D/p}$ and H_d contains a root of $x^2 + 3x + 3 = 0$.*
c) *If both f_K and e_K are odd, then $Y_d(K) \neq \emptyset$ if and only if $p = 2$, every prime dividing $D/2$ is congruent to 3 mod 4 (in particular, $\ell \equiv 3 \mod 4$), $4 \mid t_d$ and either $\mathbb{Q}(\sqrt{-2})$ splits $B_{D/p}$ or H_d contains a root of $x^2 + 2x + 2$.*

Combining this result with the work of Jordan and Livné in [**JL85**], we can find examples where $X_D(K) \neq \emptyset$ but $Y_d(K) = \emptyset$ (cf. Corollaries 3.35 and 3.36 below).

After proving the previous theorem, in Section 4 we focus on the existence of $\mathbb{Q}_p$-rational points on the Atkin-Lehner quotients of the curves Y_d. Suppose that $Y_d(\mathbb{Q}_p)$ is empty (as otherwise $\mathbb{Q}_p$-rational points obviously exist in every Atkin-Lehner quotient of Y_d), and choose a positive divisor m of D. Similarly as above, if Y_d does not decompose completely over $\mathbb{Q}_p$ or $\hat{\omega}_m$ does not act trivially on the set of geometric connected components of Y_d, then one can easily predict the emptiness of $Y_d^{(m)}(\mathbb{Q}_p)$ in many instances. Thus we may assume that Y_d decomposes completely over $\mathbb{Q}_p$, and further that $\hat{\omega}_m$ acts as an involution on each geometric connected component of Y_d. Notice that this is clearly the case if Y_d is already geometrically connected.

In this setting, a $\mathbb{Z}_p$-integral model of $Y_d^{(m)}$ is given from (3.1) as the union of $c_\infty(d)$ copies of the quotient of $\mathcal{Y}_{\Gamma_d}$ by the action induced by $\hat{\omega}_m$. In this way, the existence of $\mathbb{Q}_p$-rational points on $Y_d^{(m)}$ can be characterised by studying the action of $\hat{\omega}_m$ on the dual graph of the $\mathbb{Z}_p$-admissible curve $\mathcal{Y}_{\Gamma_d}$.

When $m = p$, the quotient of $\mathcal{Y}_{\Gamma_d}$ by $\hat{\omega}_p$ is isomorphic to the (untwisted) Mumford curve $\mathcal{M}_{\Gamma_d}/\mathbb{Z}_p$ associated with Γ_d, and by studying the dual graph of this curve we deduce the criterion for the existence of $\mathbb{Q}_p$-rational points on $Y_d^{(p)}$ (cf. Section 4.2):

THEOREM 3.2. *Assume that Y_d decomposes completely over $\mathbb{Q}_p$. Then the set $Y_d^{(p)}(\mathbb{Q}_p)$ is not empty if and only if any of the following conditions holds:*

i) *$\mathbb{Q}(\sqrt{-1})$ splits $B_{D/p}$ and $4 \mid t_d$,*
ii) *$\mathbb{Q}(\sqrt{-3})$ splits $B_{D/p}$ and $6 \mid t_d$,*
iii) *$\mathbb{Q}(\sqrt{-p})$ splits $B_{D/p}$ and $4 \mid t_d$,*

In contrast, when $m \neq p$ the criterion for the existence of $\mathbb{Q}_p$-rational points on the curve $Y_d^{(m)}$ is deduced in Sections 4.3 and 4.4 by studying the action of the lifted Atkin-Lehner involutions induced on the dual graph of $\mathcal{Y}_{\Gamma_d}$. The next result summarises Theorems 3.60 and 3.64:

[1] Strictly speaking, if the image of $\Gamma_{d,+}$ in $\mathrm{PGL}_2(\mathbb{Q}_p)$ is not a Schottky subgroup, then $\mathcal{M}_{\Gamma_{d,+}}$ is not a Mumford curve, but rather a quotient of a Mumford curve by a finite group. Some authors use the term *Mumford quotient* instead.

THEOREM 3.3. *Assume that Y_d decomposes completely over $\mathbb{Q}_p$ and $Y_d(\mathbb{Q}_p) = \emptyset$. Let $m > 1$ be a positive divisor of D/p and assume that $\hat{\omega}_m$ acts trivially on the set of geometric connected components of Y_d. Then:*

1) *$Y_d^{(m)}(\mathbb{Q}_p)$ is not empty if and only if one of the following conditions holds:*
   - i) *$B_{D/p} \simeq (-m, -p)_{\mathbb{Q}}$, and either*
     - a) *$4 \mid t_d$, or*
     - b) *$p = 3$, $\ell \mid m$, $6 \mid t_d$ and H_d contains a root of $x^2 + 3x + 3 = 0$.*
   - ii) *$B_{D/p} \simeq (-mp, -1)_{\mathbb{Q}}$ and $4 \mid t_d$.*
2) *$Y_d^{(pm)}(\mathbb{Q}_p)$ is not empty if and only if one of the following conditions holds:*
   - i) *$\mathbb{Q}(\sqrt{-m})$ splits $B_{D/p}$, and either*
     - a) *$\ell \mid m$ or $4 \mid t_d$, or*
     - b) *$m = 3$, $6 \mid t_d$ and $s_3 H_d$ contains a root of $x^2 + 3x + 3 = 0$, where $s_3 \in \mathbb{F}_{\ell^2}^\times$ is a square root of $3 \mod \ell$.*
   - ii) *$m = 2$, $4 \mid t_d$, $\mathbb{Q}(\sqrt{-1})$ splits $B_{D/p}$ and $s_2 H_d$ contains a root of $x^2 + 2x + 2 = 0$, where $s_2 \in \mathbb{F}_{\ell^2}^\times$ is a square root of $2 \mod \ell$.*

We have not tackled the existence of $\mathbb{Q}_p$-rational points on the intermediate curves Y_d of the covering $X_{D,\ell} \to X_D$ and their Atkin-Lehner quotients when $p = \ell$. The main difference with the case $p \neq \ell$ is that one needs to apply Čerednik-Drinfeld theory for Shimura curves with level structure at p (that is to say, the subgroups $U \subseteq \widehat{\mathcal{O}}_D^\times$ to be considered are not maximal at p anymore), which requires to replace Drinfeld's p-adic upper half plane by certain étale Galois coverings of it (cf. [**BC91**, III.5.7], [**Dri76**], or also [**Tei90**]). We content ourselves here to mention that using the work of Teitelbaum in [**Tei90**] it can be shown that the curves Y_d fail to have $\mathbb{Q}_\ell$-rational points very frequently. More details will appear in [**Vera**].

1. Shimura coverings of X_D

As before, we fix once and for all a prime $\ell > 3$ dividing D and consider the cyclic Galois covering of Shimura curves $X_{D,\ell} \to X_D$. Recall that the group $\Delta := \mathrm{Aut}(X_{D,\ell}/X_D)$ is isomorphic to the quotient $\widehat{\mathcal{O}}_D^\times/\{\pm 1\}\mathcal{U}_D$, which in turn is isomorphic to $\mathcal{O}_{D,\ell}^\times/\{\pm 1\}(1+I_\ell)$ because $\mathcal{U}_D$ is locally maximal outside ℓ. As in (2.1), we can regard $\mathcal{O}_{D,\ell}$ as a matrix subring of $\mathrm{M}_2(\mathbb{Z}_{\ell^2})$,

$$\mathcal{O}_{D,\ell} = \left\{ \begin{pmatrix} x & y \\ \ell\bar{x} & \bar{y} \end{pmatrix} : x, y \in \mathbb{Z}_{\ell^2} \right\} \subseteq \mathrm{M}_2(\mathbb{Z}_{\ell^2}),$$

where $x \mapsto \bar{x}$ denotes the non-trivial automorphism in $\mathrm{Gal}\,(\mathbb{Q}_{p^2}/\mathbb{Q}_p)$, and the Nebentypus character (2.6) induces an isomorphism

$$\varphi : \mathcal{O}_{D,\ell}^\times/(1 + I_\ell) \xrightarrow{\simeq} \mathbb{F}_{\ell^2}^\times \tag{3.2}$$

by setting

$$\varphi(\gamma) := x \bmod \ell\mathbb{Z}_{\ell^2} \in \mathbb{F}_{\ell^2}^\times \quad \text{if} \quad \gamma = \begin{pmatrix} x & y \\ \ell\bar{x} & \bar{y} \end{pmatrix}.$$

Therefore, φ provides an isomorphism between Δ and $\mathbb{F}_{\ell^2}^\times/\{\pm 1\}$. Furthermore, notice that if $\gamma \in \mathcal{O}_{D,\ell}^\times$ and $\varphi(\gamma(1 + I_\ell)) = x \in \mathbb{F}_{\ell^2}^\times$, then

$$\mathrm{n}(\gamma) \mod \ell\mathbb{Z}_\ell = N_{\mathbb{F}_{\ell^2}^\times/\mathbb{F}_\ell^\times}(x). \tag{3.3}$$

Besides, recall that $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ is a semidirect product of the group Δ of diamond automorphisms and the group $W_{D,\ell}$ of lifted Atkin-Lehner involutions (cf. Theorem 2.1).

As a complement to our investigation of the cyclic covering $X_{D,\ell} \to X_D$ in the previous chapter, in this section we describe in more detail the geometry and the arithmetic of its intermediate curves. This description will be used throughout the rest of the chapter.

1.1. Intermediate curves: geometry. The intermediate curves appearing in the covering $X_{D,\ell} \to X_D$ arise as the Shimura curves X_U associated with the intermediate subgroups $\mathcal{U}_D \subseteq U \subseteq \widehat{\mathcal{O}}_D^\times$. Since $\mathcal{U}_D$ is maximal outside ℓ, the curves X_U actually arise when varying U_ℓ through the subgroups of $\mathcal{O}_{D,\ell}^\times$ containing $1 + I_\ell$. If one of these subgroups does not contain -1, then the subgroup $\{\pm 1\}U_\ell$ gives rise to the same Shimura curve, thus we can restrict ourselves to those subgroups U_ℓ of $\mathcal{O}_{D,\ell}^\times$ containing $\{\pm 1\}(1 + I_\ell)$. In turn, these subgroups are in one to one correspondence with the (cyclic) subgroups Θ_U of Δ: the curve X_U defined by U_ℓ is the quotient of $X_{D,\ell}$ by the action of the subgroup of automorphisms $\Theta_U \subseteq \Delta$, the degree of $X_U \to X_D$ is equal to the index $[\Delta : \Theta_U]$, and the group of covering automorphisms of $X_U \to X_D$ is isomorphic to $\Delta_U := \Delta/\Theta_U$.

Using the identification $\Delta \simeq \mathbb{F}_{\ell^2}^\times/\{\pm 1\}$, we see the above subgroups U_ℓ in correspondence with the cyclic subgroups H of $\mathbb{F}_{\ell^2}^\times$ containing $\{\pm 1\}$. Then, the degree of $X_U \to X_D$ coincides with the index of H in $\mathbb{F}_{\ell^2}^\times$. For simplicity, let us therefore fix the following notation. For every positive divisor d of $(\ell^2 - 1)/2$, we set:

$Y_d/\mathbb{Q}$: the unique intermediate curve with $\deg(Y_d \to X_D) = d$;
H_d : the unique (cyclic) subgroup of $\mathbb{F}_{\ell^2}^\times$ with $[\mathbb{F}_{\ell^2}^\times : H_d] = d$;
$t_d := |H_d| = (\ell^2 - 1)/d$;
U_d : the compact open subgroup $U_d \subseteq \widehat{\mathcal{O}}_D^\times$ defining Y_d, with $-1 \in U_{d,\ell}$;
$\mathcal{C}_\infty(d) := \mathcal{C}_\infty(U_d)$, the set of geometric connected components of Y_d;
$c_\infty(d) := |\mathcal{C}_\infty(d)|$.

From (1.10) and (1.11), $c_\infty(d)$ equals the cardinality of $\widehat{\mathbb{Z}}^\times/\mathrm{n}(U_d)$. After (3.2) and (3.3),

$$c_\infty(d) = [\mathbb{F}_\ell^\times : N(H_d)] = (\ell - 1)/|N(H_d)|, \tag{3.4}$$

where $N = N_{\mathbb{F}_{\ell^2}^\times/\mathbb{F}_\ell^\times} : \mathbb{F}_{\ell^2}^\times \to \mathbb{F}_\ell^\times$ is the norm map. The kernel of N is $\mathbb{F}_{\ell^2}^1 := \{x \in \mathbb{F}_{\ell^2}^\times : x^{\ell+1} = 1\}$, the unique subgroup of order $\ell + 1$ in $\mathbb{F}_{\ell^2}^\times$, hence

$$|N(H_d)| = |H_d/(H_d \cap \mathbb{F}_{\ell^2}^1)| = t_d/\gcd(t_d, \ell + 1). \tag{3.5}$$

Therefore, the number $c_\infty(d)$ of geometric connected components of Y_d can be easily computed solely in terms of d and ℓ. Indeed:

LEMMA 3.4. *With the above notations,*

$$c_\infty(d) = \gcd(\ell - 1, d). \tag{3.6}$$

In particular:

a) $c_\infty(d) = 1$ *if and only if* d *is an odd divisor of* $\ell + 1$*;*
b) $c_\infty(d) = 2$ *if and only if* d *is an even divisor of* $2(\ell+1)$ *and either* $\ell \equiv 3 \pmod 4$ *or* $4 \nmid d$*;*
c) $c_\infty(d)$ *is even if and only if* d *is even, or equivalently, if and only if* $N(H_d) \subseteq \mathbb{F}_\ell^{\times 2}$.

PROOF. The equality (3.6) follows by direct computation from (3.4) and (3.5). And then the three remaining assertions are immediate, except probably the second part of (c). But notice that (3.4) tells us that $c_\infty(d)$ is even if and only if $N(H_d)$ is contained in the unique subgroup of $\mathbb{F}_\ell^\times$ of index 2, which is precisely the subgroup $\mathbb{F}_\ell^{\times 2}$ of quadratic residues modulo ℓ. □

Considering the action of the lifted Atkin-Lehner involutions $\hat{\omega}_m$ on $X_{D,\ell}$, as well as the induced involutions on the curves Y_d, we have commutative diagrams

$$\begin{array}{ccccc} X_{D,\ell} & \longrightarrow & Y_d & \longrightarrow & X_D \\ \downarrow & & \downarrow & & \downarrow \\ X_{D,\ell}^{(m)} & \longrightarrow & Y_d^{(m)} & \longrightarrow & X_D^{(m)}, \end{array}$$

where the superscript (m) means quotient by $\hat{\omega}_m$ (or ω_m, in the case of X_D), and the vertical arrows are the natural quotient maps.

Identifying the set of geometric connected components of $X_{D,\ell}$ with $\mathbb{F}_\ell^\times$, recall from (2.12) that the action of $\hat{\omega}_m$ on it is by multiplication by

$$\varepsilon(m) := \begin{cases} \left(\frac{m}{\ell}\right) & \text{if } \ell \nmid m, \\ -\left(\frac{m/\ell}{\ell}\right) & \text{if } \ell \mid m. \end{cases} \tag{3.7}$$

If we consider an intermediate curve Y_d, the action of the induced involution $\hat{\omega}_m$ on its set of geometric connected components is by multiplication by $\varepsilon_d(m) := \varepsilon(m) \mod N(H_d)$ on $\mathbb{F}_\ell^\times/N(H_d)$. Thus $\varepsilon_d(m)$ is non-trivial if and only if $\varepsilon(m) = -1$ and $-1 \notin N(H_d)$. Regarding the last condition:

LEMMA 3.5. *With the above notations, $-1 \in N(H_d)$ if and only if $\mathrm{ord}_2(d) < \mathrm{ord}_2(\ell-1)$.*

PROOF. Since $-1 \in \mathbb{F}_\ell^\times$ is the unique element of order 2 and $\mathbb{F}_\ell^\times$ is cyclic, we have that $-1 \in N(H_d)$ if and only if $|N(H_d)|$ is even. Now, from

$$|N(H_d)| = \frac{t_d}{\gcd(t_d, \ell+1)} \quad \text{and} \quad t_d = \frac{(\ell+1)(\ell-1)}{d}$$

we see that $|N(H_d)|$ is even if and only if $\mathrm{ord}_2(\ell+1) < \mathrm{ord}_2(t_d) = \mathrm{ord}_2(\ell+1) + \mathrm{ord}_2(\ell-1) - \mathrm{ord}_2(d)$, which is equivalent to saying $\mathrm{ord}_2(d) < \mathrm{ord}_2(\ell-1)$. □

After this lemma, we can easily determine whether a lifted Atkin-Lehner involution $\hat{\omega}_m$ acts trivially on the set of geometric connected components of an intermediate curve Y_d or not. In particular, we can compute the number of geometric connected components of $Y_d^{(m)}$, which is either $c_\infty(d)$ or $c_\infty(d)/2$, respectively. For example, by combining Lemmas 3.4 and 3.5:

LEMMA 3.6. *The curve $Y_d^{(m)}$ is geometrically connected if and only if either*

i) *d is an odd divisor of $\ell+1$, or*
ii) *d is an even divisor of $2(\ell+1)$, $\varepsilon(m) = -1$ and $\ell \equiv 3 \pmod 4$.*

1.2. Intermediate curves: arithmetic. Although the Shimura curve $X_{D,\ell}$ is defined over $\mathbb{Q}$, recall from the previous chapter that its geometric connected components are only defined over the ℓ-th cyclotomic extension $\mathbb{Q}(\mu_\ell)$. Indeed, the choice of a model over $\mathbb{Q}$ for $X_{D,\ell}$ induces an action of $\mathrm{Aut}(\mathbb{C})$ on $X_{D,\ell}(\mathbb{C})$, which is compatible with the action of $\mathrm{Aut}(\mathbb{C})$ through its quotient $\mathrm{Gal}\,(\mathbb{Q}^{ab}/\mathbb{Q}) \simeq \widehat{\mathbb{Z}}^\times$ on the set

$$\mathcal{C}_\infty(\mathcal{U}_D) \,\simeq\, \widehat{\mathbb{Z}}^\times/\mathrm{n}(\mathcal{U}_D) \simeq \mathbb{F}_\ell^\times$$

under the map

$$X_{D,\ell}(\mathbb{C}) \,=\, B_{D,+}^\times \setminus (\mathcal{H} \times (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times/\mathcal{U}_D) \longrightarrow \mathcal{C}_\infty(\mathcal{U}_D) \,\simeq\, \widehat{\mathbb{Z}}^\times/\mathrm{n}(\mathcal{U}_D)$$

given by $[z,b] \mapsto [\mathrm{n}(b)]$. The open subgroup $U_c \subseteq \widehat{\mathbb{Z}}^\times \simeq \mathrm{Gal}\,(\mathbb{Q}^{ab}/\mathbb{Q})$ fixing the class $[\mathrm{n}(c)]$ corresponding to a component $c \in \mathcal{C}_\infty(\mathcal{U}_D)$ is

$$U_c \,=\, \prod_{q \neq \ell} \mathbb{Z}_q^\times \times (1 + \ell\mathbb{Z}_\ell),$$

thus the number field contained in $\mathbb{Q}^{ab}$ fixed by the action of U_c is $\mathbb{Q}(\mu_\ell)$, the ℓ-th cyclotomic field. It follows that the $\ell-1$ geometric connected components of $X_{D,\ell} \times \bar{\mathbb{Q}}$ are defined over $\mathbb{Q}(\mu_\ell)$, and conjugated by the action of $\mathrm{Gal}\,(\mathbb{Q}(\mu_\ell)/\mathbb{Q})$. Hence we can write

$$X_{D,\ell} \times_{\mathbb{Q}} \mathbb{Q}(\mu_\ell) \,\simeq \bigsqcup_{\sigma \in \mathrm{Gal}\,(\mathbb{Q}(\mu_\ell)/\mathbb{Q})} {}^{\sigma}(X_{D,\ell}^0), \tag{3.8}$$

where $X_{D,\ell}^0/\mathbb{Q}(\mu_\ell)$ is a geometrically connected curve, and the isomorphism is over $\mathbb{Q}(\mu_\ell)$.

Analogously, the field of definition of the geometric connected components of an intermediate curve Y_d is determined in the same way. Replacing $X_{D,\ell}$ by Y_d and $\mathcal{C}_\infty(\mathcal{U}_D)$ by $\mathcal{C}_\infty(d)$, the open subgroup $U_{c'} \subseteq \widehat{\mathbb{Z}}^\times \simeq \mathrm{Gal}\,(\mathbb{Q}^{ab}/\mathbb{Q})$ fixing the class $[\mathrm{n}(c')] \in \widehat{\mathbb{Z}}^\times/\mathrm{n}(U_d)$ of a component $c' \in \mathcal{C}_\infty(d)$ is now

$$U_{c'} \,=\, \prod_{q \neq \ell} \mathbb{Z}_q^\times \times \mathrm{n}(U_{d,\ell}).$$

Using again the relationship between the reduced norm n on subgroups of $\mathcal{O}_{D,\ell}^\times$ containing $\{\pm 1\}(1+I_\ell)$ and the norm map N on subgroups of $\mathbb{F}_{\ell^2}^\times$ given by (3.3), we see that the subfield of $\mathbb{Q}^{ab}$ fixed by the action of $U_{c'}$ is the subextension $\mathbb{Q} \subseteq K_d \subseteq \mathbb{Q}(\mu_\ell)$ corresponding, by Galois theory, to the unique subgroup G_d of $\mathrm{Gal}\,(\mathbb{Q}(\mu_\ell)/\mathbb{Q}) \simeq \mathbb{F}_\ell^\times$ of index $c_\infty(d)$. In particular, $\mathrm{Gal}\,(K_d/\mathbb{Q}) \simeq \mathrm{Gal}\,(\mathbb{Q}(\mu_\ell)/\mathbb{Q})/G_d$ is cyclic of order $c_\infty(d)$, thus $[K_d : \mathbb{Q}] = c_\infty(d)$. Similarly as before, we obtain that the $c_\infty(d)$ geometric connected components of Y_d are now defined over K_d, and $\mathrm{Gal}\,(K_d/\mathbb{Q})$ acts freely and transitively on $\mathcal{C}_\infty(d)$. Thus we have a decomposition

$$Y_d \times_{\mathbb{Q}} K_d \simeq \bigsqcup_{\sigma \in \mathrm{Gal}\,(K_d/\mathbb{Q})} {}^{\sigma}(Y_d^0) \tag{3.9}$$

over K_d, where now Y_d^0 is a geometrically connected curve defined over K_d.

Now fix a prime p dividing D, $p \neq \ell$. We consider the curve $X_D \times_{\mathbb{Q}} \mathbb{Q}_p$ over $\mathbb{Q}_p$ obtained from X_D through extension of scalars from $\mathbb{Q}$ to $\mathbb{Q}_p$, and also the curve $X_{D,\ell} \times_{\mathbb{Q}} \mathbb{Q}_p$ obtained in the same way from $X_{D,\ell}$. Let us describe how the curve $X_{D,\ell} \times_{\mathbb{Q}} \mathbb{Q}_p$ and its quotients decompose as a union of geometrically connected curves over unramified extensions of $\mathbb{Q}_p$; this description motivates the p-adic uniformisation of the curves $X_{D,\ell}$ and Y_d that we will work out later.

The curve $X_{D,\ell} \times_{\mathbb{Q}} \mathbb{Q}_p$ still has $\ell - 1$ geometric connected components, and they are defined over $\mathbb{Q}_p(\mu_\ell)$. Since $p \neq \ell$, the ℓ-th cyclotomic extension $\mathbb{Q}_p(\mu_\ell)$ of $\mathbb{Q}_p$ is unramified, and the ℓ-th cyclotomic character $\chi_\ell : \mathrm{Gal}\,(\mathbb{Q}_p(\mu_\ell)/\mathbb{Q}_p) \to \mathbb{F}_\ell^\times$ maps the Frobenius automorphism to the inverse class of $p \mod \ell$. It follows that $[\mathbb{Q}_p(\mu_\ell) : \mathbb{Q}_p]$ equals the order of $p \mod \ell$ in $\mathbb{F}_\ell^\times$.

For each integer $f \geq 1$, let us denote by $\mathbb{Q}_{p^f}$ the unique unramified extension of $\mathbb{Q}_p$ of degree f. Recall that $\mathbb{Q}_{p^f}$ is the cyclotomic extension $\mathbb{Q}_p(\mu_{p^f-1})$ obtained by adjoining to $\mathbb{Q}_p$ the (p^f-1)-th roots of unity. Hence, if we set f to be the order of $p \mod \ell$ in $\mathbb{F}_\ell^\times$, then $\mathbb{Q}_p(\mu_\ell) = \mathbb{Q}_{p^f}$ is the unique unramified extension of degree f of $\mathbb{Q}_p$. Since f divides $\ell - 1$, let us write $\ell - 1 = fc$, where c is a positive integer.

The geometric interpretation is the following. After extending scalars from $\mathbb{Q}$ to $\mathbb{Q}_p$, the geometric connected components of $X_{D,\ell} \times_{\mathbb{Q}} \mathbb{Q}_p$ are defined over the unramified extension $\mathbb{Q}_{p^f}$ of degree f. If $c > 1$, then the Galois action of $\mathrm{Gal}\,(\mathbb{Q}_{p^f}/\mathbb{Q}_p) \simeq \mathbb{Z}/f\mathbb{Z}$ is not transitive in the set of geometric connected components of $X_{D,\ell} \times_{\mathbb{Q}} \mathbb{Q}_p$, but it defines $c = (\ell-1)/f$ Galois orbits instead, each of them having f components. Each of the geometric components of $X_{D,\ell} \times_{\mathbb{Q}} \mathbb{Q}_p$ is then isomorphic to

$$X_{D,\ell}^0 \times_{\mathbb{Q}(\mu_\ell)} \mathbb{Q}_p(\mu_\ell) = X_{D,\ell}^0 \times_{\mathbb{Q}(\mu_\ell)} \mathbb{Q}_{p^f},$$

where $X_{D,\ell}^0/\mathbb{Q}(\mu_\ell)$ is as above, hence the p-adic counterpart of (3.8) can be written as

$$X_{D,\ell} \times_{\mathbb{Q}} \mathbb{Q}_{p^f} \simeq \bigsqcup_{i=1}^{c} \bigsqcup_{\sigma \in \mathrm{Gal}\,(\mathbb{Q}_{p^f}/\mathbb{Q}_p)} {}^{\sigma}(X_{D,\ell}^0 \times_{\mathbb{Q}(\mu_\ell)} \mathbb{Q}_{p^f}).$$

Now we look at the intermediate curve $Y_d \times_{\mathbb{Q}} \mathbb{Q}_p$ in the covering $X_{D,\ell} \times_{\mathbb{Q}} \mathbb{Q}_p \to X_D \times_{\mathbb{Q}} \mathbb{Q}_p$. The field of definition $K_d\mathbb{Q}_p$ of the geometric connected components of this curve is a subfield of $\mathbb{Q}_p(\mu_\ell) = \mathbb{Q}_{p^f}$, thus it is an unramified extension of $\mathbb{Q}_p$ contained in $\mathbb{Q}_{p^f}$. Therefore, we can write $K_d\mathbb{Q}_p = \mathbb{Q}_{p^{f_d}}$ for some positive integer f_d dividing f.

In order to determine the integer f_d, observe that the ℓ-th cyclotomic character induces, by passage to the quotient, a character $\mathrm{Gal}\,(\mathbb{Q}_{p^{f_d}}/\mathbb{Q}_p) \to \mathbb{F}_\ell^\times/N(H_d)$. Similarly as before, the integer $f_d = [\mathbb{Q}_{p^{f_d}} : \mathbb{Q}_p]$ is the order of $p \mod \ell$ in $\mathbb{F}_\ell^\times/N(H_d)$. In particular, f_d divides $c_\infty(d)$. Equivalently, f_d is the smallest positive integer such that $p^{f_d} \mod \ell \in N(H_d)$ (and from this we can see again that f_d divides f: the subgroup of $N(H_d)$ generated by $p^{f_d} \mod \ell$ is also a subgroup of the subgroup of $\mathbb{F}_\ell^\times$ generated by $p \mod \ell$, and the minimality condition on f_d implies that f_d divides f). Writing $c_\infty(d) = c_p(d)f_d$, we eventually find the p-adic counterpart of (3.9):

$$Y_d \times_{\mathbb{Q}} \mathbb{Q}_{p^{f_d}} \simeq \bigsqcup_{i=1}^{c_p(d)} \bigsqcup_{\sigma \in \mathrm{Gal}\,(\mathbb{Q}_{p^{f_d}}/\mathbb{Q}_p)} {}^{\sigma}(Y_d^0 \times_{K_d} \mathbb{Q}_{p^{f_d}}).$$

2. Čerednik-Drinfeld theory

In this section we present the Theorem of Čerednik and Drinfeld on the p-adic uniformisation of Shimura curves at primes p of bad reduction, assuming that there is no level structure at p. Especially in Section 2.1, we have followed the exposition in [**BC91**].

By extending the moduli problems for Shimura curves X_U to moduli problems in the category of $\mathbb{Z}$-schemes, curves X_U admit a proper, flat, integral (but not smooth) model over $\mathbb{Z}$. We denote by $\mathcal{X}_U/\mathbb{Z}_p$ the base change from $\mathbb{Z}$ to $\mathbb{Z}_p$ of these $\mathbb{Z}$-schemes, so that $\mathcal{X}_U$ is a $\mathbb{Z}_p$-integral model of the Shimura curve X_U. In particular, we write $\mathcal{X}_D$, $\mathcal{X}_{D,\ell}$ and $\mathcal{Y}_d$ for the $\mathbb{Z}_p$-integral models thus obtained for the curves X_D, $X_{D,\ell}$ and Y_d, respectively.

2.1. Statement of the Theorem of Čerednik and Drinfeld. Let p be a prime dividing D, and assume we are given a compact open subgroup $U \subseteq \widehat{\mathcal{O}}_D^\times$ of the form $U_p^0 U^p$, where $U_p^0 := \mathcal{O}_{D,p}^\times$ and $U^p \subseteq \prod_{q\neq p} \mathcal{O}_{D,q}^\times$. In other words, assume U is maximal at p. Let also $B_{D/p}$ be the definite rational quaternion algebra of reduced discriminant D/p. One can think of $B_{D/p}$ as obtained from B_D by interchanging the local invariants at the primes p and ∞. We fix an isomorphism

$$(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times \xrightarrow{\simeq} (B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times, \tag{3.10}$$

obtained from an anti-isomorphism $B_D \otimes_{\mathbb{Q}} \mathbb{A}_f^p \longrightarrow B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p$ composed by the inversion. Having fixed this isomorphism, by a slight abuse of notation the image of an element

$$b^p = (b_v^p)_{v\neq p} \in (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$$

will be written as

$$(b^p)^{-1} = ((b_v^p)^{-1})_{v\neq p} \in (B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times.$$

In particular, $U^p \subseteq (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$ can also be regarded as a subgroup of $(B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$, so that we can compare the actions of U^p by multiplication on $(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$ and $(B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$ by reversing the side of these actions: right multiplication by $u \in U^p$ on $(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$ corresponds with left multiplication by u^{-1} on $(B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$.

We also fix an isomorphism $B_{D/p,p}^\times = (B_{D/p} \otimes_{\mathbb{Q}} \mathbb{Q}_p)^\times \simeq \mathrm{GL}_2(\mathbb{Q}_p)$ induced from an identification of the local quaternion algebra $B_{D/p,p}$ with $\mathrm{M}_2(\mathbb{Q}_p)$. Then $\mathrm{GL}_2(\mathbb{Q}_p)$ acts naturally on the left on the collection of double cosets

$$Z_U := U^p \setminus (B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times / B_{D/p}^\times.$$

This action has only finitely many orbits, thus the set

$$\mathcal{C}_p(U) := \mathrm{GL}_2(\mathbb{Q}_p) \setminus Z_U = U^p \setminus (B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times / B_{D/p}^\times$$

is finite. If we define $c_p(U) := |\mathcal{C}_p(U)|$, then the integer $c_p(U)$ is closely related to the number $c_\infty(U) := |\mathcal{C}_\infty(U)|$ of geometric connected components of the Shimura curve X_U. Indeed, the reduced norm induces now an isomorphism

$$\mathrm{GL}_2(\mathbb{Q}_p) \setminus Z_U = U^p \setminus (B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times / B_{D/p}^\times \xrightarrow{\simeq} \mathrm{n}(U^p) \setminus (\mathbb{A}_f^p)^\times / \mathbb{Q}^{>0},$$

and using that $(\mathbb{A}_f^p)^\times = \mathbb{Q}^{>0}(\widehat{\mathbb{Z}}^p)^\times$ and $\mathbb{Q}^{>0} \cap (\widehat{\mathbb{Z}}^p)^\times = \langle p \rangle = \{p^a : a \in \mathbb{Z}\}$, we can identify the right hand side with

$$\mathrm{n}(U^p) \setminus (\widehat{\mathbb{Z}}^p)^\times / \langle p \rangle.$$

But now observe that the maximality condition at p implies $\mathrm{n}(U_p) = \mathbb{Z}_p^\times$, so that we have

$$\mathrm{n}(U^p) \setminus (\widehat{\mathbb{Z}}^p)^\times \simeq \mathrm{n}(U) \setminus \widehat{\mathbb{Z}}^\times \simeq \mathcal{C}_\infty(U).$$

Regarding $\langle p \rangle$ as a subgroup of $(\widehat{\mathbb{Z}}^p)^\times$, we can therefore identify $\mathcal{C}_p(U)$ with the quotient of $\mathcal{C}_\infty(U)$ modulo $\langle p \rangle / (\mathrm{n}(U^p) \cap \langle p \rangle)$. The latter is a finite cyclic group, and its order is the smallest positive integer $f_p(U)$ such that $p^{f_p(U)} \in \mathrm{n}(U^p) \cap \mathbb{Q}^{>0}$. In particular, we have a natural projection map $\mathcal{C}_\infty(U) \to \mathcal{C}_p(U)$ and an identity

$$c_\infty(U) = c_p(U) f_p(U). \tag{3.11}$$

Geometrically, the $c_\infty(U)$ connected components of $X_U \times_{\mathbb{Q}} \bar{\mathbb{Q}}_p$ are classified into $c_p(U)$ distinct classes, each of them having $f_p(U)$ connected components. Two geometric connected components $c, c' \in \mathcal{C}_\infty(U)$ *belong to the same p-class* if c and c' have the same image in $\mathcal{C}_p(U)$.

Observe that we can choose representatives $b_i = (b_{i,v})_v \in (B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$ for the distinct p-classes of geometric connected components in $\mathcal{C}_p(U) = \mathrm{GL}_2(\mathbb{Q}_p) \setminus Z_U$ such that $b_{i,p} = 1$, $i = 1, \dots, c_p(U)$. If we write $\Gamma_i := \mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Q}_p)}(b_i)$ for the stabiliser of b_i with respect to the $\mathrm{GL}_2(\mathbb{Q}_p)$-action, then

$$\Gamma_i = \{g_p \in \mathrm{GL}_2(\mathbb{Q}_p) : g_p \cdot b_i \in U^p b_i B_{D/p}^\times\} = B_{D/p}^\times \cap b_i^{-1} U^p b_i.$$

The groups Γ_i are discrete and cocompact subgroups of $\mathrm{GL}_2(\mathbb{Q}_p)$. Moreover, they contain some power of $p \in \mathbb{Q}_p^\times \subseteq \mathrm{GL}_2(\mathbb{Q}_p)$. If $c_p(U) > 1$ and we choose $b_1 = 1 = (1, 1, \dots, 1, \dots)$, notice that $\Gamma_i = b_i^{-1} \Gamma_1 b_i$ for all $i = 2, \dots, c_p(U)$. We assume throughout that the groups Γ_i are closed under the canonical involution $b \mapsto \bar{b}$ induced from $B_{D/p}$ (it is enough to assume this for one of the Γ_i's, for example for $\Gamma_1 = B_{D/p}^\times \cap U^p$, and this amounts to assuming $\bar{U}^p = U^p$).

Finally, before stating the Theorem of Čerednik and Drinfeld, we remark that for U^p *small enough*, the collections of double cosets Z_U form a projective system, as U^p varies, on which $(B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$ acts naturally by multiplication on the left: if $b \in (B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$, multiplication on the left by b induces an isomorphism

$$\lambda_U(b) : Z_U \longrightarrow Z_{bUb^{-1}}$$

(compare this with (1.13)).

THEOREM 3.7 (Čerednik-Drinfeld). *For every U^p small enough, and with $U = U_p^0 U^p$ as before, one has an isomorphism of formal $\mathbb{Z}_p$-schemes*

$$\widehat{\mathcal{X}}_U \simeq \mathrm{GL}_2(\mathbb{Q}_p) \setminus [\widehat{\mathcal{H}}_p \widehat{\otimes} \widehat{\mathbb{Z}}_p^{\mathrm{ur}} \times Z_U], \tag{3.12}$$

where $\widehat{\mathcal{X}}_U$ is the formal completion of $\mathcal{X}_U$ along its closed fiber. This isomorphism is compatible with the natural projections as U^p varies, and also with the action of $(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times \simeq (B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$ on both sides. It also lifts to an isomorphism between the special formal $\mathcal{O}_{D,p}$-modules associated with the two formal schemes.

We refer the reader to [**BC91, Dri76**] for a proof of this theorem, and next we point out a few remarks about the statement.

REMARK 3.8. The group $\mathrm{GL}_2(\mathbb{Q}_p)$ acts on $\widehat{\mathcal{H}}_p \widehat{\otimes} \widehat{\mathbb{Z}}_p^{\mathrm{ur}}$ through the natural action on $\widehat{\mathcal{H}}_p$ and through $g \mapsto \widetilde{\mathrm{Fr}}_p^{-\mathrm{val}_p(\det g)}$ on $\widehat{\mathbb{Z}}_p^{\mathrm{ur}}$, where $\widetilde{\mathrm{Fr}}_p : \mathbb{Z}_p^{\mathrm{ur}} \to \mathbb{Z}_p^{\mathrm{ur}}$ is the lift of the Frobenius automorphism $\mathrm{Fr}_p : \bar{\mathbb{F}}_p \to \bar{\mathbb{F}}_p$ to a $\mathbb{Z}_p$-automorphism. This action is defined over $\mathbb{Z}_p$. Similarly, the right action of an element $b_p \in B_{D,p}^\times$ on $\widehat{\mathcal{X}}_U$ induced by the isomorphism

$$\rho_U(1, \dots, 1, b_p, 1, \dots) : X_U \longrightarrow X_U$$

is translated under (3.12) to the right hand side to the action on $\widehat{\mathbb{Z}}_p^{\mathrm{ur}}$ through $b_p \mapsto \widetilde{\mathrm{Fr}}_p^{-\mathrm{val}_p(\mathrm{n}(b_p))}$.

REMARK 3.9. The compatibility of the isomorphism (3.12) with the right action of $(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$ on the left hand side and the left action of $(B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$ on the right hand side requires to compare these two actions by using the anti-isomorphism in (3.10). We elaborate more on this in paragraph 2.3 below.

REMARK 3.10. The special formal $\mathcal{O}_{D,p}$-module associated with $\widehat{\mathcal{X}}_U$ is the formal completion of the universal abelian variety given by the moduli problem associated to U, whereas the special formal $\mathcal{O}_{D,p}$-module associated with the right hand side of the isomorphism in the theorem arises from the moduli description of $\widehat{\mathcal{H}}_p \widehat{\otimes} \widehat{\mathbb{Z}}_p^{\mathrm{ur}}$.

2.2. Algebraisation: decomposing $\mathcal{X}_U$ as a union of Mumford curves. Even though the isomorphism in the Theorem of Čerednik and Drinfeld stated above is an isomorphism of formal $\mathbb{Z}_p$-schemes, the left hand side is the completion of an algebraic $\mathbb{Z}_p$-scheme along its closed fibre, hence it is obviously algebraisable. As a consequence, the right hand side of (3.12) is algebraisable as well, and a closer analysis will allow us to obtain an algebraisation. For every subgroup $\Gamma \subseteq \mathrm{GL}_2(\mathbb{Q}_p)$, we write $Z\Gamma := \Gamma \cap \mathbb{Q}_p^\times$ and denote by $\Gamma' := \Gamma/Z\Gamma$ the image of Γ in $\mathrm{PGL}_2(\mathbb{Q}_p)$.

First of all, consider the natural projection map

$$\mathrm{pr} : \mathrm{GL}_2(\mathbb{Q}_p) \setminus [\widehat{\mathcal{H}}_p \widehat{\otimes} \widehat{\mathbb{Z}}_p^{\mathrm{ur}} \times Z_U] \longrightarrow \mathcal{C}_p(U) = \{[b_1], \dots, [b_{c_p(U)}]\}. \tag{3.13}$$

Since the set $\mathcal{C}_p(U) = \mathrm{GL}_2(\mathbb{Q}_p) \setminus Z_U$ is finite, we obtain a decomposition into p-classes

$$\mathrm{GL}_2(\mathbb{Q}_p) \setminus [\widehat{\mathcal{H}}_p \widehat{\otimes} \widehat{\mathbb{Z}}_p^{\mathrm{ur}} \times Z_U] = \coprod_{i=1}^{c_p(U)} \mathrm{pr}^{-1}([b_i]) \simeq \coprod_{i=1}^{c_p(U)} \Gamma_i \setminus (\widehat{\mathcal{H}}_p \widehat{\otimes} \widehat{\mathbb{Z}}_p^{\mathrm{ur}}). \tag{3.14}$$

And since all the groups Γ_i are conjugated to $\Gamma := \Gamma_1 = B_{D/p}^\times \cap U^p$, each formal $\mathbb{Z}_p$-scheme in the above disjoint union (i.e., each p-class) is isomorphic to

$$\Gamma \setminus (\widehat{\mathcal{H}}_p \widehat{\otimes} \widehat{\mathbb{Z}}_p^{\mathrm{ur}}). \tag{3.15}$$

Now define $k := k(\Gamma) \geq 1$ to be the positive integer such that $\mathrm{val}_p(Z\Gamma) = k\mathbb{Z}$. Equivalently, since every element in $Z\Gamma = \Gamma \cap \mathbb{Q}^\times$ is of the form p^r for some integer r, k is the smallest positive integer such that $p^k \in \Gamma$. Further, define $f := f(\Gamma)$ as the positive integer such that $\mathrm{val}_p(\mathrm{n}(\Gamma)) = f\mathbb{Z}$. In other words, f is the smallest positive integer such that there is an element $\gamma \in \Gamma$ with $\mathrm{val}_p(\mathrm{n}(\gamma)) = f$.

Lemma 3.11. *With notations as before,* $\mathrm{n}(\Gamma) = \mathrm{n}(U^p) \cap \mathbb{Q}^{>0}$. *In particular,* $f(\Gamma) = f_p(U)$ *(cf.* (3.11)*).*

Proof. The inclusion $\mathrm{n}(\Gamma) \subseteq \mathrm{n}(U^p) \cap \mathbb{Q}^{>0}$ is clear, since $B_{D/p}^\times$ is definite. So let $t \in \mathrm{n}(U^p) \cap \mathbb{Q}^{>0}$, regarded as an element in $\mathbb{A}_f^p$, and choose $u \in U^p$ with $\mathrm{n}(u) = t$. Since $\mathrm{n}(B_{D/p}^\times) = \mathbb{Q}^{>0}$, we can also choose $b \in B_{D/p}^\times$ with $\mathrm{n}(b) = t$. Therefore, $bu^{-1} \in (B_{D/p} \otimes \mathbb{A}_f^p)^\times$ is an element of reduced norm 1. By the Eichler-Kneser strong approximation theorem (see Theorem 1.27 or [**Vig80**, Ch. III, Théorème 4.3]), there are elements $b_1 \in B_{D/p}^\times$, $u_1 \in U^p$, both of norm 1, such that $bu^{-1} = b_1 u_1$. Therefore, $b_1^{-1} b = u_1 u$ is an equality in $U^p \cap B_{D/p}^\times = \Gamma$ and both sides of the equality have norm t. This shows the inclusion $\mathrm{n}(\Gamma) \supseteq \mathrm{n}(U^p) \cap \mathbb{Q}^{>0}$, thus the first part of the lemma follows. The second part is now just a direct consequence of the definitions of $f(\Gamma)$ and $f_p(U)$. □

Since Γ is closed under conjugation, we have $\mathrm{n}(\Gamma) \subseteq \Gamma \cap \mathbb{Q}^\times = Z\Gamma$, hence $\mathrm{val}_p(\mathrm{n}(\Gamma)) \subseteq \mathrm{val}_p(Z\Gamma)$. As a consequence $f\mathbb{Z} \subseteq k\mathbb{Z}$, so that k divides f. Further, from $Z\Gamma \subseteq \Gamma$ we deduce $2k\mathbb{Z} = \mathrm{val}_p(\det(Z\Gamma)) \subseteq \mathrm{val}_p(\mathrm{n}(\Gamma)) = f\mathbb{Z}$, hence f divides $2k$ and we must have either $f = k$ or $f = 2k$. Write

$$\Gamma_+ := \{\gamma \in \Gamma : \mathrm{val}_p(\mathrm{n}(\gamma)) \in 2k\mathbb{Z}\}, \qquad W := \Gamma/\Gamma_+.$$

If $f = 2k$, then $\Gamma_+ = \Gamma$ and W is trivial, whereas if $f = k$, then Γ_+ has index 2 in Γ and W is cyclic of order two, with its non-trivial element represented by any $w \in \Gamma$ such that $\mathrm{val}_p(\mathrm{n}(w)) = f = k$.

Proposition 3.12. *Let $\widehat{\mathcal{X}}_\Gamma$ be the formal $\mathbb{Z}_p$-scheme corresponding to the formal quotient* (3.15)*, and let $\mathcal{M}_{\Gamma_+}/\mathbb{Z}_p$ be the Mumford curve associated with Γ_+, whose formal completion along the closed fibre is the formal quotient $\Gamma_+ \setminus \widehat{\mathcal{H}}_p$. Then $\widehat{\mathcal{X}}_\Gamma$ is the formal completion along the closed fibre of a projective scheme $\mathcal{X}_\Gamma/\mathbb{Z}_p$ such that:*

a) *if $f = 2k$, then*

$$\mathcal{X}_\Gamma \times \mathbb{Z}_{p^f} \simeq \coprod_{i=1}^{f} \mathcal{M}_{\Gamma_+} \times_{\mathbb{Z}_p} \mathbb{Z}_{p^f},$$

the f copies of $\mathcal{M}_{\Gamma_+} \times_{\mathbb{Z}_p} \mathbb{Z}_{p^f}$ being conjugated by the action of $\mathrm{Gal}(\mathbb{Z}_{p^f}/\mathbb{Z}_p)$;

b) *if $f = k$, then*

$$\mathcal{X}_\Gamma \times \mathbb{Z}_{p^f} \simeq \coprod_{i=1}^{f} (\mathcal{M}_{\Gamma_+} \times_{\mathbb{Z}_p} \mathbb{Z}_{p^f})^\xi,$$

where now the superscript ξ means that $\mathcal{M}_{\Gamma_+} \times_{\mathbb{Z}_p} \mathbb{Z}_{p^f}$ is twisted by the 1-cocycle

$$\xi : \mathrm{Gal}\,(\mathbb{Z}_{p^{2f}}/\mathbb{Z}_{p^f}) \longrightarrow \mathrm{Aut}(\mathcal{M}_{\Gamma_+} \times_{\mathbb{Z}_p} \mathbb{Z}_{p^{2f}}/\mathbb{Z}_{p^{2f}}), \quad \widetilde{\mathrm{Fr}}_p^f \mapsto w \times \mathrm{id},$$

and again the f copies of this curve are conjugated by the action of $\mathrm{Gal}\,(\mathbb{Z}_{p^f}/\mathbb{Z}_p)$.

Proof. By construction, $\widehat{\mathcal{H}}_p \widehat{\otimes} \widehat{\mathbb{Z}}_p^{\mathrm{ur}}$ is the extension of scalars of the formal $\mathbb{Z}_p$-scheme $\widehat{\mathcal{H}}_p$ to $\widehat{\mathbb{Z}}_p^{\mathrm{ur}}$, thus we can endow it with its natural Weil descent datum α. Since p^k is the smallest power of p in $Z\Gamma$, and $Z\Gamma$ acts trivially on $\widehat{\mathcal{H}}_p$,

$$\Gamma \setminus (\widehat{\mathcal{H}}_p \widehat{\otimes} \widehat{\mathbb{Z}}_p^{\mathrm{ur}}) \simeq \Gamma' \setminus (Z\Gamma \setminus (\widehat{\mathcal{H}}_p \widehat{\otimes} \widehat{\mathbb{Z}}_p^{\mathrm{ur}})) \simeq \Gamma' \setminus (\widehat{\mathcal{H}}_p \widehat{\otimes} \mathbb{Z}_{p^{2k}}) \simeq \Gamma \setminus (\widehat{\mathcal{H}}_p \widehat{\otimes} \mathbb{Z}_{p^{2k}}).$$

In other words, α^{2k} is effective, and as a consequence of étale descent, α is effective as well. Therefore, we may regard (3.15) as an algebraisable formal scheme over $\mathbb{Z}_p$, thus it is the formal completion of a projective scheme $\mathcal{X}_\Gamma/\mathbb{Z}_p$ along its special fibre.

From the above observation, using that Γ_+ acts trivially on $\mathbb{Z}_{p^{2k}}$ we have therefore an isomorphism

$$\widehat{\mathcal{X}}_\Gamma \widehat{\otimes} \mathbb{Z}_{p^{2k}} \simeq [W \setminus ((\Gamma_+ \setminus \widehat{\mathcal{H}}_p) \widehat{\otimes} \mathbb{Z}_{p^{2k}})] \widehat{\otimes} \mathbb{Z}_{p^{2k}}.$$

Now the formal quotient $\Gamma_+ \setminus \widehat{\mathcal{H}}_p$ is algebraisable (see [**Mum72, Kur79**]) by a geometrically connected projective scheme $\mathcal{M}_{\Gamma_+}$ of relative dimension one over $\mathbb{Z}_p$, (a finite quotient of) a Mumford curve. By a slight abuse of notation, we call $\mathcal{M}_{\Gamma_+}$ the Mumford curve associated with Γ_+. If $f = 2k$, then W is trivial, thus the base change to $\mathbb{Z}_{p^{2k}}$ of the $\mathbb{Z}_p$-scheme $\mathcal{M}_{\Gamma_+} \times_{\mathbb{Z}_p} \mathbb{Z}_{p^{2k}}$ is isomorphic to $f = 2k$ copies of $\mathcal{M}_{\Gamma_+} \times_{\mathbb{Z}_p} \mathbb{Z}_{p^{2k}}$ (now as a $\mathbb{Z}_{p^{2k}}$-scheme) conjugated by Galois, hence item a) follows.

In contrast, when $f = k$ we find that the formal $\mathbb{Z}_p$-scheme

$$W \setminus ((\Gamma_+ \setminus \widehat{\mathcal{H}}_p) \widehat{\otimes} \mathbb{Z}_{p^{2f}}),$$

hence $\widehat{\mathcal{X}}_\Gamma$, is algebraisable by the quadratic twist $(\mathcal{M}_{\Gamma_+} \times_{\mathbb{Z}_p} \mathbb{Z}_{p^f})^\xi$ as in the statement, *regarded as a scheme over* $\mathbb{Z}_p$. Then $\mathcal{X}_\Gamma \times_{\mathbb{Z}_p} \mathbb{Z}_{p^f}$ decomposes as f copies of $(\mathcal{M}_{\Gamma_+} \times_{\mathbb{Z}_p} \mathbb{Z}_{p^f})^\xi$ (now regarded as a $\mathbb{Z}_{p^f}$-scheme), again conjugated by Galois. This completes the proof in case b). □

Remark 3.13. Proposition 3.12, together with (3.14), gives an arithmetic meaning to the notion of *p-classes* introduced when comparing the sets $\mathcal{C}_\infty(U)$ and $\mathcal{C}_p(U)$ in Section 2.1. Namely, the curve $X_U \times_{\mathbb{Q}} \mathbb{Q}_p \simeq \mathcal{X}_U \times_{\mathbb{Z}_p} \mathbb{Q}_p$ decomposes *over* $\mathbb{Q}_p$ as a union of $c_p(U)$ copies of the (not geometrically connected, in general) curve $\mathcal{X}_\Gamma \times_{\mathbb{Z}_p} \mathbb{Q}_p$. Each of these copies corresponds to a p-class in the set $\mathcal{C}_p(U)$, and the f geometric connected components in each p-class, conjugated by the action of $\mathrm{Gal}\,(\mathbb{Q}_{p^f}/\mathbb{Q}_p)$, arise only after base change to $\mathbb{Q}_{p^f}$.

2.3. p-modular automorphisms. Recall that the group $\mathrm{Aut}^{\mathrm{mod}}(X_U) \subseteq \mathrm{Aut}_{\mathbb{Q}}(X_U)$ of modular automorphisms of the Shimura curve $X_U/\mathbb{Q}$ is defined as

$$\mathrm{Aut}^{\mathrm{mod}}(X_U) := \mathrm{Norm}_{(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times}(U)/\mathbb{Q}^\times U.$$

We now describe a group of automorphisms of $\mathcal{X}_U$ closely related to $\mathrm{Aut}^{\mathrm{mod}}(X_U)$ that can be defined in a similar way from the p-adic counterpart of X_U. Indeed, we have seen above that for U small enough there is a left action of $(B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$ on the projective system Z_U: every element $b \in (B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$ induces an isomorphism $\lambda_U(b) : Z_U \to Z_{bUb^{-1}}$. It follows that the elements in $\mathrm{Norm}_{(B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times}(U^p)$ induce automorphisms of Z_U, hence automorphisms of $\widehat{\mathcal{X}}_U$. Actually, one has $\lambda_U(b) \in \mathrm{Aut}_{\mathbb{Z}_p}(\mathcal{X}_U)$ for every $b \in \mathrm{Norm}_{(B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times}(U^p)$. On the other hand, if

$b \in (B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$, then $\lambda_U(b)$ is the identity on $\mathcal{X}_U$ if and only if $b \in U^p$. In view of this, we define

$$\mathrm{Aut}^{p\text{-mod}}(\mathcal{X}_U) := \mathrm{Norm}_{(B_{D/p}\otimes_{\mathbb{Q}}\mathbb{A}_f^p)^\times}(U^p)/U^p \subseteq \mathrm{Aut}_{\mathbb{Z}_p}(\mathcal{X}_U)$$

and call $\mathrm{Aut}^{p\text{-mod}}(\mathcal{X}_U)$ the group of *p-modular automorphisms* of $\mathcal{X}_U$.

In order to exhibit the close relation between $\mathrm{Aut}^{p\text{-mod}}(\mathcal{X}_U)$ and $\mathrm{Aut}^{\mathrm{mod}}(X_U)$, write $(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times \simeq (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times \times B_{D,p}^\times$, so that $(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$ is identified as a subgroup of $(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$ via the natural monomorphism $x \mapsto (x, 1)$ into the first factor. Then, by using the anti-isomorphism in (3.10), we can also regard $(B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$ as a subgroup of $(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$.

Now let $(b_v)_{v\neq p} \in \mathrm{Norm}_{(B_{D/p}\otimes_{\mathbb{Q}}\mathbb{A}_f^p)^\times}(U^p)$. Then its image $((b_v^{-1})_{v\neq p}, 1)$ in $(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$ clearly normalises U, and furthermore, $((b_v^{-1})_{v\neq p}, 1) \in \mathbb{Q}^\times U$ if and only if $(b_v)_{v\neq p} \in U^p$ (where here U^p is regarded as a subgroup in $(B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$). Hence, the group $\mathrm{Aut}^{p\text{-mod}}(\mathcal{X}_U)$ of p-modular automorphisms of $\mathcal{X}_U$ is naturally a subgroup of $\mathrm{Aut}^{\mathrm{mod}}(X_U)$. As Remark 3.9 points out, the modular automorphisms of X_U of the form $\rho_U(((b_v^p)_{v\neq p}, 1))$ correspond with the p-modular automorphisms of $\mathcal{X}_U$ of the form $\lambda_U((b_v^p)_{v\neq p}^{-1})$.

As above, let $\Gamma := B_{D/p}^\times \cap U^p$ be regarded as a subgroup of $\mathrm{GL}_2(\mathbb{Q}_p)$, so that

$$\widehat{\mathcal{X}}_\Gamma \simeq \Gamma \setminus (\widehat{\mathcal{H}}_p \widehat{\otimes} \widehat{\mathbb{Z}}_p^{\mathrm{ur}}).$$

Then define

$$\Gamma^* := \mathrm{Norm}_{B_{D/p}^\times}(U^p),$$

which can also be regarded as a subgroup of $\mathrm{GL}_2(\mathbb{Q}_p)$. The natural inclusion of $B_{D/p}^\times$ in $(B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$ induces an inclusion $\Gamma^* \hookrightarrow \mathrm{Norm}_{(B_{D/p}\otimes_{\mathbb{Q}}\mathbb{A}_f^p)^\times}(U^p)$. Furthermore:

LEMMA 3.14. *The quotient Γ^*/Γ is a subgroup of $\mathrm{Aut}^{p\text{-}mod}(\mathcal{X}_U)$, and every p-modular automorphism in Γ^*/Γ acts trivially on the set $\mathcal{C}_p(U)$.*

PROOF. From the definitions, if $\gamma \in \Gamma^*$, then $\gamma \in \Gamma$ if and only if $\gamma \in U^p$. Therefore, the natural inclusion $\Gamma^* \hookrightarrow \mathrm{Norm}_{(B_{D/p}\otimes_{\mathbb{Q}}\mathbb{A}_f^p)^\times}(U^p)$ induces by passing to the quotient a monomorphism of groups

$$\Gamma^*/\Gamma \hookrightarrow \mathrm{Norm}_{(B_{D/p}\otimes_{\mathbb{Q}}\mathbb{A}_f^p)^\times}(U^p)/U^p = \mathrm{Aut}^{p\text{-mod}}(\mathcal{X}_U).$$

As for the second part of the statement, every element in Γ^* normalises Γ, hence its action on $\mathcal{X}_U$ as a p-modular automorphism preserves the fibres of (3.13). □

3. Local points on the curves Y_d

We keep the notations from the previous sections. Let $X_{D,\ell} \to X_D$ be the Shimura covering of X_D at a prime divisor $\ell > 3$ of D, d be a positive divisor of $(\ell^2-1)/2$ and $Y_d/\mathbb{Q}$ be the unique intermediate curve of degree d over X_D. Let also $p \neq \ell$ be a prime divisor of D. The goal of this section is to study the existence of K-rational points on Y_d for finite extensions K of $\mathbb{Q}_p$. The main tool for this purpose is Čerednik-Drinfeld theory described in Section 2.

3.1. p-adic uniformisation of the curves Y_d. Let $\mathcal{X}_D/\mathbb{Z}_p$ (resp. $\mathcal{Y}_d/\mathbb{Z}_p$) be the $\mathbb{Z}_p$-integral model for X_D (resp. Y_d) as in Section 2. In particular, $\mathcal{X}_D$ (resp. $\mathcal{Y}_d$) is a projective, but not smooth, curve over $\mathbb{Z}_p$ with generic fibre $X_D \times_{\mathbb{Q}} \mathbb{Q}_p$ (resp. $Y_d \times_{\mathbb{Q}} \mathbb{Q}_p$). Since U_d is maximal at p (because $p \neq \ell$), we can apply the Theorem of Čerednik and Drinfeld presented in the previous section to the curve Y_d.

We write

$$\Gamma_D := \widehat{\mathcal{O}}_{D/p}^{(p)\times} \cap B_{D/p}^\times = (\mathcal{O}_{D/p} \otimes_{\mathbb{Z}} \mathbb{Z}[1/p])^\times = \mathcal{O}_{D/p}^{(p)\times} \quad \text{and} \quad \Gamma_d := U_d^{(p)} \cap B_{D/p}^\times,$$

regarded as subgroups of $\mathrm{GL}_2(\mathbb{Q}_p)$ after fixing a monomorphism $B_{D/p} \hookrightarrow B_{D/p} \otimes_{\mathbb{Q}} \mathbb{Q}_p$ and an isomorphism $B_{D/p} \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq \mathrm{M}_2(\mathbb{Q}_p)$. Notice that Γ_d is naturally a subgroup of Γ_D. Indeed, writing

$$\nu : \Gamma_D \hookrightarrow \mathcal{O}_{D/p,\ell}^\times \tag{3.16}$$

for the natural inclusion of Γ_D into $\mathcal{O}_{D/p,\ell}^\times$, we clearly have $\Gamma_d = \nu^{-1}(U_{d,\ell})$. By a slight abuse of notation, we will often just write $\Gamma_d = \Gamma_D \cap U_{d,\ell}$. Furthermore, fixing an anti-isomorphism $\mathcal{O}_{D,\ell}^\times \to \mathcal{O}_{D/p,\ell}^\times$ compatible with (3.10), the isomorphism in (3.2) gives rise to an analogous isomorphism

$$\psi : (1+I_\ell) \setminus \mathcal{O}_{D/p,\ell}^\times \xrightarrow{\simeq} \mathbb{F}_{\ell^2}^\times, \tag{3.17}$$

where here we still denote by I_ℓ the unique maximal ideal of $\mathcal{O}_{D/p,\ell}$, consisting of the non-invertible elements. If $\gamma \in \mathcal{O}_{D/p,\ell}^\times$ and we set $x = \psi((1+I_\ell)\gamma) \in \mathbb{F}_{\ell^2}^\times$, then

$$\mathrm{n}(\gamma) \mod \ell\mathbb{Z}_\ell = N_{\mathbb{F}_{\ell^2}^\times/\mathbb{F}_\ell^\times}(x). \tag{3.18}$$

LEMMA 3.15. *Γ_d is a normal subgroup of Γ_D, and $[\Gamma_D : \Gamma_d] c_p(d) = d$.*

PROOF. First of all, observe that since $1 + I_\ell$ is normal in $\mathcal{O}_{D/p,\ell}^\times$ and $(1+I_\ell) \setminus \mathcal{O}_{D/p,\ell}^\times \simeq \mathbb{F}_{\ell^2}^\times$ is abelian, $U_{d,\ell}$ is also normal in $\mathcal{O}_{D/p,\ell}^\times$. Now we prove that Γ_d is normal in Γ_D, which by means of the natural inclusion ν from (3.16) is equivalent to proving that

$$\nu(g^{-1}\gamma g) \in \nu(\Gamma_d) = \nu(\Gamma_D) \cap U_{d,\ell} \quad \text{for all } g \in \Gamma_D, \gamma \in \Gamma_d.$$

Since clearly $\nu(g^{-1}\gamma g) \in \nu(\Gamma_D)$, this holds if and only if $\nu(g^{-1}\gamma g) = \nu(g^{-1})\nu(\gamma)\nu(g) \in U_{d,\ell}$. And this is true because $U_{d,\ell}$ is normal in $\mathcal{O}_{D/p,\ell}^\times$, $\nu(g) \in \mathcal{O}_{D/p,\ell}^\times$ and $\nu(\gamma) \in U_{d,\ell}$.

Besides, it is clear that $\nu(\Gamma_d) \subseteq U_{d,\ell}$, thus composing ν with the natural quotient homomorphism $\mathcal{O}_{D/p,\ell}^\times \to U_{d,\ell} \setminus \mathcal{O}_{D/p,\ell}^\times$ we obtain a monomorphism

$$\Gamma_D/\Gamma_d \hookrightarrow U_{d,\ell} \setminus \mathcal{O}_{D/p,\ell}^\times.$$

Furthermore, the quotient of $U_{d,\ell} \setminus \mathcal{O}_{D/p,\ell}^\times$ by Γ_D/Γ_d can be identified with $\mathcal{C}_p(d)$, thus $d = [\Gamma_D : \Gamma_d] c_p(d)$ as claimed. Indeed, since

$$\widehat{\mathcal{O}}_{D/p}^{(p)\times} \setminus (B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times / B_{D/p}^\times$$

is trivial, it follows that every class in

$$\mathcal{C}_p(d) = U_d^{(p)} \setminus (B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times / B_{D/p}^\times$$

is represented by $(1, \dots, 1, a_\ell, 1, \dots)$ for some $a_\ell \in \mathcal{O}_{D/p,\ell}^\times$ modulo $U_{d,\ell}$. Even more, Γ_D acts transitively on these classes, and the stabiliser of an arbitrary class is $\Gamma_d \subseteq \Gamma_D$. □

While the integers $k(\Gamma_D)$ and $f(\Gamma_D)$ are both equal to 1, this might not be the case for the integers $k_d := k(\Gamma_d)$ and $f_d := f(\Gamma_d)$, but they are easily determined:

LEMMA 3.16. *k_d is the smallest positive integer such that $p^{k_d} \mod \ell$ belongs to $H_d \subseteq \mathbb{F}_{\ell^2}^\times$, and f_d is the smallest positive integer such that $p^{f_d} \mod \ell$ belongs to $N(H_d) \subseteq \mathbb{F}_\ell^\times$.*

PROOF. The integer k_d is the smallest positive integer such that $p^{k_d} \in \Gamma_d$. Since clearly $p \in B_{D/p}^\times$, k_d is actually the smallest positive integer such that $p^{k_d} \in U_d^p$. Further, as $p \in \mathcal{O}_{D/p,q}^\times$ for all primes $q \neq p$, we deduce that $p^{k_d} \in \Gamma_d$ if and only if $p^{k_d} \in U_{d,\ell}$. But using the isomorphism ψ from (3.17), this is equivalent to $p^{k_d} \mod \ell \in H_d$. As for the integer f_d, by Lemma 3.11 we know that f_d is the smallest positive integer such that $p^{f_d} \in \mathrm{n}(U_d^p)$. Since U_d is maximal outside ℓ, this condition is equivalent to saying that $p^{f_d} \in \mathrm{n}(U_{d,\ell})$. By (3.18), this happens if and only if $p^{f_d} \in N(H_d)$. □

REMARK 3.17. Plainly, the integers k_d and f_d are explicitly computable from ℓ, p and d. Indeed, let f be the order of $p \mod \ell$ in $\mathbb{F}_\ell^\times$. Equivalently, f is the order of the cyclic group $\langle p \mod \ell \rangle$ in $\mathbb{F}_\ell^\times \subseteq \mathbb{F}_{\ell^2}^\times$. Then k_d is the order of the image of $\langle p \mod \ell \rangle$ in $\mathbb{F}_{\ell^2}^\times / H_d$, thus

$$k_d = \frac{f}{\gcd(f, t_d)}, \quad \text{where } t_d := |H_d|.$$

Similarly, f_d is the order of the image of $\langle p \mod \ell \rangle$ in $\mathbb{F}_\ell^\times/N(H_d)$, hence using (3.5) and (3.6) we have

$$f_d = \frac{f}{\gcd(f, |N(H_d)|)}, \quad \text{where } |N(H_d)| = \frac{t_d}{\gcd(t_d, \ell+1)} = \frac{\ell-1}{\gcd(\ell-1, d)}.$$

Notice that the notation for the integer $f_d = f(\Gamma_d)$ is coherent with the notation used in Section 1.2. Indeed, once the integers k_d and f_d are determined, with $c_\infty(d) = c_p(d)f_d$, Proposition 3.12 (see also Remark 3.13) provides the p-adic uniformisation of the curve Y_d and makes more precise our digression in Section 1.2. Namely, one has a decomposition (over $\mathbb{Z}_p$)

$$\mathcal{Y}_d \simeq \bigsqcup_{i=1}^{c_p(d)} \mathcal{Y}_{\Gamma_d} \tag{3.19}$$

of $\mathcal{Y}_d$ as a union of its p-classes, all of them isomorphic to a curve $\mathcal{Y}_{\Gamma_d}/\mathbb{Z}_p$: two geometric connected components of $\mathcal{Y}_d$ belong to the same p-class if and only if both are geometric connected components of the same copy of $\mathcal{Y}_{\Gamma_d}$. Furthermore,

$$\mathcal{Y}_{\Gamma_d} \times_{\mathbb{Z}_p} \mathbb{Z}_{p^{f_d}} \simeq \bigsqcup_{\sigma \in \mathrm{Gal}\,(\mathbb{Z}_{p^{f_d}}/\mathbb{Z}_p)} {}^{\sigma}(\mathcal{Y}^0_{\Gamma_d}), \tag{3.20}$$

where $\mathcal{Y}^0_{\Gamma_d}/\mathbb{Z}_{p^{f_d}}$ is geometrically connected. Moreover, $\mathcal{Y}^0_{\Gamma_d}$ is isomorphic to either

a) the base change $\mathcal{M}_{\Gamma_{d,+}} \times_{\mathbb{Z}_p} \mathbb{Z}_{p^{f_d}}$ of the Mumford curve $\mathcal{M}_{\Gamma_{d,+}}/\mathbb{Z}_p$ to $\mathbb{Z}_{p^{f_d}}$, if $f_d = 2k_d$, or
b) the quadratic Frobenius twist $(\mathcal{M}_{\Gamma_{d,+}} \times_{\mathbb{Z}_p} \mathbb{Z}_{p^{f_d}})^\xi$, if $f_d = k_d$, where ξ is induced by the 1-cocycle

$$\mathrm{Gal}\,(\mathbb{Z}_{p^{2f_d}}/\mathbb{Z}_{p^{f_d}}) \longrightarrow \mathrm{Aut}(\mathcal{M}_{\Gamma_{d,+}} \times_{\mathbb{Z}_p} \mathbb{Z}_{p^{2f_d}}/\mathbb{Z}_{p^{2f_d}}), \quad \widetilde{\mathrm{Fr}}_p^{f_d} \mapsto w_p \times \mathrm{id},$$

where $w_p \in \Gamma_d$ represents the non-trivial class in $W = \Gamma_d/\Gamma_{d,+}$ (i.e., $w_p \in \Gamma_d$ is any element with $\mathrm{val}_p(\mathrm{n}(w_p)) = f_d$).

As a direct consequence, we find:

Proposition 3.18. *Assume $f_d > 1$, and let $K/\mathbb{Q}_p$ be a finite extension. If $\mathbb{Q}_{p^{f_d}} \not\subseteq K$, then the set $Y_d(K)$ is empty. In particular, $Y_d(\mathbb{Q}_p) = \emptyset$. In contrast, when $\mathbb{Q}_{p^{f_d}}$ is a subfield of K:*

a) *if $f_d = k_d$, then $Y_d(K) \neq \emptyset$ if and only if $(\mathcal{M}_{\Gamma_{d,+}} \times_{\mathbb{Z}_p} \mathbb{Z}_{p^{f_d}})^\xi(K) \neq \emptyset$.*
b) *if $f_d = 2k_d$, then $Y_d(K) \neq \emptyset$ if and only if $(\mathcal{M}_{\Gamma_{d,+}} \times_{\mathbb{Z}_p} \mathbb{Z}_{p^{f_d}})(K) \neq \emptyset$.*

Therefore, when $f_d > 1$ we can prove the non-existence of K-rational points on Y_d for *infinitely many* finite extensions $K/\mathbb{Q}_p$ (namely, for all $K/\mathbb{Q}_p$ not containing $\mathbb{Q}_{p^{f_d}}$ as a subfield), although the set $X_D(K)$ may be non-empty. By combining Proposition 3.18 with [**JL85**], we can give explicit sufficient conditions for $Y_d(K) = \emptyset$ and $X_D(K) \neq \emptyset$ to hold simultaneously. Because of its simplicity, let us point out the following particular case:

Corollary 3.19. *Assume $f_d > 1$, and let $K/\mathbb{Q}_p$ be a finite extension of $\mathbb{Q}_p$ whose residual degree $f(K/\mathbb{Q}_p)$ is even and such that $\mathbb{Q}_{p^{f_d}} \not\subseteq K$. Then $Y_d(K) = \emptyset$ and $X_D(K) \neq \emptyset$.*

Proof. The assertion $Y_d(K) = \emptyset$ follows from the previous proposition, whereas the non-emptiness of $X_D(K)$ follows from [**JL85**, Theorem 5.1]. □

Focusing on the study of $\mathbb{Q}_p$-rational points, again using the work of Jordan and Livné we find the following:

Corollary 3.20. *Assume $\ell \equiv 3 \pmod 4$ and $D = 2\ell q_1 \cdots q_{2r}$ for pairwise distinct primes $q_i \equiv 3 \pmod 4$, $1 \leq i \leq 2r$, $r \geq 0$. Let d be a positive divisor of $(\ell^2-1)/2$. If the order of 2 in $\mathbb{F}_\ell^\times$ does not divide $N_d := (\ell-1)/\gcd(\ell-1, d)$, then $Y_d(\mathbb{Q}_2) = \emptyset$, although $X_D(\mathbb{Q}_2) \neq \emptyset$.*

PROOF. By [**JL85**, Theorem 5.6], the set $X_D(\mathbb{Q}_2)$ is non-empty because every prime divisor of $D/2$ is congruent to 3 modulo 4. Hence, if we set $f := \mathrm{ord}_{\mathbb{F}_\ell^\times}(2)$, then we must show that $Y_d(\mathbb{Q}_2)$ is empty if f does not divide N_d.

From (3.4) and (3.6), the integer N_d is precisely the order of $N(H_d)$ in $\mathbb{F}_\ell^\times$, where $H_d \subseteq \mathbb{F}_{\ell^2}^\times$ is the unique subgroup of index d in $\mathbb{F}_{\ell^2}^\times$. From Remark 3.17, it is immediate that if f does not divide N_d then $f_d > 1$ (and conversely), hence the claim follows by applying Proposition 3.18. □

For each prime $\ell \equiv 3 \pmod 4$ with $3 < \ell < 25$, the positive divisors d of $(\ell^2-1)/2$ satisfying the conditions of the previous corollary are listed in Table 3.1. Thus by construction, for every pair (ℓ, d) in Table 3.1 we have $Y_d(\mathbb{Q}_2) = \emptyset$ and $X_D(\mathbb{Q}_2) \neq \emptyset$ for every D as in the statement of the corollary.

ℓ	$n = (\ell^2-1)/2$	positive divisors d of n with $f_d > 1$
7	24	3, 6, 12, 24
11	60	2, 4, 5, 6, 10, 12, 15, 20, 30, 60
19	180	2, 3, 4, 6, 9, 10, 12, 15, 18, 20, 30, 36, 45, 60, 90, 180
23	264	11, 22, 33, 44, 66, 88, 132, 264

TABLE 1. Some examples of pairs (ℓ, d) for which $Y_d(\mathbb{Q}_2) = \emptyset$ but $X_D(\mathbb{Q}_2) \neq \emptyset$.

Henceforth, we focus on the case $f_d = 1$ (in particular, $k_d = 1$ as well), that is to say, $p \bmod \ell \in N(H_d)$. According to the p-adic uniformisation of the curves Y_d described above, studying the existence of K-rational points on Y_d for finite extensions K of $\mathbb{Q}_p$ amounts to studying the existence of K-rational points on the twisted Mumford curve $\mathcal{M}^{\xi}_{\Gamma_{d,+}}$. As we show below, this can be done very much in the same way as it is done in [**JL85**] for the Shimura curve X_D. The rest of this section is thus devoted to prove Theorem 3.1.

Under the assumption $f_d = 1$, from (3.19) and (3.20) we have an isomorphism of $\mathbb{Z}_p$-schemes

$$\mathcal{Y}_d \simeq \coprod_{i=1}^{c_p(d)} \mathcal{Y}_{\Gamma_d},$$

where the curve $\mathcal{Y}_{\Gamma_d}/\mathbb{Z}_p$ is isomorphic to $\mathcal{M}^{\xi}_{\Gamma_{d,+}}/\mathbb{Z}_p$, the quadratic twist of the Mumford curve $\mathcal{M}_{\Gamma_{d,+}}/\mathbb{Z}_p$ by the 1-cocycle

$$\xi : \mathrm{Gal}\,(\mathbb{Z}_{p^2}/\mathbb{Z}_p) \longrightarrow \mathrm{Aut}(\mathcal{M}_{\Gamma_{d,+}} \times \mathbb{Z}_{p^2}/\mathbb{Z}_{p^2}), \quad \mathrm{Fr}_p \longmapsto w_p \times \mathrm{id}.$$

In particular, $\mathcal{Y}_{\Gamma_d}/\mathbb{Z}_p$ is an *admissible curve* in the sense of Definition 1.65, and its special fibre is therefore described by a graph with lengths (its *dual graph*). By virtue of Hensel's Lemma, there exists a K-rational point on Y_d if and only if the special fibre of a regular model of $\mathcal{Y}_{\Gamma_d} \times_{\mathbb{Z}_p} \mathcal{O}_K$ contains a smooth $\mathbb{F}_K$-rational point, where $\mathcal{O}_K$ and $\mathbb{F}_K$ are the ring of integers of K and its residue field, respectively. And the latter problem can be tackled by studying the combinatorics of the dual graph of $\mathcal{Y}_{\Gamma_d}$.

Using the notations of Section 5 in Chapter 1, the goal of Section 3.2 below is to determine and describe the dual graph $\mathcal{G}(\mathcal{Y}_{\Gamma_d}/\mathbb{Z}_p)$ of the admissible curve $\mathcal{Y}_{\Gamma_d}$. If $K/\mathbb{Q}_p$ is a finite extension with ring of integers $\mathcal{O}_K$ and residue field $\mathbb{F}_K$, then in Section 3.3 we conclude with a proof of Theorem 3.1 by translating the existence of a smooth $\mathbb{F}_K$-rational point on the special fibre of a regular model of $\mathcal{Y}_{\Gamma_d} \times_{\mathbb{Z}_p} \mathcal{O}_K$ (hence of a K-rational point on $\mathcal{Y}_{\Gamma_d}$, by Hensel's Lemma) into a combinatorial condition on $\mathcal{G}(\mathcal{Y}_{\Gamma_d}/\mathbb{Z}_p)$.

3.2. Combinatorics of the dual graphs. As above, we fix a positive divisor d of $(\ell^2-1)/2$ and the corresponding intermediate curve Y_d of the Shimura covering $X_{D,\ell} \to X_D$. Let U_d be the intermediate subgroup $\mathcal{U}_D \subseteq U_d \subseteq \widehat{\mathcal{O}}^\times$ defining the Shimura curve Y_d (with the convention that $-1 \in U_d$). When describing the p-adic uniformisation of Y_d, recall that we regard $\Gamma_d = U_d^{(p)} \cap B_{D/p}^\times$

as a subgroup of $\mathrm{GL}_2(\mathbb{Q}_p)$ through a fixed embedding $B_{D/p} \hookrightarrow B_{D/p,p} \simeq \mathrm{M}_2(\mathbb{Q}_p)$. We also defined the index two subgroup

$$\Gamma_{d,+} = \{\gamma \in \Gamma_d : \mathrm{val}_p(\mathrm{n}(\gamma)) \in 2\mathbb{Z}\} \subseteq \Gamma_d,$$

so that the non-trivial class in $W_d := \Gamma_d/\Gamma_{d,+}$ is represented by an element $w_p \in \Gamma_d$ with $\mathrm{val}_p(\mathrm{n}(w_p)) = 1$. If $\mathcal{T}_p$ denotes the Bruhat-Tits tree associated with $\mathrm{GL}_2(\mathbb{Q}_p)$, then the quotients

$$\mathcal{G}_d := \Gamma_d \setminus \mathcal{T}_p, \quad \mathcal{G}_{d,+} := \Gamma_{d,+} \setminus \mathcal{T}_p$$

are naturally finite graphs with lengths. Since the action of $Z(\mathrm{GL}_2(\mathbb{Q}_p)) = \mathbb{Q}_p^\times$ is trivial on $\mathcal{T}_p$, we can replace the groups Γ_d and $\Gamma_{d,+}$ by their images Γ'_d and $\Gamma'_{d,+}$ in $\mathrm{PGL}_2(\mathbb{Q}_p)$, respectively.

Observe that taking $d = 1$ we have $Y_1 = X_D$. In this case, $\Gamma_1 = \widehat{\mathcal{O}}_D^{(p)\times} =: \Gamma_D$ and the finite graphs with lengths $\mathcal{G}_D := \mathcal{G}_1$, $\mathcal{G}_{D,+} := \mathcal{G}_{1,+}$ are described in detail in [**Kur79**]. Let us write $\ell_D := \ell_1$ for the length function on $\mathcal{G}_D$ and $\mathcal{G}_{D,+}$. Since we will describe the finite graph with lengths $\mathcal{G}_d$ from $\mathcal{G}_D$, and then we will obtain a description of $\mathcal{G}_{d,+}$ from $\mathcal{G}_d$ in an analogous way as $\mathcal{G}_{D,+}$ is described from $\mathcal{G}_D$, let us start by recalling briefly the description of $\mathcal{G}_D$ (see *ibid.* for further details).

The set of vertices of $\mathcal{T}_p$ is by definition

$$\mathrm{Ver}(\mathcal{T}_p) = \mathrm{PGL}_2(\mathbb{Q}_p)/\mathrm{PGL}_2(\mathbb{Z}_p) \simeq B_{D/p,p}^\times/\mathbb{Q}_p^\times \mathcal{O}_{D/p,p}^\times,$$

and it is in bijection with the set of maximal orders $\mathcal{O}$ in $B_{D/p}$ which are locally equal to $\mathcal{O}_{D/p}$ at every prime $q \neq p$. If $\tilde{v} \in \mathrm{Ver}(\mathcal{T}_p)$ is represented by $g \in B_{D/p,p}^\times \simeq \mathrm{GL}_2(\mathbb{Q}_p)$, then the maximal order $\mathcal{O}_{\tilde{v}}$ corresponding to $\tilde{v}$ is the unique maximal order such that $\mathcal{O}_{\tilde{v},q} = \mathcal{O}_{D/p,q} = \mathcal{O}_{D/p} \otimes_{\mathbb{Z}} \mathbb{Z}_q$ for every finite prime q and $\mathcal{O}_{\tilde{v},p} = g\mathcal{O}_{D/p,p}g^{-1}$. The set of vertices $\mathrm{Ver}(\mathcal{G}_D)$ is then $\Gamma_D \setminus \mathrm{Ver}(\mathcal{T}_p)$, where Γ_D acts naturally on $\mathrm{Ver}(\mathcal{T}_p)$ by conjugation using the above description in terms of maximal orders.

The cardinality of $\mathrm{Ver}(\mathcal{G}_D)$ is $h := h(B_{D/p})$, the class number of $B_{D/p}$; write $\mathrm{Ver}(\mathcal{G}_D) = \{v_1, \ldots, v_h\}$, and choose maximal orders $\mathcal{O}_i := \mathcal{O}_{\tilde{v}_i}$ corresponding to vertices $\tilde{v}_i$ in $\mathcal{T}_p$ above v_i, for each $i = 1, \ldots, h$. The length $\ell_D(v_i)$ of v_i is defined to be the cardinality of $\mathrm{Stab}_{\Gamma'_D}(\tilde{v}_i) = \mathcal{O}_i^\times/\mathbb{Z}^\times$. Unless $D/p = 2$ or 3, it follows that $\ell_D(v_i) = 1$, 2, or 3. Further, deciding the number h_j of vertices in $\mathcal{G}_D$ of length j, for $j = 1, 2, 3$, amounts to computing the number of optimal embeddings of $\mathbb{Z}[\sqrt{-1}]$ and $\mathbb{Z}[(1+\sqrt{-3})/2]$ into the orders $\mathcal{O}_1, \ldots, \mathcal{O}_h$. By using Eichler's embedding theorems, it turns out (see [**Kur79**, p. 291]) that

$$h_2 = \frac{1}{2}\prod_{q|D/p}\left(1 - \left(\frac{-4}{q}\right)\right), \quad h_3 = \frac{1}{2}\prod_{q|D/p}\left(1 - \left(\frac{-3}{q}\right)\right), \quad h_1 = h - h_2 - h_3. \tag{3.21}$$

Similarly as for vertices, the length $\ell_D(y)$ of an edge $y \in \mathrm{Ed}(\mathcal{G}_D)$ is by definition the cardinality of $\mathrm{Stab}_{\Gamma'_D}(\tilde{y})$, where now $\tilde{y}$ is any edge in $\mathcal{T}_p$ above y. If $v = o(y)$ is the origin of the edge y and we choose lifts $\tilde{y}$ and $\tilde{v} = o(\tilde{y})$ in $\mathcal{T}_p$ of y and v, respectively, then $\mathrm{Stab}_{\Gamma'_D}(\tilde{y})$ is clearly a subgroup of $\mathrm{Stab}_{\Gamma'_D}(\tilde{v})$, thus $\ell_D(y)$ divides $\ell_D(v)$. Further, fixed $v \in \mathrm{Ver}(\mathcal{G}_D)$, the number of edges emanating from v having a given length is easily computed following the table in [**Kur79**, Proposition 4.2].

In order to describe the graph $\mathcal{G}_d$ from $\mathcal{G}_D$, recall from Lemma 3.15 that Γ_d is naturally a normal subgroup of Γ_D. Furthermore, under our assumption that $f_d = k_d = 1$, we have $p \in U_{d,\ell}$, so that $\Gamma_d = \Gamma_D \cap U_{d,\ell}$ contains $\Gamma_D \cap Z(\mathrm{GL}_2(\mathbb{Q}_p)) = \mathbb{Z}[1/p]^\times$, hence $\Gamma_d \cap Z(\mathrm{GL}_2(\mathbb{Q}_p)) = \mathbb{Z}[1/p]^\times$ as well. As a consequence, since both $\mathbb{Z}[1/p]^\times$ and Γ_d are normal in Γ_D we have

$$\Gamma'_D/\Gamma'_d = (\Gamma_D/\mathbb{Z}[1/p]^\times)/(\Gamma_d/\mathbb{Z}[1/p]^\times) \simeq \Gamma_D/\Gamma_d.$$

This implies that $d_{\mathcal{G}} := [\Gamma_D : \Gamma_d]$ is the degree of the natural projection map $\pi_d : \mathcal{G}_d \to \mathcal{G}_D$ (which is also the degree of $\pi_{d,+} : \mathcal{G}_{d,+} \to \mathcal{G}_{D,+}$). By Lemma 3.15, $d_{\mathcal{G}} c_p(d) = d$.

However, let us remark that the natural maps π_d and $\pi_{d,+}$ are not morphisms of graphs with lengths in general, in the sense that they preserve lengths, because they might not do it. Indeed,

let $\tilde{x}$ be either a vertex or an edge in $\mathcal{T}_p$ as before, and let x (resp. x_+) be its image in $\mathcal{G}_d$ (resp. $\mathcal{G}_{d,+}$). Then the length of x (resp. of x_+) is defined to be

$$\ell_d(x) := |\operatorname{Stab}_{\Gamma'_d}(\tilde{x})| \qquad (\text{resp. } \ell_{d,+}(x_+) := |\operatorname{Stab}_{\Gamma'_{d,+}}(\tilde{x})|).$$

It is easily seen that this definition does not depend on the representative $\tilde{x}$ in $\mathcal{T}_p$. Focusing first on the description of $\mathcal{G}_d$, we start by observing that the lengths

$$\ell_d(x) = |\operatorname{Stab}_{\Gamma'_d}(\tilde{x})| \quad \text{and} \quad \ell_D(\pi_d(x)) = |\operatorname{Stab}_{\Gamma'_D}(\tilde{x})|$$

are related by

$$\ell_D(\pi_d(x)) = |\operatorname{Stab}_{\Gamma'_D/\Gamma'_d}(\tilde{x})|\ell_d(x) = \frac{|\operatorname{Stab}_{\Gamma'_D}(\tilde{x})|}{|\operatorname{Stab}_{\Gamma'_D}(\tilde{x}) \cap \Gamma'_d|}\ell_d(x).$$

Under our assumption $\ell > 3$, $\ell_D(\pi_d(x)) = |\operatorname{Stab}_{\Gamma'_D}(\tilde{x})|$ is either 1, 2, or 3, hence

$$\ell_d(x) = \begin{cases} \ell_D(\pi_d(x)) & \text{if } \operatorname{Stab}_{\Gamma'_D}(\tilde{x}) \subseteq \Gamma'_d, \\ 1 & \text{if } \operatorname{Stab}_{\Gamma'_D}(\tilde{x}) \cap \Gamma'_d = \{1\}. \end{cases} \tag{3.22}$$

LEMMA 3.21. *Let $\tilde{v}$ be a vertex in $\mathcal{T}_p$, and write v for its image in $\mathcal{G}_d$.*

a) *If $\ell_D(\pi_d(v)) = 1$, then $\ell_d(v) = 1$.*
b) *If $\ell_D(\pi_d(v)) = 2$, then $\ell_d(v) = 2$ if and only if $4 \mid t_d$. Otherwise, $\ell_d(v) = 1$.*
c) *If $\ell_D(\pi_d(v)) = 3$, then $\ell_d(v) = 3$ if and only if $6 \mid t_d$. Otherwise, $\ell_d(v) = 1$.*

PROOF. The statement in a) is clear, since $\ell_D(\pi_d(v))$ is divisible by $\ell_d(v)$. By (3.22), in order to prove b) and c) we shall determine when $\operatorname{Stab}_{\Gamma'_D}(\tilde{v}) \subseteq \Gamma'_d$. Equivalently, we shall determine when $\operatorname{Stab}_{\Gamma_D}(\tilde{v}) \subseteq \Gamma_d$. If $\mathcal{O}_{\tilde{v}}$ denotes the maximal order corresponding to $\tilde{v}$, by using the monomorphism ν from (3.16) this inclusion holds if and only if $\nu(\mathcal{O}_{\tilde{v}}^\times)$ is a subgroup of $U_{d,\ell}$. Now the isomorphism $\psi : (1 + I_\ell) \setminus \mathcal{O}_{D/p,\ell}^\times \to \mathbb{F}_{\ell^2}^\times$ induces an isomorphism $U_{d,\ell} \setminus \mathcal{O}_{D/p,\ell}^\times \simeq \mathbb{F}_{\ell^2}^\times / H_d$, so that $\nu(\mathcal{O}_{\tilde{v}}^\times)$ is a subgroup of $U_{d,\ell}$ if and only if

$$\psi((1 + I_\ell)\nu(\mathcal{O}_{\tilde{v}}^\times))$$

is a subgroup of H_d.

Assume that $\ell_D(\pi_d(v)) = 2$, so that $\operatorname{Stab}_{\Gamma_D}(\tilde{v}) = \mathcal{O}_{\tilde{v}}^\times = \{\pm 1, \pm i\}$, where $i \in \mathcal{O}_{\tilde{v}}^\times$ satisfies $i^2 + 1 = 0$. By the above discussion we have $\ell_d(v) = 2$ if and only if $\psi((1 + I_\ell)\nu(i)) \in H_d$. First of all, observe that $\nu(i) \notin 1 + I_\ell$, because $\mathrm{n}(\nu(i) - 1) = 2 \notin \ell\mathbb{Z}$. And also notice that $\nu(i)^2 = -1 \notin 1 + I_\ell$, again because ℓ is odd. In other words, the image of $\nu(i)$ in $(1 + I_\ell) \setminus \mathcal{O}_{D/p,\ell}^\times$ has order 4, hence also $\psi((1 + I_\ell)\nu(i))$ has order 4. Being $\mathbb{F}_{\ell^2}^\times$ cyclic, it follows that $\psi((1 + I_\ell)\nu(i)) \in H_d$ if and only if 4 divides t_d, the order of H_d. This proves b).

If $\ell_D(\pi_d(v)) = 3$, then $\operatorname{Stab}_{\Gamma_D}(\tilde{v}) = \mathcal{O}_{\tilde{v}}^\times = \{\pm 1, \pm\omega, \pm\omega^2\}$, where $\omega \in \mathcal{O}_{\tilde{v}}^\times$ satisfies $\omega^2 + \omega + 1 = 0$, and we can proceed similarly as before. Since $\ell > 3$ and $\mathrm{n}(\nu(\omega) - 1) = \mathrm{n}(\nu(\omega^2) - 1) = 3$, we see that neither $\nu(\omega)$ nor $\nu(\omega^2)$ belong to $1 + I_\ell \subseteq \mathcal{O}_{D/p,\ell}^\times$. Moreover, $\omega^3 = -1$, so that we also have $\nu(\omega^3) \notin 1 + I_\ell$. Therefore, the image of $\nu(\omega)$ in $(1 + I_\ell) \setminus \mathcal{O}_{D/p,\ell}^\times$ must still have order 6, thus also the order of $\psi((1 + I_\ell)\nu(\omega))$ in $\mathbb{F}_{\ell^2}^\times$ is 6. Again, H_d is the unique (cyclic) subgroup of order t_d in $\mathbb{F}_{\ell^2}^\times$, thus we conclude that $\psi((1 + I_\ell)\nu(\omega)) \in H_d$ if and only if 6 divides t_d. This proves c). □

From this lemma, we can determine how many vertices of given length are in $\mathcal{G}_d$. Indeed, let v_0 be a vertex in $\mathcal{G}_D$, and let $\pi_d^{-1}(v_0) \subseteq \mathrm{Ver}(\mathcal{G}_d)$ be the set of vertices of $\mathcal{G}_d$ above v_0. If $\ell_D(v_0) = 1$, then it is clear that $\pi_d^{-1}(v_0)$ consists of $d_\mathcal{G}$ vertices of length 1. Besides, if $\ell_D(v_0) = 2$ (resp. 3), then $\pi_d^{-1}(v_0)$ consists of $d_\mathcal{G}$ vertices of length 2 (resp. 3) if $4 \mid t_d$ (resp. $6 \mid t_d$), and $d_\mathcal{G}/2$ (resp. $d_\mathcal{G}/3$) vertices of length 1 otherwise.

If for positive integers r, s, we set

$$\phi_r(s) = \begin{cases} 1 & \text{if } r \mid s, \\ 0 & \text{if } r \nmid s, \end{cases}, \quad \phi'_r(s) = 1 - \phi_r(s) = \begin{cases} 0 & \text{if } r \mid s, \\ 1 & \text{if } r \nmid s, \end{cases}$$

then we can summarise the above computations as follows:

COROLLARY 3.22. *Let h_i denote the number of vertices in $\mathcal{G}_D$ of length i, $i = 1, 2, 3$, as in (3.21). If $h_{d,i}$ denotes the number of vertices in $\mathcal{G}_d$ of length i, $i = 1, 2, 3$, then*

$$h_{d,2} = \phi_4(t_d) d_{\mathcal{G}} h_2, \quad h_{d,3} = \phi_6(t_d) d_{\mathcal{G}} h_3, \quad h_{d,1} = d_{\mathcal{G}}(h_1 + \frac{\phi_4'(t_d)h_2}{2} + \frac{\phi_6'(t_d)h_3}{3}),$$

and therefore the total number of vertices in $\mathcal{G}_d$ is computed as $h_d = h_{d,1} + h_{d,2} + h_{d,3}$.

COROLLARY 3.23. *With the above notations:*

a) *There exists a vertex of length 2 in $\mathcal{G}_d$ if and only if $\mathbb{Q}(\sqrt{-1})$ splits $B_{D/p}$ and $4 \mid t_d$.*
b) *There exists a vertex of length 3 in $\mathcal{G}_d$ if and only if $\mathbb{Q}(\sqrt{-3})$ splits $B_{D/p}$ and $6 \mid t_d$.*

We can also compute the lengths of the edges in $\mathcal{G}_d$. Fix a vertex v in $\mathcal{G}_d$, and let $\tilde{v}$ be a vertex of $\mathcal{T}_p$ above v. Then let $\mathrm{Star}(v)$ be the set of edges y of $\mathcal{G}_d$ with $o(y) = v$ and, analogously, let $\mathrm{Star}(\tilde{v})$ be the set of edges $\tilde{y}$ of $\mathcal{T}_p$ with $o(\tilde{y}) = \tilde{v}$. Recall that $|\mathrm{Star}(\tilde{v})| = p + 1$. There is a natural map $\mathrm{Star}(\tilde{v}) \to \mathrm{Star}(v)$, and $\ell_d(y)$ divides $\ell_d(v)$ for every $y \in \mathrm{Star}(v)$. Furthermore,

$$p + 1 = \sum_{y \in \mathrm{Star}(v)} \frac{\ell_d(v)}{\ell_d(y)}.$$

From this relation, it is clear that $\ell_d(y) = 1$ for every $y \in \mathrm{Star}(v)$ if $\ell_d(v) = 1$. Besides, if $\ell_d(v) = 2$ or 3, then the above equality can be rewritten as

$$p + 1 = \ell_d(v)|\{y \in \mathrm{Star}(v) : \ell_d(y) = 1\}| + |\{y \in \mathrm{Star}(v) : \ell_d(y) = \ell_d(v)\}|,$$

so that it is enough to determine how many edges of length $\ell_d(v)$ are in $\mathrm{Star}(v)$ to describe $\mathrm{Star}(v)$ completely. But this is the same local problem as in [**Kur79**, p. 292], thus we deduce the following:

PROPOSITION 3.24. *Given a vertex v in $\mathcal{G}_d$, its length $\ell_d(v) \in \{1, 2, 3\}$ can be computed by Lemma 3.21 and, according to the value of $\ell_d(v)$, the integers*

$$s_k(v) := |\{y \in \mathrm{Star}(v) : \ell_d(y) = k\}|, \quad k = 1, 2, 3,$$

can be obtained from the following table, where $(\frac{-4}{\cdot})$ and $(\frac{-3}{\cdot})$ denote the Kronecker symbol:

	$s_1(v)$	$s_2(v)$	$s_3(v)$
$\ell_d(v) = 1$	$p + 1$	0	0
$\ell_d(v) = 2$	$\frac{1}{2}(p - (\frac{-4}{p}))$	$1 + (\frac{-4}{p})$	0
$\ell_d(v) = 3$	$\frac{1}{3}(p - (\frac{-3}{p}))$	0	$1 + (\frac{-3}{p})$

We notice that the above table is the same as in [**Kur79**, Proposition 4.2], with the rows corresponding to $D/p = 2$ and 3 removed, as we have assumed $\ell > 3$. This proposition, together with Lemma 3.21 and Corollary 3.22 gives a precise description of the combinatorics of $\mathcal{G}_d$.

COROLLARY 3.25. *With the above notations:*

a) *There exists an edge of length 2 in $\mathcal{G}_d$ if and only if $\mathbb{Q}(\sqrt{-1})$ splits $B_{D/p}$, $4 \mid t_d$ and $p \not\equiv 3 \pmod 4$.*
b) *There exists an edge of length 3 in $\mathcal{G}_d$ if and only if $\mathbb{Q}(\sqrt{-3})$ splits $B_{D/p}$, $6 \mid t_d$ and $p \not\equiv 2 \pmod 3$.*

Now we describe the graph $\mathcal{G}_{d,+}$ by using the natural map $\mathcal{G}_{d,+} \to \mathcal{G}_d$, in the same way as it is done in [**Kur79**, Section 4] for $\mathcal{G}_{D,+}$ and $\mathcal{G}_D$. Namely, start by writing the set of vertices $\mathrm{Ver}(\mathcal{T}_p)$ of the Bruhat-Tits tree as $\mathrm{Ver}(\mathcal{T}_p) = V_1 \sqcup V_2$, in such a way that for every pair of vertices $\tilde{v}_i \in V_i$, $\tilde{v}_j \in V_j$, the distance between $\tilde{v}_i$ and $\tilde{v}_j$ is even if and only if $i = j$. Then, observe that $\Gamma_{d,+} V_i = V_i$ for $i = 1, 2$, whereas $\gamma V_1 = V_2$ and $\gamma V_2 = V_1$ for every $\gamma \in \Gamma_d - \Gamma_{d,+}$. Equivalently, this can be reformulated by saying that $\Gamma_{d,+} V_i = V_i$ for $i = 1, 2$ and $w_p V_1 = V_2$, $w_p V_2 = V_1$.

Therefore, every fibre of the natural maps

$$\mathrm{Ver}(\mathcal{G}_{d,+}) \to \mathrm{Ver}(\mathcal{G}_d) \quad \text{and} \quad \mathrm{Ed}(\mathcal{G}_{d,+}) \to \mathrm{Ed}(\mathcal{G}_d)$$

consists of two elements, and by construction we find the following:

PROPOSITION 3.26. *There exists no edge $y \in \mathrm{Ed}(\mathcal{G}_{d,+})$ such that $\bar{y} = y$. In particular,*

$$(\mathcal{G}(\mathcal{M}_{\Gamma_{d,+}}/\mathbb{Z}_p), F(\mathcal{M}_{\Gamma_{d,+}}/\mathbb{Z}_p)) \simeq (\mathcal{G}_{d,+}, \mathrm{id}),$$

that is, $\mathcal{G}_{d,+}$ is the dual graph of the Mumford curve $\mathcal{M}_{\Gamma_{d,+}}/\mathbb{Z}_p$. Further, the dual graph of $\mathcal{Y}_{\Gamma_d}/\mathbb{Z}_p$ is the same graph with lengths $\mathcal{G}_{d,+}$, but with Frobenius action given by w_p. That is to say,

$$(\mathcal{G}(\mathcal{Y}_{\Gamma_d}/\mathbb{Z}_p), F(\mathcal{Y}_{\Gamma_d}/\mathbb{Z}_p)) \simeq (\mathcal{G}_{d,+}, w_p).$$

PROOF. The non-existence of edges $y \in \mathrm{Ed}(\mathcal{G}_{d,+})$ such that $y = \bar{y}$ follows directly from the above construction of $\mathcal{G}_{d,+}$. This implies that $(\mathcal{G}_{d,+})^* = \mathcal{G}_{d,+}$, and therefore the isomorphism of pairs

$$(\mathcal{G}(\mathcal{M}_{\Gamma_{d,+}}/\mathbb{Z}_p), F(\mathcal{M}_{\Gamma_{d,+}}/\mathbb{Z}_p)) \simeq (\mathcal{G}_{d,+}, \mathrm{id}),$$

is consequence of [**Kur79**, Proposition 3.2]. Finally, by applying Propositions 1.69 and 3.12 we obtain that

$$(\mathcal{G}(\mathcal{Y}_{\Gamma_d}/\mathbb{Z}_p), F(\mathcal{Y}_{\Gamma_d}/\mathbb{Z}_p)) \simeq (\mathcal{G}_{d,+}, w_p).$$

□

Also, since w_p does not fix vertices or edges, it follows that the length of a vertex or an edge in $\mathcal{G}_{d,+}$ is the same as the length of its image in $\mathcal{G}_d$. In view of this, we will also write ℓ_d for the length function on $\mathcal{G}_{d,+}$. It will be clear from the context whether we use ℓ_d as the length function on $\mathcal{G}_{d,+}$ or on $\mathcal{G}_d$. In particular:

LEMMA 3.27. *The number of vertices of length i in $\mathcal{G}_{d,+}$, for $i = 1, 2, 3$, is $2h_{d,i}$, where the integers $h_{d,i}$ are as in Corollary 3.22. Further, if $v \in \mathrm{Ver}(\mathcal{G}_{d,+})$ is such that $\ell_d(v) = k$, $k \in \{1, 2, 3\}$, then the number of edges in $\mathrm{Star}(v)$ of length k is $s_k(v)$, where $s_k(v)$ is as in Proposition 3.24.*

On the other hand, there may exist edges y in $\mathcal{G}_d$ such that $\bar{y} = y$ (observe that such an edge exists if and only if there is an edge y' in $\mathcal{G}_{d,+}$ with $w_p(y') = \overline{y'}$). The existence of such edges can be detected by studying certain quadratic equations. Indeed, let us define a set of quadratic equations depending on p and d (and ℓ) in the following way:

$$\mathcal{F}_{p,d} := \begin{cases} \{x^2 + 2 = 0, x^2 + 2x + 2 = 0, x^2 - 2x + 2 = 0\} & \text{if } p = 2 \text{ and } 4 \mid t_d, \\ \{x^2 + 3 = 0, x^2 + 3x + 3 = 0, x^2 - 3x + 3 = 0\} & \text{if } p = 3 \text{ and } 6 \mid t_d, \\ \{x^2 + p = 0\} & \text{otherwise.} \end{cases} \tag{3.23}$$

LEMMA 3.28. *There exists an edge $y \in \mathrm{Ed}(\mathcal{G}_d)$ such that $\bar{y} = y$ if and only if Γ_d contains a root of some equation in $\mathcal{F}_{p,d}$.*

PROOF. Assume there exists an edge $y \in \mathrm{Ed}(\mathcal{G}_d)$ such that $\bar{y} = y$. Write $v = o(y)$, and let $\tilde{v} \in \mathrm{Ver}(\mathcal{T}_p)$ be a vertex above v. Let also $\tilde{y} \in \mathrm{Star}(\tilde{v})$ be an edge above y. Then there exists $\gamma \in \Gamma_d$ such that $\gamma(\tilde{y}) = \bar{\tilde{y}}$. In particular, $\gamma^2 \in \mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Q}_p)}(\tilde{v}) = \mathbb{Q}_p^\times \mathcal{O}_{\tilde{v},p}^\times$, so that we can write $\gamma^2 = p^n u$, for some $n \in \mathbb{Z}$ and $u \in \mathcal{O}_{\tilde{v},p}^\times$. Further, observe that $\mathrm{val}_p(\mathrm{n}(\gamma))$ must be odd, because the distance between $\tilde{v}$ and $\gamma(\tilde{v})$ is odd, hence n is odd. If $n = 2b + 1$, we can replace $p^{-b}\gamma$ by γ (because $p \in \Gamma_d$), thus we have $\gamma^2 = pu$, where $u \in \mathcal{O}_{\tilde{v}}^\times \cap U_{d,\ell}$ (locally at ℓ, $u \in U_{d,\ell}$ because both p and γ lie in Γ_d). Moreover, we have $\gamma \in \mathcal{O}_{\tilde{v}}$. Now, since u is a unit in $\mathcal{O}_{\tilde{v}}$, we have the following possibilities:

i) $u = \pm 1$,
ii) $u^2 + 1 = 0$, or
iii) $u^2 \pm u + 1 = 0$.

As in [**Kur79**, p. 295], the cases $u = 1$ and $u^2 + u + 1 = 0$ cannot occur. Furthermore, since (locally at ℓ) u must lie in $U_{d,\ell}$, the case $u^2 + 1 = 0$ (resp. $u^2 - u + 1 = 0$) can only occur if $4 \mid t_d$ (resp. $6 \mid t_d$). Therefore, again proceeding as in *loc. cit.*, the above three cases are translated, respectively, into the following three options:

I) γ is a root of $x^2 + p = 0$,

II) $p = 2$, $4 \mid t_d$ and γ is a root of $x^2 \pm 2x + 2 = 0$, or
III) $p = 3$, $6 \mid t_d$ and γ is a root of $x^2 \pm 3x + 3 = 0$.

Thus γ is a root in Γ_d of some equation in $\mathcal{F}_{p,d}$.

Conversely, if $\gamma \in \Gamma_d$ is a root of some equation in $\mathcal{F}_{p,d}$, then either condition I), II) or III) holds. In particular, choosing a vertex $\tilde{v}$ of $\mathcal{T}_p$ such that $\gamma \in \mathcal{O}_{\tilde{v}}$, then clearly there is some edge $\tilde{y} \in \mathrm{Star}(\tilde{v})$ such that $\gamma(\tilde{y}) = \bar{\tilde{y}}$, hence the image y of $\tilde{y}$ in $\mathcal{G}_d$ satisfies $\bar{y} = y$. □

For $d = 1$, so that $Y_1 = X_D$, $\Gamma_1 = \mathcal{O}_{D/p}^{(p)\times}$ and $\mathcal{G}_1 = \mathcal{G}_D$, conditions $4 \mid t_d$ and $6 \mid t_d$ are obviously satisfied, since $t_d = (\ell^2 - 1)/2$. Thus the above lemma is just the computation in [**Kur79**, p. 295]. By examining the equations in $\mathcal{F}_p := \mathcal{F}_{p,1}$, there is an edge $y \in \mathrm{Ed}(\mathcal{G}_D)$ such that $\bar{y} = y$ if and only if one of the following conditions holds:

i) $p = 2$ and either $\mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{-1})$ splits $B_{D/p}$,
ii) $p > 2$ and $\mathbb{Q}(\sqrt{-p})$ splits $B_{D/p}$.

This is equivalent to saying that a quadratic order containing the roots of some equation in $\mathcal{F}_p$ embeds into some maximal order in $B_{D/p}$, and more precisely the number of edges $y \in \mathrm{Ed}(\mathcal{G}_D)$ such that $\bar{y} = y$ can be computed by counting the number of inequivalent optimal embeddings from such quadratic orders into the maximal orders $\mathcal{O}_1, \ldots, \mathcal{O}_h$ (cf. *loc. cit.*).

Plainly, if Γ_d contains a root of some equation in $\mathcal{F}_{p,d}$, then $\Gamma_{d'}$ contains a root of some equation in $\mathcal{F}_{p,d'}$ for every $d' \mid d$. In terms of dual graphs, if $\mathcal{G}_d$ has an edge y satisfying $\bar{y} = y$, then its image y' in $\mathcal{G}_{d'}$ also verifies $\bar{y}' = y'$. In particular, if Γ_d contains a root of some equation in $\mathcal{F}_{p,d}$, then $\mathcal{O}_{D/p}^{(p)\times}$ contains a root of some equation in $\mathcal{F}_p = \mathcal{F}_{p,1}$.

In view of this, we shall study the existence of solutions in Γ_d of the quadratic equations in the set $\mathcal{F}_{p,d}$ assuming the existence of such solutions in $\mathcal{O}_{D/p}^{(p)\times}$. We carry out the details case by case in the next lemmas, where we make use of the natural morphism

$$\mathcal{O}_{D/p}^{(p)\times} \hookrightarrow \mathcal{O}_{D/p,\ell}^{\times} \longrightarrow (1 + I_\ell) \setminus \mathcal{O}_{D/p,\ell}^{\times} \xrightarrow{\psi} \mathbb{F}_{\ell^2}^{\times}$$

induced by ψ. If $\gamma \in \mathcal{O}_{D/p}^{(p)\times}$ is an arbitrary element, we write $\psi(\gamma)$ for its image in $\mathbb{F}_{\ell^2}^{\times}$ under the above composition. In particular, notice that $\gamma \in \Gamma_d$ if and only if $\psi(\gamma) \in H_d$.

LEMMA 3.29. *Assume that $\mathcal{O}_{D/p}^{(p)\times}$ has a root of $x^2 + p$. Then Γ_d has a root of $x^2 + p$ if and only if $4 \mid t_d$.*

PROOF. Let $\tau, -\tau \in \mathbb{F}_{\ell^2}^{\times}$ be the two roots of $x^2 + p$ in $\mathbb{F}_{\ell^2}^{\times}$. If $\gamma \in \mathcal{O}_{D/p}^{(p)\times}$ is a root of $x^2 + p$, then either $\psi(\gamma) = \tau$ or $\psi(\gamma) = -\tau$, and since $-1 \in H_d$, we deduce that $\gamma \in \Gamma_d$ if and only if $\tau \in H_d$. Observe that this condition does not depend on the choice of γ, hence assuming that $\mathcal{O}_{D/p}^{(p)\times}$ has a root of $x^2 + p$, we deduce that Γ_d has a root of $x^2 + p$ if and only if $\tau \in H_d$. Thus we shall prove that $-p$ is a square in H_d if and only if $4 \mid t_d$.

Indeed, under our running assumption $f_d = 1$, we have $p \mod \ell \in N(H_d)$, thus there exists an element $a \in H_d$ such that $a^{\ell+1} = p$ and it follows that p is a square in H_d. We deduce that $-p$ is a square in H_d if and only if so is -1, and this is equivalent to saying that 4 divides $t_d = |H_d|$. □

Next we consider the quadratic polynomials $F_p^{\pm}(x) := x^2 \pm px + p$ when p is either 2 or 3.

LEMMA 3.30. *Assume that p is either 2 or 3, and suppose that $\mathcal{O}_{D/p}^{(p)\times}$ has a root of either $F_p^+(x)$ or $F_p^-(x)$. Then Γ_d has a root of either $F_p^+(x)$ or $F_p^-(x)$ if and only if H_d has a root of $F_p^+(x)$ (or, equivalently, of $F_p^-(x)$).*

PROOF. Fix a root $\sigma_+ \in \mathbb{F}_{\ell^2}^{\times}$ of $F_p^+(x)$. Then the roots of $F_p^+(x)$ (resp. $F_p^-(x)$) in $\mathbb{F}_{\ell^2}^{\times}$ are σ_+ and $\sigma'_+ := -\sigma_+ - p$ (resp. $\sigma_- := -\sigma_+$ and $\sigma'_- := \sigma_+ + p$). With these notations, it is straightforward to check that the existence of a root $\gamma \in \mathcal{O}_{D/p}^{(p)\times}$ of either $F_p^+(x)$ or $F_p^-(x)$ implies that there are elements $\gamma_+, \gamma'_+, \gamma_-, \gamma'_- \in \mathcal{O}_{D/p}^{(p)\times}$ such that $\psi(\gamma_+) = \sigma_+$, $\psi(\gamma'_+) = \sigma'_+$, $\psi(\gamma_-) = \sigma_-$

and $\psi(\gamma_+) = \sigma'_-$ (for instance, if γ is a root of $F_p^+(x)$, then one can set $\gamma_+ := \gamma$, $\gamma'_+ := -\gamma - p$, $\gamma_- := -\gamma$ and $\gamma'_- := \gamma + p$).

Similarly as in the previous lemma, the fact that at least one of the roots σ_+, σ'_+, σ_- and σ'_- lies in H_d does not depend on the choice of γ. Therefore, assuming that $\mathcal{O}_{D/p}^{(p)\times}$ has a root of either $F_p^+(x)$ or $F_p^-(x)$, then Γ_d has a root of either $F_p^+(x)$ or $F_p^-(x)$ if and only if at least one of the roots σ_+, σ'_+, σ_- and σ'_- belongs to H_d. Using that $-1 \in H_d$, since $\sigma_- = -\sigma_+$ and $\sigma'_- = -\sigma'_+$, this is in turn equivalent to saying that either σ_+ or σ'_+ lies in H_d, and hence the statement follows. □

Corollary 3.31. *Assume that $f_d = 1$ as before. Then Γ_d contains a root of some equation in the set $\mathcal{F}_{p,d}$ if and only if one of the following conditions holds:*

i) *$\mathbb{Q}(\sqrt{-p})$ splits $B_{D/p}$ and $4 \mid t_d$,*
ii) *$p = 2$, $4 \mid t_d$, $\mathbb{Q}(\sqrt{-1})$ splits $B_{D/p}$ and H_d contains a root of $x^2 + 2x + 2 = 0$, or*
iii) *$p = 3$, $6 \mid t_d$, $\mathbb{Q}(\sqrt{-3})$ splits $B_{D/p}$ and H_d contains a root of $x^2 + 3x + 3 = 0$.*

3.3. Proof of Theorem 3.1. Finally, we can use now the description of the graphs $\mathcal{G}_d$ and $\mathcal{G}_{d,+}$ from the previous section to prove Theorem 3.1. If K is a finite extension of $\mathbb{Q}_p$, as we said above the existence of K-rational points on the curve Y_d is equivalent to the existence of K-rational points on $\mathcal{Y}_{\Gamma_d}$, and this question can be tackled by looking at the combinatorics of the graph with lengths $\mathcal{G}_{d,+}$.

Indeed, the curve $\mathcal{Y}_{\Gamma_d}/\mathbb{Z}_p$ is admissible, and by Proposition 3.26 its dual graph is the finite graph with lengths $\mathcal{G}_{d,+}$ with Frobenius action given by w_p. Let $\mathcal{O}_K$ and $\mathbb{F}_K \simeq \mathbb{F}_{p^{f_K}}$ be the ring of integers of K and its residue field, respectively, and write $f_K := f(K/\mathbb{Q}_p)$, $e_K := e(K/\mathbb{Q}_p)$. In order to study the existence of K-rational points on Y_d, we may look at the base change $\mathcal{Y}_{\Gamma_d,\mathcal{O}_K} := \mathcal{Y}_{\Gamma_d} \times_{\mathbb{Z}_p} \mathcal{O}_K$. By Hensel's Lemma, the set $\mathcal{Y}_{\Gamma_d,\mathcal{O}_K}(K)$ is not empty (hence so is $Y_d(K)$) if and only if the special fibre of a regular model of $\mathcal{Y}_{\Gamma_d,\mathcal{O}_K}$ has a smooth $\mathbb{F}_K$-rational point. We can obtain such a regular model by resolving singularities, and by Proposition 1.68 the result is still an admissible curve over $\mathcal{O}_K$, whose dual graph is the finite graph with lengths $\widetilde{\mathcal{G}_{d,+}^{e_K}}$, with Frobenius action given by $w_p^{f_K}$. The existence of a smooth $\mathbb{F}_K$-rational point on the special fibre is then read out from this graph.

With these observations, the next statement accounts for item a) in Theorem 3.1:

Proposition 3.32. *If f_K is even, then $Y_d(K) \neq \emptyset$.*

Proof. If f_K is even, then $w_p^{f_K}$ is the identity on $\mathcal{G}_{d,+}$, thus it is also the identity on $\widetilde{\mathcal{G}_{d,+}^{e_K}}$. In particular, every vertex v in $\widetilde{\mathcal{G}_{d,+}^{e_K}}$ is fixed by $w_p^{f_K}$, hence every component of the special fibre of $\widetilde{\mathcal{Y}_{\Gamma_d,\mathcal{O}_K}}$ is rational over $\mathbb{F}_K$. Since there are at most $p+1$ edges emanating from v, there are at most $p+1$ double points on the corresponding component. But since $f_K > 1$, this component has $p^{f_K} + 1 > p + 1$ points rational over $\mathbb{F}_K$, hence there is a smooth $\mathbb{F}_K$-rational point. By Hensel's Lemma, this completes the proof. □

In contrast, when f_K is odd the existence of a K-rational point is characterised in terms of the finite graph $\mathcal{G}_{d,+}$ as follows:

Proposition 3.33. *If f_K is odd, then $Y_d(K) \neq \emptyset$ if and only if there is an edge $y \in \mathcal{G}_{d,+}$ such that $e_K \ell_d(y)$ is even and $w_p(y) = \bar{y}$. Equivalently, if and only if there is an edge $y \in \mathrm{Ed}(\mathcal{G}_d)$ such that $e_K \ell_d(y)$ is even and $\bar{y} = y$.*

Proof. As explained above, by Hensel's Lemma we shall characterise the existence of a smooth $\mathbb{F}_K$-rational point on the special fibre $(\widetilde{\mathcal{Y}_{\Gamma_d,\mathcal{O}_K}})_0$, whose dual graph is $(\widetilde{\mathcal{G}_{d,+}^{e_K}}, w_p^{f_K})$.

If there is such a point, then $(\widetilde{\mathcal{Y}_{\Gamma_d,\mathcal{O}_K}})_0$ has a component rational over $\mathbb{F}_K$, that is, $\widetilde{\mathcal{G}_{d,+}^{e_K}}$ has a vertex fixed by $w_p^{f_K} = w_p$. But since w_p fixes no vertices on $\mathcal{G}_{d,+}$, this happens if and only if $\mathcal{G}_{d,+}^{e_K}$ has an edge y' of even length such that $w_p(y') = \bar{y'}$, which is the same as saying that $\mathcal{G}_{d,+}$ has an edge y such that $e_K \ell(y)$ is even and $w_p(y) = \bar{y}$.

Conversely, suppose $\mathcal{G}_{d,+}$ has en edge y with $e_K\ell(y)$ even and $w_p(y) = \bar{y}$. Then $\mathcal{G}_{d,+}^{e_K}$ has an edge y' of even length with $w_p(y') = \bar{y'}$. Again, we deduce that $\widetilde{\mathcal{G}_{d,+}^{e_K}}$ has a vertex fixed by w_p, which corresponds to an $\mathbb{F}_K$-rational component of $(\widetilde{\mathcal{Y}_{\Gamma_d,\mathcal{O}_K}})_0$ isomorphic to $\mathbb{P}^1_{\mathbb{F}_K}$ and having at most 2 double points. Since $2 < p^{f_K} + 1$, it follows that this component must have a smooth $\mathbb{F}_K$-rational point.

The second assertion in the statement follows immediately from the fact that the length of an edge in $\mathcal{G}_{d,+}$ and the length of its image in $\mathcal{G}_d$ is the same. □

By applying our description of the graphs $\mathcal{G}_{d,+}$ and $\mathcal{G}_d$, we end up with a proof of items b) and c) stated in Theorem 3.1.

COROLLARY 3.34. *Assume that f_K is odd.*

a) *If e_K is even, then $Y_d(K) \neq \emptyset$ if and only if one of the following conditions holds:*
   i) *$\mathbb{Q}(\sqrt{-p})$ splits $B_{D/p}$ and $4 \mid t_d$,*
   ii) *$p = 2$, $4 \mid t_d$, $\mathbb{Q}(\sqrt{-1})$ splits $B_{D/p}$ and H_d contains a root of $x^2 + 2x + 2 = 0$, or*
   iii) *$p = 3$, $6 \mid t_d$, $\mathbb{Q}(\sqrt{-3})$ splits $B_{D/p}$ and H_d contains a root of $x^2 + 3x + 3 = 0$.*

b) *If e_K is odd, then $Y_d(K) \neq \emptyset$ if and only if $p = 2$, every prime dividing $D/2$ is congruent to 3 mod 4 (in particular, $\ell \equiv 3 \mod 4$), $4 \mid t_d$ and either $\mathbb{Q}(\sqrt{-2})$ splits $B_{D/p}$ or H_d contains a root of $x^2 + 2x + 2$.*

PROOF. When e_K is even, Proposition 3.33 says that $Y_d(K) \neq \emptyset$ if and only if there is an edge $y \in \mathcal{G}_d$ such that $w_p(y) = \bar{y}$. Then a) follows directly from Lemma 3.28 and Corollary 3.31.

As for b), suppose that e_K is odd. Then we know that $X_D(K)$ is empty unless $p = 2$ or $D = 2p$. Since $\ell > 3$, we can assume that $p = 2$, as otherwise $X_D(K)$ is empty and therefore $Y_d(K)$ is necessarily empty as well (we could also deduce this by using Proposition 3.33 and our study of $\mathcal{G}_{d,+}$).

If $Y_d(K)$ is not empty, Proposition 3.33 implies the existence of an edge $y \in \mathcal{G}_d$ such that $\ell_d(y) = 2$ and $\bar{y} = y$. By Corollary 3.25 and Lemma 3.28, this is equivalent to saying that $\mathbb{Q}(\sqrt{-1})$ splits $B_{D/p}$, $4 \mid t_d$ and Γ_d contains a root of some equation in $\mathcal{F}_{2,d}$. Using Lemmas 3.29 and 3.30, this is equivalent to saying that $\mathbb{Q}(\sqrt{-1})$ splits $B_{D/p}$, $4 \mid t_d$ and either $\mathbb{Q}(\sqrt{-2})$ splits $B_{D/p}$ or H_d contains a root of $x^2 + 2x + 2$. Here notice that the condition that $\mathbb{Q}(\sqrt{-1})$ splits $B_{D/p}$ is equivalent to saying that every prime dividing D/p is congruent to 3 mod 4, thus we find b).

Conversely, suppose that $\mathbb{Q}(\sqrt{-1})$ splits $B_{D/p}$, $4 \mid t_d$ and either $\mathbb{Q}(\sqrt{-2})$ splits $B_{D/p}$ or H_d contains a root of x^2+2x+2. Since $\mathbb{Q}(\sqrt{-1})$ splits $B_{D/p}$ and $4 \mid t_d$, we can choose $\gamma \in \Gamma_d$ satisfying $\gamma^2 + 1 = 0$, and there is a vertex $\tilde{v} \in \mathrm{Ver}(\mathcal{T}_p)$ such that $\gamma(\tilde{v}) = \tilde{v}$, so that $\mathrm{Stab}_{\Gamma'_{d,+}}(\tilde{v}) = \{[1], [\gamma]\}$. If v is the image of $\tilde{v}$ in $\mathcal{G}_d$ (or in $\mathcal{G}_{d,+}$), then $\ell_d(v) = 2$.

Now if $\mathbb{Q}(\sqrt{-2})$ splits $B_{D/p}$, there is an element $\gamma' \in \mathcal{O}_{D/2}^{(2)\times}$ such that $(\gamma')^2 + 2 = 0$. Since $4 \mid t_d$, Lemma 3.29 implies that actually $\gamma' \in \Gamma_d$. Having norm 2, γ' induces the same element as w_2 in $\Gamma_d/\Gamma_{d,+}$, hence the image y in $\mathcal{G}_d$ of the edge $\tilde{y} := \tilde{v} \to \gamma'(\tilde{v})$ satisfies $\ell_d(y) = 2$ and $\bar{y} = y$.

On the other hand, suppose H_d contains a root of the quadratic equation $x^2 + 2x + 2$. Since $\gamma - 1$ and $-\gamma - 1$ are roots in $\mathcal{O}_{D/2}^{(2)\times}$ of $x^2 + 2x + 2 = 0$, and they map to the two distinct roots of this quadratic equation in $\mathbb{F}_{\ell^2}^\times$, at least one of them lies in H_d by assumption, so either $\gamma - 1$ or $-\gamma - 1$ belongs to Γ_d. Let us write $\gamma' = \gamma - 1$ or $-\gamma - 1$ accordingly. Similarly as before, define $\tilde{v}' := \gamma'(\tilde{v})$ and let $\tilde{y} = \tilde{v} \to \tilde{v}' \in \mathrm{Ed}(\mathcal{T}_p)$. The element γ also fixes $\tilde{v}'$, and therefore the image y of $\tilde{y}$ in $\mathcal{G}_d$ satisfies $\ell_d(y) = 2$ and $\bar{y} = y$. This finishes the proof of b). □

Combining Theorem 3.1 with [**JL85**, Theorems 5.4, 5.6], we can give explicit conditions for the set $Y_d(K)$ to be empty even in cases where $X_D(K)$ is not.

COROLLARY 3.35. *Assuming that $f_d = 1$, suppose that one of the following conditions is satisfied:*

a) *$p \neq 2, 3$, $\mathbb{Q}(\sqrt{-p})$ splits $B_{D/p}$ and $4 \nmid t_d$;*

b) *$p = 2$, and either*

i) $\mathbb{Q}(\sqrt{-2})$ *splits* $B_{D/2}$ *and* $4 \nmid t_d$, *or*
ii) $\mathbb{Q}(\sqrt{-1})$ *splits* $B_{D/2}$ *and either* $4 \nmid t_d$ *or* H_d *does not contain any root of* $x^2+2x+2 = 0$.

c) $p = 3$, $\mathbb{Q}(\sqrt{-3})$ *splits* $B_{D/3}$, $4 \nmid t_d$ *and either* $6 \nmid t_d$ *or* H_d *does not contain any root of* $x^2 + 3x + 3 = 0$.

If $K/\mathbb{Q}_p$ *is any finite extension such that* $f(K/\mathbb{Q}_p)$ *is odd and* $e(K/\mathbb{Q}_p)$ *is even, then* $X_D(K) \neq \emptyset$ *and* $Y_d(K) = \emptyset$.

COROLLARY 3.36. *Assuming that* $f_d = 1$, *suppose that* $p = 2$, *every prime dividing* $D/2$ *is congruent to* 3 *modulo* 4 *and either* $4 \nmid t_d$ *or* $\mathbb{Q}(\sqrt{-2})$ *does not split* $B_{D/2}$ *and* H_d *does not contain any root of* $x^2 + 2x + 2 = 0$. *If* $K/\mathbb{Q}_p$ *is any finite extension such that both* $f(K/\mathbb{Q}_p)$ *and* $e(K/\mathbb{Q}_p)$ *are even, then* $X_D(K) \neq \emptyset$ *and* $Y_d(K) = \emptyset$.

4. $\mathbb{Q}_p$-rational points on Atkin-Lehner quotients of Y_d

After studying local points on the curves Y_d, we now focus on the study of $\mathbb{Q}_p$-rational points on the quotients of these curves by the lifted Atkin-Lehner involutions $\hat{\omega}_m$ attached to positive divisors m of D. By analogy to the classical case, we call these curves *Atkin-Lehner quotients of* Y_d, and we denote by $Y_d^{(m)}$ the quotient of Y_d by the action of $\hat{\omega}_m$. In order to simplify the discussion, we assume throughout that $Y_d(\mathbb{Q}_p) = \emptyset$, as otherwise the sets $Y_d^{(m)}(\mathbb{Q}_p)$ are clearly non-empty for every positive divisor m of D as well. Equivalently, we thus assume that $\mathcal{Y}_{\Gamma_d}(\mathbb{Q}_p) = \emptyset$.

Again, we exploit the p-adic uniformisation of the curves Y_d worked out in Section 3.1. As it happens when studying the curves Y_d, there is a big difference between the cases $f_d = 1$ and $f_d > 1$. Moreover, in cases where Y_d is not geometrically connected we shall take into account whether $\varepsilon_d(m) = 1$ or not (i.e., whether $\hat{\omega}_m$ acts trivially on the set $\mathcal{C}_\infty(d)$ or not). After some considerations regarding these questions, we will soon restrict ourselves to the case $f_d = 1$ and $\varepsilon_d(m) = 1$. Our study of the existence of $\mathbb{Q}_p$-rational points on the curves $Y_d^{(m)}$ then borrows some of the ideas in Kurihara's and Ogg's work (cf. [**Kur79**], [**Ogg85**]).

4.1. p-adic uniformisation of the curves $Y_d^{(m)}$ and first considerations. We fix as usual a positive divisor d of $(\ell^2-1)/2$ and the corresponding intermediate curve Y_d of $X_{D,\ell} \to X_D$. Let also p be a prime dividing D/ℓ. Recall from Section 3.1 that Čerednik-Drinfeld theory applied to the curves Y_d provides us with isomorphisms

$$\mathcal{Y}_d \simeq \coprod_{i=1}^{c_p(d)} \mathcal{Y}_{\Gamma_d}, \qquad \mathcal{Y}_{\Gamma_d} \times_{\mathbb{Z}_p} \mathbb{Z}_{p^{f_d}} \simeq \coprod_{j=0}^{f_d-1} \widetilde{\mathrm{Fr}}_p^{\,j}(\mathcal{Y}^0_{\Gamma_d}),$$

where $\mathcal{Y}_{\Gamma_d}$ is defined over $\mathbb{Z}_p$ and $\mathcal{Y}^0_{\Gamma_d}/\mathbb{Z}_{p^{f_d}}$ is isomorphic to either the base change of the Mumford curve $\mathcal{M}_{\Gamma_{d,+}}$ to $\mathbb{Z}_{p^{f_d}}$ or a quadratic twist of it (cf. (3.19) and (3.20)). From these isomorphisms we also recover the fact that the $c_\infty(d) = c_p(d)f_d$ geometric connected components of Y_d, indexed by the set $\mathcal{C}_\infty(d)$, are classified into $c_p(d)$ distinct p-classes, one for each element in $\mathcal{C}_p(d)$, corresponding to the $c_p(d)$ copies of the curve $\mathcal{Y}_{\Gamma_d}/\mathbb{Z}_p$. This corresponds with the natural quotient map

$$\mathcal{C}_\infty(d) \simeq \mathbb{F}_\ell^\times/N(H_d) \longrightarrow \mathcal{C}_p(d) \simeq \mathbb{F}_\ell^\times/N(H_d)\langle p\rangle.$$

Fix a positive divisor m of D. If $\hat{\omega}_m$ acts trivially on the set $\mathcal{C}_\infty(d)$ of geometric connected components of Y_d, (i.e., $\varepsilon_d(m) = 1$) then it obviously acts trivially as well on the set $\mathcal{C}_p(d)$ of p-classes. And when this is the case, we can predict easily the non-existence of $\mathbb{Q}_p$-rational points on $Y_d^{(m)}$ in many instances:

PROPOSITION 3.37. *Assume that* $Y_d(\mathbb{Q}_p) = \emptyset$ *and* $\varepsilon_d(m) = 1$. *If* $f_d > 1$, *then* $Y_d^{(m)}(\mathbb{Q}_p) = \emptyset$.

PROOF. Under the hypothesis $\varepsilon_d(m) = 1$, the involution $\hat{\omega}_m$ induces an involution on each geometric connected component of Y_d, which we still denote by $\hat{\omega}_m$. In particular, $\mathcal{Y}_d^{(m)}$ still

decomposes over $\mathbb{Z}_p$ as $c_p(d)$ copies of a curve $\mathcal{Y}_{\Gamma_d}^{(m)}$ (namely, the quotient of $\mathcal{Y}_{\Gamma_d}$ by $\hat{\omega}_m$), and each of these curves has f_d geometric connected components, which are only defined over $\mathbb{Z}_{p^{f_d}}$ and conjugated by $\mathrm{Gal}\,(\mathbb{Z}_{p^{f_d}}/\mathbb{Z}_p)$. In particular, $\mathcal{Y}_{\Gamma_d}^{(m)}(\mathbb{Q}_p)$ is empty, hence so is the set $Y_d^{(m)}(\mathbb{Q}_p)$.

Alternatively, suppose there exists a point $P \in Y_d^{(m)}(\mathbb{Q}_p) = \emptyset$. Then there must be a point $Q \in Y_d(\bar{\mathbb{Q}}_p)$ such that $\{Q, \hat{\omega}_m(Q)\}$ is stable under the action of $\mathrm{Gal}\,(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$. But notice that both Q and $\hat{\omega}_m(Q)$ lie in the same geometric connected component of $\mathcal{Y}_d$. However, if $\sigma \in \mathrm{Gal}\,(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ induces a non-trivial automorphism in $\mathrm{Gal}\,(\mathbb{Q}_{p^{f_d}}/\mathbb{Q}_p)$, then $\sigma(Q)$ lies in a different geometric connected component of $\mathcal{Y}_d$ as Q, hence $\sigma(Q) \notin \{Q, \hat{\omega}_m(Q)\}$, a contradiction. □

Besides, if $\varepsilon_d(m) \neq 1$ it is important to distinguish whether $\hat{\omega}_m$ acts on each p-class of geometric connected components or not. In this regard:

LEMMA 3.38. *Assume that $\varepsilon_d(m) \neq 1$. Then $\hat{\omega}_m$ acts trivially on the set $\mathcal{C}_p(d)$ of p-classes if and only if the integer f_d is even.*

PROOF. Suppose that $\varepsilon_d(m) \neq 1$, i.e. $\varepsilon(m) = -1$ and $-1 \notin N(H_d)$. In particular, this implies that $|N(H_d)|$ is odd. By construction, the action of $\hat{\omega}_m$ on the set $\mathcal{C}_p(d) \simeq \mathbb{F}_\ell^\times / N(H_d)\langle p \rangle$ is trivial if and only if $-1 \in N(H_d)\langle p \rangle$. Being $\mathbb{F}_\ell^\times$ cyclic, this holds if and only if the order of $N(H_d)\langle p \rangle$ is even. And since $|N(H_d)|$ is odd, this is in turn equivalent to saying that the order of p in $\mathbb{F}_\ell^\times / N(H_d)$ is even. But this is exactly the same as f_d being even. □

PROPOSITION 3.39. *Assume that $\varepsilon_d(m) \neq 1$ and $Y_d(\mathbb{Q}_p) = \emptyset$. If $f_d \neq 2$, then $Y_d^{(m)}(\mathbb{Q}_p) = \emptyset$.*

PROOF. Suppose that $\varepsilon_d(m) \neq 1$ and $Y_d(\mathbb{Q}_p) = \emptyset$, and assume first that f_d is odd. By the previous lemma, $\hat{\omega}_m$ acts non-trivially on the set $\mathcal{C}_p(d)$ (in particular, $c_p(d)$ is even), and therefore $\mathcal{Y}_d^{(m)}/\mathbb{Z}_p$ is isomorphic (over $\mathbb{Z}_p$) to $c_p(d)/2$ copies of the curve $\mathcal{Y}_{\Gamma_d}$. Since $Y_d(\mathbb{Q}_p) = \emptyset$ by hypothesis, $\mathcal{Y}_{\Gamma_d}(\mathbb{Q}_p)$ is empty and the statement follows. Alternatively, suppose there is a $\mathbb{Q}_p$-rational point $P \in Y_d^{(m)}(\mathbb{Q}_p)$. Then there is a point $Q \in Y_d(\bar{\mathbb{Q}}_p)$ such that the set $\{Q, \hat{\omega}_m(Q)\}$ is stable under the action of $\mathrm{Gal}\,(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$. But since $Y_d(\mathbb{Q}_p)$ is empty, there exists some $\sigma \in \mathrm{Gal}\,(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ such that $\sigma(Q) = \hat{\omega}_m(Q)$. However, this is not possible, because $\sigma(Q)$ lies in the same p-class as Q, whereas $\hat{\omega}_m(Q)$ does not.

Now assume that f_d is even and $f_d \neq 2$. By the previous lemma, $\hat{\omega}_m$ acts trivially on the set of p-classes. Therefore, $\hat{\omega}_m$ induces an involution on each copy of $\mathcal{Y}_{\Gamma_d}$, which we still denote by $\hat{\omega}_m$. But since $\varepsilon_d(m) \neq 1$, $\hat{\omega}_m$ identifies the f_d geometric connected components of $\mathcal{Y}_{\Gamma_d}$ in pairs, and it follows that $\mathcal{Y}_{\Gamma_d}^{(m)} := \mathcal{Y}_{\Gamma_d}/\langle \hat{\omega}_m \rangle$ decomposes over $\mathbb{Z}_{p^{f_d/2}}$ as the disjoint union of $f_d/2$ geometrically connected curves, all of them defined over $\mathbb{Z}_{p^{f_d/2}}$ and conjugated by $\mathrm{Gal}\,(\mathbb{Z}_{p^{f_d/2}}/\mathbb{Z}_p)$. As a consequence the set $\mathcal{Y}_{\Gamma_d}^{(m)}(\mathbb{Q}_p)$ is empty because $f_d/2 > 1$, so $Y_d^{(m)}(\mathbb{Q}_p)$ is empty as well. □

REMARK 3.40. Recall that both $\varepsilon_d(m)$ and f_d can be easily computed, by using (3.7) together with Lemma 3.5 and Remark 3.17, respectively. Therefore, by combining Theorem 3.1 with Propositions 3.37 and 3.39, we can provide many concrete instances where the set $Y_d^{(m)}(\mathbb{Q}_p)$ is empty.

REMARK 3.41. When $\varepsilon_d(m) \neq 1$, Proposition 3.39 leaves open the question of determining whether $Y_d^{(m)}(\mathbb{Q}_p)$ is empty or not only in the case $f_d = 2$. This corresponds to the situation where $\mathcal{Y}_{\Gamma_d}$ decomposes over $\mathbb{Z}_{p^2}$ as the disjoint union of a geometrically connected curve $\mathcal{Y}_{\Gamma_d}^0/\mathbb{Z}_{p^2}$ and its Frobenius conjugate $\mathcal{Y}_{\Gamma_d}^1 := \widetilde{\mathrm{Fr}}_p(\mathcal{Y}_{\Gamma_d}^0)$, which are permuted also by the action of $\hat{\omega}_m$. The Atkin-Lehner quotient $\mathcal{Y}_{\Gamma_d}^{(m)}$ is therefore a model for $\mathcal{Y}_{\Gamma_d}^0$ over $\mathbb{Z}_p$. The twists of Mumford curves that one needs to deal with in order to study the existence of $\mathbb{Q}_p$-rational points on $\mathcal{Y}_{\Gamma_d}^{(m)}$ in this setting are not in the scope of this thesis, so we will not consider this particular case.

We thus assume for the rest of the chapter that $f_d = 1$ and $\varepsilon_d(m) = 1$. In particular, notice that $\mathcal{Y}_d/\mathbb{Z}_p$ decomposes completely over $\mathbb{Z}_p$ (in other words, $c_\infty(d) = c_p(d)$). Hence we have an

isomorphism of $\mathbb{Z}_p$-schemes

$$\mathcal{Y}_d^{(m)} \simeq \coprod_{i=1}^{c_p(d)} \mathcal{Y}_{\Gamma_d}^{(m)}, \tag{3.24}$$

where $\mathcal{Y}_{\Gamma_d}^{(m)}$ stands for the quotient of $\mathcal{Y}_{\Gamma_d}$ by the action of the involution induced by $\hat{\omega}_m$ on $\mathcal{Y}_{\Gamma_d}$, which we still denote $\hat{\omega}_m$. Recall that $\mathcal{Y}_{\Gamma_d}/\mathbb{Z}_p$ is the quadratic twist $\mathcal{M}^{\xi}_{\Gamma_{d,+}}$ of the Mumford curve over $\mathbb{Z}_p$ associated with $\Gamma_{d,+}$ by the cohomology class corresponding to the 1-cocycle

$$\xi : \mathrm{Gal}\,(\mathbb{Z}_{p^2}/\mathbb{Z}_p) \longrightarrow \mathrm{Aut}(\mathcal{M}_{\Gamma_{d,+}} \times_{\mathbb{Z}_p} \mathbb{Z}_{p^2}/\mathbb{Z}_{p^2}), \quad \widetilde{\mathrm{Fr}}_p \longmapsto w_p \times \mathrm{id}.$$

As we did for the curve Y_d, next we study the existence of $\mathbb{Q}_p$-rational points on the curve $\mathcal{Y}_{\Gamma_d}^{(m)}$ (hence on $\mathcal{Y}_d^{(m)}$) by studying the existence of smooth $\mathbb{F}_p$-rational points on the special fibre of a regular model and applying Hensel's Lemma. And for this, we translate again the problem into a combinatorial issue on the dual graph $\mathcal{G}_{d,+}$ of the admissible curve $\mathcal{Y}_{\Gamma_d}/\mathbb{Z}_p$.

Remark 3.42. As pointed out in Remark 2.18, the Atkin-Lehner involutions on X_D can be lifted to $X_{D,\ell}$ in more than one way, although the structure of $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ as an abstract group does not depend on the choice of the involutions $\hat{\omega}_m$.

When considering intermediate curves Y_d and an Atkin-Lehner involution ω_m, it might still be the case that $\mathrm{Aut}^{\mathrm{mod}}(Y_d)$ contains more than one involution lifting ω_m. And in certain cases, the action of these lifted involutions on the set $\mathcal{C}_\infty(d)$ can be different (this will not be the case, of course, if Y_d is geometrically connected, for example). Nevertheless, we remark that when this occurs, the quotients of Y_d by different lifts of ω_m are different curves. Throughout this chapter, we always consider $\hat{\omega}_m$ to be the lifted Atkin-Lehner involution as in Definition 2.10.

4.2. $\mathbb{Q}_p$-rational points on $Y_d^{(p)}$. We start by studying the Atkin-Lehner quotient of Y_d by the involution $\hat{\omega}_p$, where recall that we are always assuming that $p \neq \ell$. First of all, we notice that the hypothesis $f_d = 1$ already implies that $\varepsilon_d(p) = 1$, thus we do not need to make this extra assumption:

Lemma 3.43. *Under the hypothesis $f_d = 1$, we always have $\varepsilon_d(p) = 1$. Furthermore, the action of $\hat{\omega}_p$ on the curve $\mathcal{Y}_{\Gamma_d}$ corresponds to the involution induced by w_p on $\mathcal{M}^{\xi}_{\Gamma_{d,+}}$.*

Proof. Our assumption $f_d = 1$ implies that $c_p(d) = c_\infty(d)$. If this integer is odd, then it must be $\varepsilon_d(p) = 1$. Assume on the contrary that $c_p(d) = c_\infty(d)$ is even. This means that $N(H_d)$ is a subgroup of $\mathbb{F}_\ell^{\times 2} \subseteq \mathbb{F}_\ell^\times$, the subgroup of $\mathbb{F}_\ell^\times$ consisting of the quadratic residues modulo ℓ. Since $f_d = 1$ is equivalent to $p \mod \ell$ being in $N(H_d)$, it follows that $(\frac{p}{\ell}) = 1$, hence $\varepsilon(p) = 1$, so that $\varepsilon_d(p) = 1$ as well. This proves the first assertion.

As for the second part, the action of the lifted involution $\hat{\omega}_p$ on $\widehat{\mathcal{Y}}_d$, the p-adic counterpart of $Y_d \times_{\mathbb{Q}} \bar{\mathbb{Q}}$, is induced (through (3.12)) by the modular automorphism

$$\rho_{U_d}(1, \dots, 1, \mathrm{w}_p, 1, \dots, 1, \alpha_p, 1, \dots) = \rho_{U_d}(\mathrm{w}_p)\rho_{U_d}(\alpha_p) : Y_d \longrightarrow Y_d,$$

with

$$\mathrm{w}_p = \begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix} \in \mathcal{O}_{D,p} \quad \text{and} \quad \alpha_p = \begin{pmatrix} s_p & 0 \\ 0 & \bar{s}_p \end{pmatrix} \in \mathcal{O}_{D,\ell}^\times,$$

where $s_p \in \mathbb{Z}_{\ell^2}^\times$ reduces to a square root of p modulo ℓ in $\mathbb{F}_{\ell^2}^\times$, and $a \mapsto \bar{a}$ denotes the non-trivial automorphism in $\mathrm{Gal}\,(\mathbb{Z}_{\ell^2}/\mathbb{Z}_\ell)$. By the assumption $f_d = 1$, the automorphism induced by $\rho_{U_d}(\mathrm{w}_p)$ acts on $\mathcal{Y}_{\Gamma_d}$ as the involution induced by w_p, via the isomorphism (3.12). Therefore, we need to show that $\rho_{U_d}(\alpha_p)$ induces the identity isomorphism, which is equivalent to showing that $\alpha_p \in U_{d,\ell}$. But since we are assuming that $f_d = 1$, it turns out that $p \mod \ell = x^{\ell+1}$ for some $x \in H_d \subseteq \mathbb{F}_{\ell^2}^\times$. Since ℓ is odd, in particular $p \mod \ell$ is the square of an element in H_d. Hence, the reduction of s_p to $\mathbb{F}_{\ell^2}^\times$ lies in H_d, which implies that $\alpha_p \in U_{d,\ell}$ and the statement follows. □

As a consequence of this lemma, an integral model $\mathcal{Y}_d^{(p)}/\mathbb{Z}_p$ of the Atkin-Lehner quotient $Y_d^{(p)}$ is obtained by taking the quotient of each connected component by w_p, thus

$$\mathcal{Y}_d^{(p)} \simeq \bigsqcup_{i=1}^{c_p(d)} \mathcal{Y}_{\Gamma_d}^{(p)} \simeq \bigsqcup_{i=1}^{c_p(d)} \mathcal{M}_{\Gamma_d},$$

where in the last isomorphism we use that the quotient of the twisted Mumford curve $\mathcal{M}^{\xi}_{\Gamma_{d,+}}/\mathbb{Z}_p$ by the involution w_p is precisely the (untwisted) Mumford curve $\mathcal{M}_{\Gamma_d}/\mathbb{Z}_p$ associated with $\Gamma_d \subseteq \mathrm{GL}_2(\mathbb{Q}_p)$. In particular:

Corollary 3.44. *Assume that $f_d = 1$. Then $Y_d^{(p)}(\mathbb{Q}_p) \neq \emptyset$ if and only if $\mathcal{M}_{\Gamma_d}(\mathbb{Q}_p) \neq \emptyset$.*

Similarly as for $\mathcal{M}_{\Gamma_{d,+}}$, now the dual graph of $\mathcal{M}_{\Gamma_d}/\mathbb{Z}_p$ is the finite graph with lengths $\mathcal{G}_d^* := (\Gamma_d \backslash \mathcal{T}_p)^*$, with trivial Frobenius action, and where the superscript $*$ means that one has to remove from $\mathcal{G}_d$ those edges y with $\bar{y} = y$ (see [**Kur79**, Proposition 3.2]). In contrast to the case of $\mathcal{G}_{d,+}$, now such edges may exist as we saw in Lemma 3.28. We thus have the following:

Lemma 3.45. *Assume that $f_d = 1$. The set $Y_d^{(p)}(\mathbb{Q}_p)$ is not empty if and only if the graph $\mathcal{G}_d$ has a vertex of non-trivial length or an edge y with $\bar{y} = y$.*

Proof. "In general", every vertex in the finite graph $\mathcal{G}_d$ has $p+1$ edges in its star, and a smooth rational point on the special fibre of (a regular model of) $\mathcal{M}_{\Gamma_d}/\mathbb{Z}_p$ exists if and only if there is some vertex in $\widetilde{\mathcal{G}}_d^*$ with less than $p+1$ edges emanating from it. But this happens if and only if there is a vertex $v \in \mathrm{Ver}(\mathcal{G}_d)$ such that either v has non-trivial length or there is some edge y in $\mathcal{G}_d$ emanating from v such that $\bar{y} = y$ (such an edge is removed in $\mathcal{G}_d^*$, hence the vertex corresponding to v in $\widetilde{\mathcal{G}}_d^*$ has less than $p+1$ edges in its star). Then the statement follows by applying Hensel's Lemma. □

After our description of $\mathcal{G}_d$, we conclude with the following criterion for the existence of $\mathbb{Q}_p$-rational points on $Y_d^{(p)}$:

Theorem 3.46. *Assume that $f_d = 1$. Then the set $Y_d^{(p)}(\mathbb{Q}_p)$ is not empty if and only if any of the following conditions holds:*

i) *$\mathbb{Q}(\sqrt{-1})$ splits $B_{D/p}$ and $4 \mid t_d$,*
ii) *$\mathbb{Q}(\sqrt{-3})$ splits $B_{D/p}$ and $6 \mid t_d$,*
iii) *Γ_d contains a root of some equation in $\mathcal{F}_{p,d}$.*

Proof. It follows immediately from the previous lemma together with Corollary 3.23 and Lemma 3.28. Indeed, condition i) (resp. ii)) is equivalent to $\mathcal{G}_d$ having an vertex of length 2 (resp. 3), whereas condition iii) is equivalent to $\mathcal{G}_d$ having an edge y such that $\bar{y} = y$. □

By virtue of Corollary 3.31, Theorem 3.2 is now a direct consequence of this theorem.

From [**Ogg85**], we know that $X_D^{(p)}(\mathbb{Q}_p)$ is not empty if and only if either $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-3})$ or $\mathbb{Q}(\sqrt{-p})$ splits $B_{D/p}$. This obviously holds when either of the conditions in the previous result is satisfied, since $Y_d^{(p)}(\mathbb{Q}_p) \neq \emptyset$ implies that $X_D^{(p)}(\mathbb{Q}_p) \neq \emptyset$. Combining Theorem 3.2 with [**Ogg85**, p. 206], we point out the following:

Corollary 3.47. *Assume that $f_d = 1$, and suppose that either $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-3})$ or $\mathbb{Q}(\sqrt{-p})$ splits $B_{D/p}$. Furthermore, in case that either $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-p})$ splits $B_{D/p}$, assume also that $4 \nmid t_d$, whereas if $\mathbb{Q}(\sqrt{-3})$ splits $B_{D/p}$, assume that $6 \nmid t_d$. Then $Y_d^{(p)}(\mathbb{Q}_p) = \emptyset$ and $X_D^{(p)}(\mathbb{Q}_p) \neq \emptyset$.*

Example 3.48. Take $\ell = 5$, and let p be a prime such that $(\frac{-p}{5}) = 1$. Set $D = \ell p = 5p$, and observe that the quadratic fields $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-p})$ do not split $B_5 = B_{D/p}$, whereas $\mathbb{Q}(\sqrt{-3})$ does. Further, choose a positive divisor d of $(\ell^2-1)/2 = 12$ such that $f_d = 1$ and $d \neq 1, 2$ (hence $6 \nmid t_d$). Then the previous corollary applies and we conclude that $Y_d^{(p)}(\mathbb{Q}_p)$ is empty but $X_{5p}^{(p)}(\mathbb{Q}_p)$ is not.

We can illustrate this example by means of the corresponding dual graphs. The class number of B_5 is 1, so that $\mathcal{G}_D$ consists of only one vertex v of length 3. For simplicity, assume that $(\frac{-3}{p}) = -1$, so that $\mathrm{Star}(v)$ consists of $(p+1)/3$ edges y_i of length 1, all of them satisfying $\bar{y}_i \neq y_i$. Under the previous conditions, the graph $\mathcal{G}_d$ consists of $d_{\mathcal{G}}/3$ vertices of length 1 mapping to v. Further, each vertex $v' \in \mathrm{Ver}(\mathcal{G}_d)$ has $p+1$ edges y'_i of trivial length in its star, all of them satisfying again $\bar{y}'_i \neq y'_i$. This clearly implies that the special fibre of $\mathcal{Y}^{(p)}_{\Gamma_d}$ cannot have a smooth $\mathbb{F}_p$-rational point.

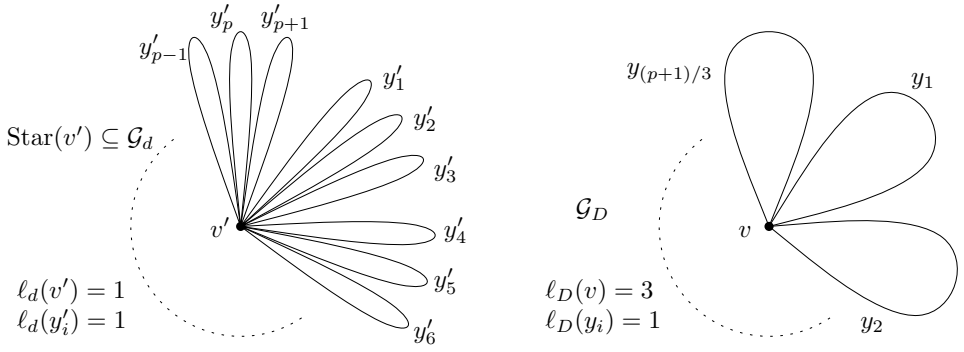

FIGURE 1. The graph $\mathcal{G}_D$ and the star of any vertex $v' \in \mathrm{Ver}(\mathcal{G}_d)$.

For example, take $p = 11$. Since $\mathrm{ord}_{\mathbb{F}_5^\times}(11) = 1$, one has $f_d = 1$ for all d. Furthermore, $(\frac{-11}{5}) = 1$ and $(\frac{-3}{11}) = -1$, hence the above conditions apply if we choose d to be either 3 or 6 (the values for which $6 \nmid t_d$). In each case, Y_d has 1 or 2 geometric connected components, respectively.

4.3. $\mathbb{Q}_p$-rational points on $Y_d^{(m)}$: the case $p \nmid m$. Next we consider the quotient of Y_d by a lifted Atkin-Lehner involution $\hat{\omega}_m$ associated with a positive divisor m of D/p, $m > 1$. We still assume that $f_d = 1$ and $\varepsilon_d(m) = 1$, thus we have a decomposition of $\mathcal{Y}_d^{(m)}$ over $\mathbb{Z}_p$ as in (3.24) and the set $Y_d^{(m)}(\mathbb{Q}_p)$ is not empty if and only if so is the set $\mathcal{Y}^{(m)}_{\Gamma_d}(\mathbb{Q}_p)$. In order to study the set $\mathcal{Y}^{(m)}_{\Gamma_d}(\mathbb{Q}_p)$ by looking at the graph with lengths $\mathcal{G}_{d,+}$, first we describe the action of $\hat{\omega}_m$ on it.

Recall that the involution $\hat{\omega}_m$ acting on Y_d is defined as a modular automorphism, that is, $\hat{\omega}_m = \rho_{U_d}(b)$ for some $b \in (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$ normalising U_d. Further, since we are assuming $p \nmid m$ we can choose b to be of the form $(b^p, 1) \in (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times \times B_{D,p}^\times$. As in Section 2.3, this implies that the involution $\hat{\omega}_m$ corresponds, in the p-adic counterpart of Y_d, to the p-modular automorphism $\lambda_{U_d}((b_v^p)^{-1})$ acting on $\mathcal{Y}_d$. We start by describing this p-modular automorphism.

More precisely, assume first that $m = q$ is a prime dividing D/p. If $q \neq \ell$, then

$$\hat{\omega}_q = \rho_{U_d}(\dots, 1, \dots, \mathrm{w}_q, \dots, 1, \dots, \alpha_q, \dots, 1, \dots),$$

where

$$\mathrm{w}_q = \begin{pmatrix} 0 & 1 \\ q & 0 \end{pmatrix} \in \mathcal{O}_{D,q} \quad \text{and} \quad \alpha_q = \begin{pmatrix} s_q & 0 \\ 0 & \bar{s}_q \end{pmatrix} \in \mathcal{O}_{D,\ell}^\times,$$

with $s_q \in \mathbb{Z}_{\ell^2}$ such that $s_q^2 \equiv q \mod \ell\mathbb{Z}_{\ell^2}$. In contrast, $\hat{\omega}_\ell = \rho_{U_d}(\dots, \mathrm{w}_\ell, \dots)$ (cf. Definition 2.10).

When m is not prime, $\hat{\omega}_m$ is obtained by composing the involutions $\hat{\omega}_q$ for all the primes q dividing m. Since all the involutions $\hat{\omega}_q$ commute one with each other, this is well-defined, and without loss of generality we can write the involution $\hat{\omega}_m$ acting on Y_d as

$$\hat{\omega}_m = \rho_{U_d}(\alpha_m) \cdot \prod_{\substack{q \mid m, \\ q \neq \ell}} \rho_{U_d}(\mathrm{w}_q),$$

where the elements w_q are as above (notice that $\mathrm{w}_q^2 = q$), and where $\alpha_m \in B_{D,\ell}^\times$ is given by

$$\alpha_m = \begin{cases} \prod_{q \mid m} \alpha_q & \text{if } \ell \nmid m, \\ \mathrm{w}_\ell \prod_{q \mid \frac{m}{\ell}} \alpha_q, & \text{if } \ell \mid m. \end{cases}$$

Notice that if $\ell \nmid m$, then $\mathrm{val}_\ell(\mathrm{n}(\alpha_m)) = 0$, whereas if $\ell \mid m$, then $\mathrm{val}_\ell(\mathrm{n}(\alpha_m)) = \mathrm{val}_\ell(\mathrm{n}(\mathrm{w}_\ell)) = 1$.

Since $p \nmid m$, the action of $\hat{\omega}_m$ on the p-adic counterpart of the adèlic description of Y_d, is then given by the p-modular automorphism

$$\lambda_{U_d}(\alpha_m^{-1}) \cdot \prod_{\substack{q|m,\\ q\neq\ell}} \lambda_{U_d}(\mathrm{w}_q^{-1}).$$

Here we write $\mathrm{w}_q^{-1} \in B_{D/p,q}^\times$ and $\alpha_m^{-1} \in B_{D/p,\ell}^\times$ for the images of w_q and α_m, respectively, according to our fixed anti-isomorphism between $(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$ and $(B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$. Thus the action of $\hat{\omega}_m$ on

$$\mathrm{GL}_2(\mathbb{Q}_p) \setminus [\widehat{\mathcal{H}}_p \widehat{\otimes} \widehat{\mathbb{Z}}_p^{\mathrm{ur}} \times Z_{U_d}]$$

is given by the rule

$$[x, z, [(a_v)]] \longmapsto [x, z, [(\dots, a_v, \dots, \mathrm{w}_q^{-1} a_q, \dots, \alpha_m^{-1} a_\ell, \dots)]]. \tag{3.25}$$

This gives therefore the action of $\hat{\omega}_m$ on $\mathcal{Y}_d$. In order to describe the action of $\hat{\omega}_m$ induced on each copy of $\mathcal{Y}_{\Gamma_d}$, we may identify $\mathcal{Y}_{\Gamma_d}$ with the p-class corresponding to the trivial element in $\mathcal{C}_p(d)$. Then, the action of $\hat{\omega}_m$ on $\mathcal{Y}_{\Gamma_d}$ is described just by restricting (3.25) to double cosets of the form

$$[x, z, [(1, 1, \dots, 1, \dots)]],$$

on which we have

$$[x, z, [(1, 1, \dots, 1, \dots)]] \longmapsto [x, z, [(1, 1, \dots, \mathrm{w}_q^{-1}, \dots, \alpha_m^{-1}, \dots, 1, \dots)]],$$

where α_m^{-1} is in the ℓ-th position. Since $\hat{\omega}_m$ acts trivially on the set $\mathcal{C}_p(d)$ of p-classes, there exist elements $g \in \mathrm{GL}_2(\mathbb{Q}_p)$, $b \in B_{D/p}^\times$ and $u = (u_v)_{v\neq p} \in U_d^p$ such that

$$[gu(1, 1, \dots, \mathrm{w}_q^{-1}, \dots, \alpha_m^{-1}, \dots, 1, \dots)b] = [(1, 1, \dots, 1, \dots)].$$

From this, we deduce the following:

i) $gb = 1$ (at the p-th place), so that $g = b^{-1} \in B_{D/p}^\times$ is in fact global;
ii) $u_v b = 1$ at the places v such that $v \neq p, \ell$, $v \nmid m$, hence $g = b^{-1} \in U_{d,v} = \mathcal{O}_{D/p,v}^\times$ for all such places;
iii) $u_q \mathrm{w}_q^{-1} b = 1$ for all primes $q \mid m$, $q \neq \ell$, thus in particular $\mathrm{val}_q(\mathrm{n}(g)) = -\mathrm{val}_q(\mathrm{n}(b)) = -1$ for all these primes;
iv) $u_\ell \alpha_m^{-1} b = 1$, so that $\mathrm{val}_\ell(\mathrm{n}(g)) = -\mathrm{val}_\ell(\mathrm{n}(b)) = -\mathrm{val}_\ell(\mathrm{n}(\alpha_m))$, hence $\mathrm{val}_\ell(\mathrm{n}(g))$ is either -1 or 0, according to whether $\ell \mid m$ or not, respectively.

Hence, the lifted Atkin-Lehner involution $\hat{\omega}_m$ acts on $\mathcal{Y}_{\Gamma_d}$ via the action of $g \in B_{D/p}^\times \subseteq B_{D/p,p}^\times \simeq \mathrm{GL}_2(\mathbb{Q}_p)$ through $\mathcal{H}_p$, using that $\mathcal{Y}_{\Gamma_d}$ is the algebraisation of the Mumford quotient

$$W \setminus ((\Gamma_d \setminus \widehat{\mathcal{H}}_p) \widehat{\otimes} \widehat{\mathbb{Z}}_{p^2}).$$

Since $\mathbb{Q}^\times \hookrightarrow \mathbb{Q}_p^\times = Z(\mathrm{GL}_2(\mathbb{Q}_p))$ acts trivially on this quotient, we see that $\hat{\omega}_m$ acts on $\mathcal{Y}_{\Gamma_d}$ via the action of $w_m := mg$ through $\mathcal{H}_p$ as well. From i)-iv) above, we notice that $w_m \in \mathcal{O}_{D/p}^{(p)}$ normalises Γ_d (so that $w_m \in \Gamma_d^*$), $\mathrm{n}(w_m) = m$ and $w_m^2 \in m\Gamma_d \subseteq \mathbb{Q}^\times \Gamma_d$. Further, locally at ℓ we have $w_m \in m\alpha_m^{-1} U_{d,\ell}$. Regarding this local condition, observe the following:

LEMMA 3.49. *Locally at ℓ, $w_m \in \alpha_m U_{d,\ell}$, thus in particular $w_m^2 = mu$ for some $u \in \mathcal{O}_{D/p}^{(p)\times} \cap U_{d,\ell}$.*

PROOF. Since we know that $w_m \in m\alpha_m^{-1} U_{d,\ell}$, it is enough to prove that $m \in \alpha_m^2 U_{d,\ell}$. We distinguish the cases $\ell \nmid m$ and $\ell \mid m$. In the first case, we can write

$$\alpha_m = \begin{pmatrix} s & 0 \\ 0 & \bar{s} \end{pmatrix} \in \mathcal{O}_{D/p,\ell}, \quad s \in \mathbb{Z}_{\ell^2}, s^2 \equiv m \mod \ell\mathbb{Z}_{\ell^2}.$$

Therefore,

$$\alpha_m^2 = \begin{pmatrix} m+\ell c & 0 \\ 0 & m+\ell\bar{c} \end{pmatrix}$$

for some $c \in \mathbb{Z}_{\ell^2}$. Multiplying (on the right) by

$$u = \begin{pmatrix} 1+\ell x & 0 \\ 0 & 1+\ell\bar{x} \end{pmatrix} \in 1+I_\ell, \quad x = -c(m+\ell c)^{-1} \in \mathbb{Z}_{\ell^2},$$

we find $\alpha_m^2 u = m$, and since $U_{d,\ell} \supseteq 1+I_\ell$, the claim follows.

If $\ell \mid m$, then α_m is defined slightly different, namely

$$\alpha_m = \begin{pmatrix} 0 & 1 \\ \ell & 0 \end{pmatrix} \begin{pmatrix} s & 0 \\ 0 & \bar{s} \end{pmatrix} \in \mathcal{O}_{D/p,\ell}, \quad s \in \mathbb{Z}_{\ell^2}, s^2 \equiv \frac{m}{\ell} \mod \ell\mathbb{Z}_{\ell^2}.$$

Now, one checks that

$$\alpha_m^2 = \pm\ell \begin{pmatrix} \frac{m}{\ell}+\ell c & 0 \\ 0 & \frac{m}{\ell}+\ell\bar{c} \end{pmatrix}$$

for some $c \in \mathbb{Z}_{\ell^2}$. Proceeding as before, and noting that we always have $-1 \in U_{d,\ell}$ by our choice of the subgroup U_d, it holds again that $\alpha_m^2 u = m$ for some $u \in U_{d,\ell}$, and the claim also follows in this case.

Finally, the last assertion in the statement is now easily obtained by using that α_m normalises $U_{d,\ell}$, its square is $\pm m$ and $-1 \in U_{d,\ell}$. □

Altogether, we have proved the following:

PROPOSITION 3.50. *The lifted Atkin-Lehner involution $\hat{\omega}_m$ acts on $\mathcal{Y}_{\Gamma_d}$ as the automorphism induced by the action of an element $w_m \in \mathcal{O}_{D/p}^{(p)} \cap \Gamma_d^*$ on $\mathcal{H}_p$ as above. Further, w_m has reduced norm m, $w_m^2 \in m\Gamma_d$ and, locally at ℓ, $w_m \in \alpha_m U_{d,\ell}$ and $w_m^2 = mu$ for some $u \in \mathcal{O}_{D/p}^{(p)\times} \cap U_{d,\ell}$.*

Observe that the action of $w_m \in \Gamma_d^*$ on $\mathcal{Y}_{\Gamma_d}$ depends only on the image of w_m in $\Gamma_d^*/\mathbb{Q}^\times\Gamma_d$. It is important to remark, however, that we can choose w_m satisfying the properties stated in the above proposition. On the other hand, the above proposition also describes the action of $\hat{\omega}_m$ on the dual graph of the special fibre of $\mathcal{Y}_{\Gamma_d}$. Namely, it is naturally given by the action induced by w_m on $\mathcal{T}_p$.

Later we will make use of the following observation concerning the element w_m:

LEMMA 3.51. *Let $\alpha \in \mathcal{O}_{D/p}^{(p)}$ be an element of reduced norm m normalising $\mathcal{O}_{D/p}^{(p)\times}$. Then $\alpha \in w_m\Gamma_d$ if and only if locally at ℓ it holds that $\alpha \in \alpha_m U_{d,\ell}$.*

PROOF. Indeed, it is plain that the condition is local at ℓ, as U_d is maximal outside ℓ. And at the prime ℓ, using that $w_m \in \alpha_m U_{d,\ell}$ we deduce that $\alpha \in w_m U_{d,\ell}$ if and only if $\alpha \in \alpha_m U_{d,\ell}$. □

Once the action of $\hat{\omega}_m$ on $\mathcal{Y}_{\Gamma_d}$ (resp. on $\mathcal{G}_{d,+}$) is described through the action of $w_m \in \Gamma_d^*$ on $\mathcal{H}_p$ (resp. on $\mathcal{T}_p$), we are in position to study the existence of smooth $\mathbb{F}_p$-rational points on the special fibre of a regular model of $\mathcal{Y}_{\Gamma_d}^{(m)}$ by looking at the dual graph of $\mathcal{Y}_{\Gamma_d}/\mathbb{Z}_p$.

Let us consider the finite graph with lengths

$$\mathcal{G}_{d,+}^{(m)} := \langle w_m \rangle \setminus \mathcal{G}_{d,+} = \langle \Gamma_{d,+}, w_m \rangle \setminus \mathcal{T}_p.$$

Under our assumption that $p \nmid m$, this turns to be the dual graph of $\mathcal{Y}_{\Gamma_d}^{(m)}$:

LEMMA 3.52. *There is no edge y in $\mathcal{G}_{d,+}^{(m)}$ such that $\bar{y} = y$. As a consequence, the finite graph $\mathcal{G}_{d,+}^{(m)}$ is the dual graph of $\mathcal{Y}_{\Gamma_d}^{(m)}$, with Frobenius action given by w_p.*

PROOF. This follows by a similar argument to the one we used when studying the graph $\mathcal{G}_{d,+}$ from $\mathcal{G}_d$. Indeed, consider again the partition $\mathrm{Ver}(\mathcal{T}_p) = V_1 \sqcup V_2$ as before. Since $\mathcal{G}_{d,+}$ does not have edges y such that $\bar{y} = y$, such an edge exists in $\mathcal{G}_{d,+}^{(m)}$ if and only if there exists an edge y in $\mathcal{G}_{d,+}$ with $w_m(y) = \bar{y}$. But since $\mathrm{n}(w_m) = m$ and $p \nmid m$, it follows that $w_m(V_i) = V_i$ for $i = 1, 2$, thus there cannot be such an edge. □

Further, we emphasise the following:

LEMMA 3.53. *There is no vertex in $\mathcal{G}_{d,+}^{(m)}$ fixed by w_p.*

PROOF. Assume that there is a vertex v in $\mathcal{G}_{d,+}^{(m)}$ such that $w_p(v) = v$. Since w_p fixes no vertex in $\mathcal{G}_{d,+}$, a preimage v' of v in $\mathcal{G}_{d,+}$ satisfies $w_p(v') = w_m(v')$. But therefore v' is fixed by $w_m^{-1}w_p$, and this is not possible because $w_m^{-1}w_p$ switches the sets of vertices V_1 and V_2. □

In other words, the special fibre of $\mathcal{Y}_{\Gamma_d}^{(m)}$ has no component rational over $\mathbb{F}_p$. If $\mathcal{Y}_{\Gamma_d}^{(m)}$ is already regular, which is equivalent to saying that every edge of $\mathcal{G}_{d,+}^{(m)}$ has length 1, then Hensel's Lemma implies that $\mathcal{Y}_{\Gamma_d}^{(m)}(\mathbb{Q}_p)$ is empty, hence so is $Y_d^{(m)}(\mathbb{Q}_p)$. In general:

PROPOSITION 3.54. *Assume that $f_d = 1$ and $\varepsilon_d(m) = 1$ as before. If $Y_d(\mathbb{Q}_p) = \emptyset$ and $p \nmid m$, then the set $Y_d^{(m)}(\mathbb{Q}_p)$ is not empty if and only if either*

i) *there exists an edge y in $\mathcal{G}_{d,+}$ of odd length such that $w_m(y) = y$ and $w_p(y) = \bar{y}$, or*
ii) *there exists an edge y in $\mathcal{G}_{d,+}$ of even length such that $w_p w_m(y) = \bar{y}$.*

PROOF. By the above observations, the special fibre of a regular model of $\mathcal{Y}_{\Gamma_d}^{(m)}$ has a smooth $\mathbb{F}_p$-rational point if and only if the graph $\widetilde{\mathcal{G}}_{d,+}^{(m)}$ has a vertex fixed by w_p which is the origin of less than $p+1$ edges. But in view of the previous lemma, this happens if and only if such a vertex has appeared during the resolution of singularities, that is to say, if and only if there exists an edge y_m of even length in $\mathcal{G}_{d,+}^{(m)}$ such that $w_p(y_m) = \bar{y}_m$. By Hensel's Lemma, this is therefore equivalent to the set $\mathcal{Y}_{\Gamma_d}^{(m)}(\mathbb{Q}_p)$ being non-empty, and therefore to the non-emptiness of $Y_d^{(m)}(\mathbb{Q}_p)$ as well.

If the morphism $\mathcal{G}_{d,+} \to \mathcal{G}_{d,+}^{(m)}$ is ramified at y_m, the previous condition is equivalent to saying that there exists an edge y in $\mathcal{G}_{d,+}$ satisfying $w_m(y) = y$ and $w_p(y) = \bar{y}$. Observe that this edge is necessarily of odd length because we are assuming that $Y_d(\mathbb{Q}_p)$ is empty, thus i) is satisfied.

In contrast, if the morphism $\mathcal{G}_{d,+} \to \mathcal{G}_{d,+}^{(m)}$ is not ramified at y_m, the above condition holds if and only if there is an edge y in $\mathcal{G}_{d,+}$ of even length such that either $w_p(y) = \bar{y}$ or $w_p w_m(y) = \bar{y}$. The first case is excluded because we are assuming that $Y_d(\mathbb{Q}_p)$ is empty, and therefore condition ii) holds. □

Now we translate the conditions of this proposition into explicit arithmetic conditions. For the first one, we need a couple of lemmas whose essence is the same as that of Lemmas 3.29 and 3.30.

LEMMA 3.55. *Let $\alpha \in \mathcal{O}_{D/p}^{(p)}$ be a solution of $x^2 + m = 0$. If $\ell \mid m$, then $\alpha \in w_m\Gamma_d$, whereas if $\ell \nmid m$, then $\alpha \in w_m\Gamma_d$ if and only if $4 \mid t_d$.*

PROOF. By Lemma 3.51, we know that $\alpha \in w_m\Gamma_d$ if and only if, locally at ℓ, it holds that $\alpha \in \alpha_m U_{d,\ell}$.

Assume first that $\ell \mid m$. Then $\alpha_m = \mathrm{w}_\ell \alpha'_m$, where $\alpha'_m \in \mathcal{O}_{D/p,\ell}^\times$ and $\tau' := \psi(\alpha'_m) \in \mathbb{F}_{\ell^2}^\times$ is a square root of m/ℓ in $\mathbb{F}_{\ell^2}^\times$. In this case, $\alpha \in \alpha_m U_{d,\ell}$ is equivalent to $\mathrm{w}_\ell^{-1}\alpha \in \alpha'_m U_{d,\ell}$, and by applying ψ this is in turn equivalent to $\psi(\mathrm{w}_\ell^{-1}\alpha) \in \tau' H_d$. But now observe that $\mathrm{w}_\ell^{-1}\alpha$ is a square root of m/ℓ in $\mathcal{O}_{D/p,\ell}^\times$, hence its image by ψ is either τ' or $-\tau'$. Since $-1 \in H_d$, we deduce that $\psi(\mathrm{w}_\ell^{-1}\alpha) \in \tau' H_d$, hence the assertion follows.

Now suppose that $\ell \nmid m$. In this case, $\alpha_m \in \mathcal{O}_{D/p,\ell}^\times$ and $\tau := \psi(\alpha_m) \in \mathbb{F}_{\ell^2}^\times$ is a square root of m in $\mathbb{F}_{\ell^2}^\times$. Besides, we also have $\alpha \in \mathcal{O}_{D/p,\ell}^\times$, but $\psi(\alpha) \in \mathbb{F}_{\ell^2}^\times$ is a square root of $-m$ in $\mathbb{F}_{\ell^2}^\times$ instead. Again, $\alpha \in \alpha_m U_{d,\ell}$ is now equivalent to $\psi(\alpha) \in \tau H_d$, hence we conclude that $\alpha \in \alpha_m U_{d,\ell}$ if and only if -1 is a square in H_d, which is equivalent to saying that $4 \mid t_d$. □

The next lemma deals with the existence of roots in $w_m\Gamma_d$ of the quadratic polynomials $F_m^\pm(x) := x^2 \pm mx + m$, when m is either 2 or 3.

LEMMA 3.56. *Assume that m is either 2 or 3, and suppose that $\mathcal{O}_{D/p}^{(p)}$ has a root of either $F_m^+(x)$ or $F_m^-(x)$. Then $w_m\Gamma_d$ has a root of either $F_m^+(x)$ or $F_m^-(x)$ if and only if $s_m H_d$ contains a root of $F_m^+(x)$ (or, equivalently, of $F_m^-(x)$), where $s_m \in \mathbb{F}_{\ell^2}^\times$ is a square root of m.*

PROOF. First notice that since $\ell > 3$ every root of either $F_m^+(x)$ or $F_m^-(x)$ in $\mathcal{O}_{D/p}^{(p)}$ can be regarded locally at ℓ as an element in $\mathcal{O}_{D/p,\ell}^\times$, thus it can be mapped by ψ to $\mathbb{F}_{\ell^2}^\times$. Then one proves, as in Lemma 3.30, that assuming the existence of a root in $\mathcal{O}_{D/p}^{(p)}$ of either $F_m^+(x)$ or $F_m^-(x)$ is actually equivalent to assuming that $\mathcal{O}_{D/p}^{(p)}$ contains roots of $F_m^+(x)$ and $F_m^-(x)$ mapping under ψ to each of the four roots in $\mathbb{F}_{\ell^2}^\times$ of $F_m^+(x)F_m^-(x)$. Finally, using that $\psi(\alpha_m) \in \mathbb{F}_{\ell^2}^\times$ is a square root of m in $\mathbb{F}_{\ell^2}^\times$ and $-1 \in H_d$, so that $\psi(\alpha_m)H_d = s_m H_d$, one checks that one of such roots belongs to $w_m\Gamma_d$ if and only if its image under ψ lies in $s_m H_d$. □

We are now in position to translate condition i) in Proposition 3.54 by using the previous lemmas:

LEMMA 3.57. *Assume that $f_d = 1$, $\varepsilon_d(m) = 1$ and $p \nmid m$, and let $s_3 \in \mathbb{F}_{\ell^2}^\times$ be a square root of 3 in $\mathbb{F}_{\ell^2}^\times$. Then condition i) in Proposition 3.54 holds if and only if $B_{D/p} \simeq (-m,-p)_{\mathbb{Q}}$ and the following two conditions are satisfied:*

a) *either $4 \mid t_d$ or $p = 3$, $6 \mid t_d$ and H_d has a root of $x^2 + 3x + 3 = 0$;*
b) *either $\ell \mid m$, or $4 \mid t_d$, or $m = 3$, $6 \mid t_d$ and $s_3 H_d$ has a root of $x^2 + 3x + 3 = 0$.*

PROOF. Assume the hypotheses, and suppose first that condition i) in Proposition 3.54 holds, so that there is an edge $y \in \mathrm{Ed}(\mathcal{G}_{d,+})$ such that $\ell_d(y)$ is odd (hence 1 or 3), $w_m(y) = y$ and $w_p(y) = \bar{y}$. Let $\tilde{y} \in \mathrm{Ed}(\mathcal{T}_p)$ be any edge above y, and set $\tilde{v} := o(\tilde{y})$.

As in the proof of Lemma 3.28, on the one hand there is an element $\beta_o \in \Gamma_d \cap \mathcal{O}_{\tilde{v}}$ with $\beta_o(\tilde{y}) = \bar{\tilde{y}}$ such that $\beta_o^2 = pu_\beta$, where $u_\beta \in \Gamma_d \cap \mathcal{O}_{\tilde{v}}^\times$. Since $\ell_d(y)$ is odd, we find out moreover that either $u_\beta = -1$ or $u_\beta^2 - u_\beta + 1 = 0$. The second option implies, moreover, that $6 \mid t_d$. It follows that either $\beta_o^2 + p = 0$ or $p = 3$ and $\beta_o^2 \pm 3\beta_o + 3 = 0$, thus by Lemmas 3.29 and 3.30 condition a) holds. Further, if we are in the second option we can assume in the following that $\beta_o^2 + 3\beta_o + 3 = 0$ (replace β_o by $-\beta_o$, if necessary). On the other hand, there is an element $\gamma \in \Gamma_d$ such that $\gamma w_m(\tilde{y}) = \tilde{y}$. Writing $\alpha_o := \gamma w_m$, we see that $\alpha_o \in \mathcal{O}_{\tilde{v}} \cap w_m\Gamma_d$ satisfies $\alpha_o(\tilde{v}) = \tilde{v}$, hence also $\alpha_o^2(\tilde{v}) = \tilde{v}$. Similarly as in the proof of Lemma 3.28, we have $\alpha_o^2 = mu_\alpha$ for some $u_\alpha \in \Gamma_d \cap \mathcal{O}_{\tilde{v}}^\times$, and again using that $\ell_d(y) = 1$ or 3, we have in fact that either $u_\alpha = -1$ or $u_\alpha^2 - u_\alpha + 1 = 0$. The first case implies that $\alpha_o^2 + m = 0$, whereas in the second case it follows that $m = 3$, $6 \mid t_d$ and $\alpha_o^2 \pm 3\alpha_o + 3 = 0$, hence condition b) holds as well by virtue of Lemmas 3.55 and 3.56. Again, we assume henceforth that $\alpha_o^2 + 3\alpha_o + 3 = 0$ if we are in the second case.

Now it remains to prove that $B_{D/p} \simeq (-m,-p)_{\mathbb{Q}}$. Suppose first that $u_\beta = u_\alpha = -1$, and take $\alpha := \alpha_o$, $\beta := \beta_o$. Then $\alpha^2 = -m$ and $\beta^2 = -p$, thus the claim will follow if we prove that $\alpha\beta = -\beta\alpha$. Indeed, let $\gamma := \alpha^{-1}\beta\alpha \in \Gamma_d$. Then $\gamma^2 = -p$, so that $\mathbb{Q}(\gamma) = \mathbb{Q}(\beta) \simeq \mathbb{Q}(\sqrt{-p})$, and it follows that either $\gamma = \beta$ or $\gamma = -\beta$. The first option is excluded, since $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ are two distinct quadratic subfields of $B_{D/p}$, hence $\gamma = -\beta$ and consequently our claim is proved.

Suppose now that $u_\beta = -1$, but $u_\alpha^2 - u_\alpha + 1 = 0$, thus in particular $m = 3$. Set $\beta := \beta_o$ and $\alpha := 2\alpha_o + 3$; we have $\beta^2 = -p$ and $\alpha^2 = -m = -3$. Defining as before $\gamma := \alpha^{-1}\beta\alpha$, we see that $\mathbb{Q}(\gamma) = \mathbb{Q}(\beta) \simeq \mathbb{Q}(\sqrt{-p})$, and again it follows that $\alpha\beta = -\beta\alpha$, hence $B_{D/p} \simeq (-m,-p)_{\mathbb{Q}}$. By symmetry, the case where $u_\alpha = -1$ and $u_\beta^2 - u_\beta + 1 = 0$ (thus $p = 3$) is done in the same way. And finally, notice that $u_\alpha \neq -1$ and $u_\beta \neq -1$ cannot occur simultaneously, since this would imply $p = m = 3$.

Conversely, suppose that $B_{D/p} \simeq (-m,-p)_{\mathbb{Q}}$ and both a) and b) hold. We have to prove that there is an edge $y \in \mathrm{Ed}(\mathcal{G}_{d,+})$ of odd length such that $w_m(y) = y$ and $w_p(y) = \bar{y}$. Indeed, let $\alpha, \beta \in B_{D/p}$ be such that $\alpha^2 = -m$, $\beta^2 = -p$ and $\alpha\beta = -\beta\alpha$, and choose a maximal order $\mathcal{O}_{\tilde{v}}$ containing α and β, for some vertex $\tilde{v} \in \mathrm{Ver}(\mathcal{T}_p)$. First we use condition a). By Corollary 3.31, Γ_d contains a root β_o of some equation in $\mathcal{F}_{p,d}$. Indeed, if $4 \mid t_d$, then it follows from Lemma 3.29 that $\beta \in \Gamma_d$: in this case, let us just write $\beta_o := \beta$. Otherwise, $p = 3$ and H_d contains a root of $x^2 + 3x + 3 = 0$. As in Lemma 3.30, the elements $(\beta - 3)/2, (-\beta - 3)/2 \in \mathcal{O}_{D/3}^{(3)\times}$ are roots of $x^2 + 3x + 3 = 0$, mapping to the two roots of $x^2 + 3x + 3 = 0$ in $\mathbb{F}_{\ell^2}^\times$. Since one of them is in H_d either $(\beta - 3)/2$ or $(-\beta - 3)/2$ lies in Γ_d: set $\beta_o := (\beta - 3)/2$ or $\beta_o := (-\beta - 3)/2$ accordingly. In

any case, $\beta_o \in \Gamma_d$ is a root of an equation in $\mathcal{F}_{p,d}$. Thus if we set $\tilde{v}' := \beta_o(\tilde{v})$ and $\tilde{y}$ denotes the edge from $\tilde{v}$ to $\tilde{v}'$, then $\beta_o(\tilde{y}) = \bar{\tilde{y}}$ by Lemma 3.28 (actually, β_o acts like w_p on $\mathcal{G}_{d,+}$). As a consequence, if y denotes the image of $\tilde{y}$ in $\mathcal{G}_{d,+}$, then $w_p(y) = \bar{y}$. Since $Y_d(\mathbb{Q}_p)$ is empty by hypothesis, the length of y is necessarily odd.

Secondly, we use now condition b). If $\ell \mid m$ or $4 \mid t_d$, then by Lemma 3.55 we have that $\alpha \in w_m\Gamma_d$. In this case, set $\alpha_o := \alpha$. Otherwise, if $m = 3$ and s_3H_d has a root of $x^2 + 3x + 3 = 0$, similarly as before one of the elements $(\alpha-3)/2$, $(-\alpha-3)/2 \in \mathcal{O}^{(p)}_{D/p}$ lies actually in $w_m\Gamma_d$: we write α_o for any of them satisfying this condition, and notice that α_o is a root of $x^2+3x+3 = 0$. In any case, the element α_o induces the same action as w_m on the graph $\mathcal{G}_{d,+}$, because $p \nmid m$. Therefore, it remains to prove that $w_m(y) = y$, which amounts to proving that the edge $\alpha_o(\tilde{y}) \in \mathrm{Ed}(\mathcal{T}_p)$ lies above y. First of all, observe that locally at p we have $\alpha_o \in \mathcal{O}^\times_{\tilde{v},p}$, so that $\alpha_o(\tilde{v}) = \tilde{v}$. Thus it is enough to prove that $\alpha_o(\tilde{v}')$ is a vertex above the end vertex of y, i.e. above the same vertex as $\tilde{v}'$. For doing so, we translate the relation $\alpha\beta = -\beta\alpha$ into a relation between $\alpha_o\beta_o$ and $\beta_o\alpha_o$, depending on the expression of α_o and β_o in terms of α and β, respectively. The details can be done case by case:

1) Suppose that $\alpha_o = \alpha$ and $\beta_o = \beta$. Then we have clearly $\alpha_o\beta_o = -\beta_o\alpha_o$. As a consequence,
$$\alpha_o(\tilde{v}') = \alpha_o\beta_o(\tilde{v}) = -\beta_o\alpha_o(\tilde{v}) = \beta(\tilde{v}) = \tilde{v}',$$
and therefore $\alpha_o(\tilde{y}) = \tilde{y}$, which obviously implies our claim.
2) Now suppose that $m = 3$ and $\alpha_o := (\pm\alpha - 3)/2$. Then α_o satisfies the quadratic equation $\alpha_o^2 + 3\alpha + 3 = 0$. In particular, observe that $\mathrm{tr}(\alpha_o) = -3$ and $\mathrm{n}(\alpha_o) = 3$. Since $p \nmid m$, in this case we necessarily have $\beta_o = \beta$. Then from the relation $\alpha\beta = -\beta\alpha$ it follows that
$$\alpha_o\beta_o = \frac{1}{2}(\pm\alpha - 3)\beta = \frac{1}{2}(\pm\alpha\beta - 3\beta) = \frac{1}{2}(\mp\beta\alpha - 3\beta) = -\beta_o\alpha_o + 3\beta_o = -\beta_o(\alpha_o + 3).$$
But notice that $\mathrm{n}(\alpha_o + 3) = 3$, so that $\alpha_o + 3 \in \mathcal{O}^\times_{\tilde{v},p}$ fixes $\tilde{v}$. Therefore,
$$\alpha_o(\tilde{v}') = \alpha_o\beta_o(\tilde{v}) = -\beta_o(\alpha_o + 3)(\tilde{v}) = \beta_o(\tilde{v}) = \tilde{v}',$$
and again this implies that $\alpha_o(\tilde{y}) = \tilde{y}$ as we wanted.
3) When $p = 3$ and $\beta_o := (\pm\beta - 3)/2 \in \Gamma_d$, one can proceed in the same way as in 2), we leave the details to the reader.

□

Condition ii) in Proposition 3.54 is translated into a very explicit condition in Lemma 3.59 below. In its proof, we use the following lemma, which is proved in the same way as Lemma 3.55 by using that the assumption $f_d = 1$ implies that H_d contains the square roots in $\mathbb{F}^\times_{\ell^2}$ of p mod ℓ.

LEMMA 3.58. *Let $\alpha \in \mathcal{O}^{(p)}_{D/p}$ be a solution of $x^2 + mp = 0$. If $\ell \mid m$, then $\alpha \in w_m\Gamma_d$, whereas if $\ell \nmid m$, then $\alpha \in w_m\Gamma_d$ if and only if $4 \mid t_d$.*

LEMMA 3.59. *Assume $f_d = 1$, $\varepsilon_d(m) = 1$ and $p \nmid m$. Then condition ii) in Proposition 3.54 holds if and only if $4 \mid t_d$ and $B_{D/p} \simeq (-mp, -1)_{\mathbb{Q}}$.*

PROOF. Assume the hypotheses, and suppose that condition ii) in Proposition 3.54 holds, so that there is an edge $y \in \mathrm{Ed}(\mathcal{G}_{d,+})$ of length 2 such that $w_pw_m(y) = \bar{y}$. Choose an edge $\tilde{y} \in \mathrm{Ed}(\mathcal{T}_p)$ above y, and let $\tilde{v} := o(y)$. Since $\ell_d(y) = 2$, there is an element $\beta \in \Gamma_d \cap \mathcal{O}^\times_{\tilde{v}}$ such that $\beta^2 + 1 = 0$. This implies, in particular, that $4 \mid t_d$. On the other hand, since $w_pw_m(y) = \bar{y}$, there is an element $\gamma \in \Gamma_d$ such that $\gamma w_m(\tilde{y}) = \bar{\tilde{y}}$, thus $(\gamma w_m)^2(\tilde{y}) = \tilde{y}$. Write $\alpha := \gamma w_m$, and observe that $\alpha \in \mathcal{O}_{\tilde{v}} \cap w_m\Gamma_d$ normalises Γ_d. Besides, since w_m normalises Γ_d and $w_m^2 \in m\Gamma_d$, we have that $\alpha^2 = m\gamma'$ for some $\gamma' \in \Gamma_d$. Now, since $p \nmid m$ and $\mathrm{dist}(\alpha(\tilde{v}), \tilde{v}) = 1$, we deduce that $\mathrm{val}_p(\mathrm{n}(\gamma'))$ is odd, thus as in the proof of Lemma 3.28 we can assume it is 1. Then we can write $\alpha^2 = pmu$ for some $u \in \mathcal{O}^\times_{\tilde{v}}$, but observe that $\mathcal{O}^\times_{\tilde{v}}/\mathbb{Z}^\times = \{[1], [\beta]\}$. If it were $u = \pm\beta$, we would have $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$, and this is not possible. Therefore, $u = \pm 1$, and since $B_{D/p}$ is definite, the only option is $u = -1$ and this implies that $\alpha^2 = -pm$. Finally, observe that $\alpha^{-1}\beta\alpha$ fixes $\tilde{y}$, hence

in particular $\alpha^{-1}\beta\alpha \in \mathcal{O}_{\tilde{v}}^{\times}$. Since $\beta \neq \pm 1$, it follows that $\alpha^{-1}\beta\alpha = \pm\beta$. But $\alpha^{-1}\beta\alpha = \beta$ is not possible, hence we have $\alpha\beta = -\beta\alpha$, and we conclude that $B_{D/p} \simeq (-1, -pm)_{\mathbb{Q}}$.

Conversely, assume that $4 \mid t_d$ and $B_{D/p} = (-mp, -1)_{\mathbb{Q}}$, and choose elements $\alpha, \beta \in B_{D/p}$ satisfying $\alpha^2 = -pm$, $\beta^2 = -1$ and $\alpha\beta = -\beta\alpha$. We can also choose a maximal order $\mathcal{O}_{\tilde{v}}$ containing α and β for some vertex $\tilde{v} \in \mathrm{Ver}(\mathcal{T}_p)$. Let $\tilde{v}' := \alpha(\tilde{v})$ (which is at distance 1 from $\tilde{v}$), $\tilde{y}$ be the edge from $\tilde{v}$ to $\tilde{v}'$ and v, y be their images in $\mathcal{G}_{d,+}$, respectively. Since $4 \mid t_d$, the element β actually lies in Γ_d (one can argue as in the proof of Lemma 3.21, for example), and we deduce that $\mathrm{Stab}_{\Gamma'_{d,+}}(\tilde{v}) = \{[1], [\beta]\}$, hence $\ell_d(v) = 2$. On the other hand, $\beta(\tilde{v}') = \beta\alpha(\tilde{v}) = -\alpha\beta(\tilde{v}) = \alpha(\tilde{v}) = \tilde{v}'$, thus β fixes $\tilde{y}$ as well, hence $\ell_d(y) = 2$. Finally, $\alpha(\tilde{y}) = \bar{\tilde{y}}$, and from Lemma 3.58 we have $\alpha \in w_m\Gamma_d$ because $4 \mid t_d$. This implies that $w_m(y') = \bar{y}'$, where y' is the image of y in $\mathcal{G}_d$, which means that either $w_m(y) = \bar{y}$ or $w_p w_m(y) = \bar{y}$. But since $p \nmid m$, the first option cannot occur, so that $w_p w_m(y) = \bar{y}$. Therefore, condition ii) in Proposition 3.54 is satisfied. □

As a direct consequence of Proposition 3.54 together with Lemmas 3.57 and 3.59, we conclude with the following criterion for the existence of $\mathbb{Q}_p$-rational points on $Y_d^{(m)}$, which accounts for part 1) of Theorem 3.3. Notice that condition i) is indeed equivalent to the conditions in Lemma 3.57, since $p = 3$ and $m = 3$ cannot hold simultaneously.

THEOREM 3.60. *Assume that $f_d = 1$, $\varepsilon_d(m) = 1$ and $p \nmid m$. If $Y_d(\mathbb{Q}_p) = \emptyset$, then the set $Y_d^{(m)}(\mathbb{Q}_p)$ is not empty if and only if one of the following conditions holds:*

i) *$B_{D/p} \simeq (-m, -p)_{\mathbb{Q}}$, and either*
   a) *$4 \mid t_d$, or*
   b) *$p = 3$, $\ell \mid m$, $6 \mid t_d$ and H_d contains a root of $x^2 + 3x + 3 = 0$.*

ii) *$B_{D/p} \simeq (-mp, -1)_{\mathbb{Q}}$ and $4 \mid t_d$.*

COROLLARY 3.61. *Assume that $f_d = 1$, $\varepsilon_d(m) = 1$, $p \nmid m$ and $Y_d(\mathbb{Q}_p) = \emptyset$. If $4 \nmid t_d$ and $p \neq 3$, then $Y_d^{(m)}(\mathbb{Q}_p) = \emptyset$.*

4.4. $\mathbb{Q}_p$-rational points on $Y_d^{(pm)}$. Lastly, we discuss the existence of $\mathbb{Q}_p$-rational points on the quotients of Y_d by lifted Atkin-Lehner involutions of the form $\hat{\omega}_{pm}$, where $m \mid D/p$ and $m > 1$. As above, we assume that $f_d = 1$ and $\varepsilon_d(pm) = 1$. By Lemma 3.43 observe that our assumption is equivalent to $f_d = 1$ and $\varepsilon_d(m) = 1$. Similarly as before, $\hat{\omega}_{pm}$ induces an action on each copy of $\mathcal{Y}_{\Gamma_d}$ in (3.19), and the set $Y_d^{(pm)}(\mathbb{Q}_p)$ is non-empty if and only if $\mathcal{Y}_{\Gamma_d}^{(pm)}(\mathbb{Q}_p)$ is non-empty.

Now, since $\hat{\omega}_{pm} = \hat{\omega}_p\hat{\omega}_m = \hat{\omega}_m\hat{\omega}_p$, its action on $\mathcal{Y}_{\Gamma_d}$ is induced by the action of $w_p w_m$ (or $w_m w_p$) on $\widehat{\mathcal{H}}_p$. Besides, the action of $\hat{\omega}_{pm}$ on the graph $\mathcal{G}_{d,+} = \Gamma_{d,+} \setminus \mathcal{T}_p$ is naturally induced by the action of $w_p w_m$ on $\mathcal{T}_p$, so we are lead to consider the finite graph with lengths

$$\mathcal{G}_{d,+}^{(pm)} := \langle \Gamma_{d,+}, w_p w_m \rangle \setminus \mathcal{T}_p.$$

In contrast to the case of $\mathcal{G}_{d,+}^{(m)}$ (with $p \nmid m$), where it holds that $\mathcal{G}_{d,+}^{(m)*} = \mathcal{G}_{d,+}^{(m)}$, now it might be the case that $\mathcal{G}_{d,+}^{(pm)*} \neq \mathcal{G}_{d,+}^{(pm)}$, because $\mathcal{G}_{d,+}^{(pm)}$ can have edges y with $\bar{y} = y$. Thus $\mathcal{G}_{d,+}^{(pm)}$ is not necessarily the dual graph of $\mathcal{Y}_{\Gamma_d}^{(pm)}$.

LEMMA 3.62. *Let $m > 1$ be a divisor of D/p, and assume that $f_d = 1$, $Y_d(\mathbb{Q}_p) = \emptyset$ and $\varepsilon_d(m) = 1$. Then $Y_d^{(pm)}(\mathbb{Q}_p)$ is not empty if and only if there exists a vertex v in $\mathcal{G}_{d,+}$ such that $w_m(v) = v$.*

PROOF. Suppose first that $Y_d^{(pm)}(\mathbb{Q}_p)$ is non-empty, hence so is $\mathcal{Y}_{\Gamma_d}^{(pm)}(\mathbb{Q}_p)$. Therefore, there is a vertex $x \in \mathrm{Ver}(\widetilde{\mathcal{G}}_{d,+}^{(pm)})$ such that $w_p(x) = x$. If x was already a vertex of $\mathcal{G}_{d,+}^{(pm)}$, then a preimage v of x in $\mathcal{G}_{d,+}$ would satisfy either $w_p(v) = v$ or $w_p(v) = w_p w_m(v)$. The first option is not possible because w_p fixes no vertex in $\mathcal{G}_{d,+}$, hence $w_p(v) = w_p w_m(v)$, and as a consequence $v = w_m(v)$.

Otherwise, the vertex x has appeared during the resolution of singularities. This implies that $\mathcal{G}_{d,+}^{(pm)}$ has an edge y of even length such that $w_p(y) = \bar{y}$. Now we claim that if y has two distinct

preimages y_1 and $y_2 = w_p w_m(y_1)$ in $\mathcal{G}_{d,+}$, then we have the same situation for both y_1 and y_2. Indeed, the length of both y_1 and y_2 equals the length of y in $\mathcal{G}_{d,+}^{(pm)}$, as the natural projection is not ramified at y, and the identity $w_p(y) = \bar{y}$ implies that for $i = 1, 2$ we have either $w_p(y_i) = \bar{y}_i$ or $w_p(y_i) = \overline{w_p w_m(y_i)} = w_p w_m(\bar{y}_i)$. But since $p \nmid m$, the second option is not possible[2]. Then both y_1 and y_2 are edges of even length in $\mathcal{G}_{d,+}$ such that $w_p(y_1) = \bar{y}_1$ and $w_p(y_2) = \bar{y}_2$ as claimed. But this contradicts our assumption that $Y_d(\mathbb{Q}_p)$ is empty. Therefore we may assume that y has a unique preimage z in $\mathcal{G}_{d,+}$ (i.e., $w_p w_m$ is ramified at y). But this means that $w_p w_m(z) = z$, which again is not possible because $p \nmid m$.

Conversely, assume there is a vertex $v \in \mathcal{G}_{d,+}$ such that $w_m(v) = v$. Then the image x of v in $\mathcal{G}_{d,+}^{(pm)}$ is fixed by w_p. Therefore, $\mathcal{Y}_{\Gamma_d}^{(pm)}(\mathbb{Q}_p)$, hence $Y_d^{(pm)}(\mathbb{Q}_p)$, is non-empty, except possibly if the vertex x is the origin of $p+1$ edges y such that $w_p(y) = \bar{y}$. Let us work out this case.

Assume that x is in fact the origin of $p+1$ edges y such that $w_p(y) = \bar{y}$. First we claim that if this is the case then the vertex v is the origin of $p+1$ edges z such that $w_m(z) = z$. Indeed, write $v' := w_p(v)$, and notice that $v' = w_p w_m(v)$, so that v and v' are the two distinct preimages of x in $\mathcal{G}_{d,+}$. Observe that since x is the origin of $p+1$ edges, then x has trivial length, and as a consequence every edge y emanating from x has trivial length as well. In particular, every edge $y \in \mathrm{Star}(x)$ has two distinct preimages of trivial length in $\mathcal{G}_{d,+}$, one in $\mathrm{Star}(v)$ and the other one in $\mathrm{Star}(v')$. Fix an edge $y \in \mathrm{Star}(x)$, and let z be the unique edge in $\mathrm{Star}(v)$ above y. Since we are assuming $w_p(y) = \bar{y}$, we deduce that either $w_p(z) = \bar{z}$ or $w_p(z) = \overline{w_p w_m(z)} = w_p w_m(\bar{z})$. The latter is not possible because $p \nmid m$, hence it is $w_p(z) = \bar{z}$. Besides, $w_m(z)$ maps to the same edge as $w_p(z) = \bar{z}$. Therefore, either $w_m(z) = \bar{z}$ or $w_m(z) = w_p w_m w_m(\bar{z}) = w_p(\bar{z}) = z$. Again, the first option is excluded because $p \nmid m$, so that $w_m(z) = z$. The same argument applies for every edge $y \in \mathrm{Star}(x)$, thus our claim is proved. Secondly, our claim implies in turn that w_m fixes every vertex of $\mathcal{G}_{d,+}$ at distance 1 of v. Being $\mathcal{G}_{d,+}$ connected, this implies that w_m acts trivially on $\mathcal{G}_{d,+}$. Therefore, if we write g_d (resp. $g_d^{(m)}$) for the genus of $\mathcal{Y}_{\Gamma_d}$ (resp. $\mathcal{Y}_{\Gamma_d}^{(m)}$), then it follows that $g_d = g_d^{(m)}$, and by applying the Riemann-Hurwitz formula, we deduce that $g_d \geq (g_d + 1)/2$, hence g_d is either 0 or 1. But this implies that there is some vertex in $\mathcal{G}_{d,+}$ which has less than $p+1$ edges emanating from it, and therefore its image in $\mathcal{G}_{d,+}^{(pm)}$ is a vertex fixed by w_p and with less than $p+1$ edges in its star, thus by Hensel's Lemma $\mathcal{Y}_{\Gamma_d}^{(pm)}(\mathbb{Q}_p)$ is not empty. Indeed, if every vertex of $\mathcal{G}_{d,+}$ were the origin of $p+1$ edges, then every vertex in $\mathcal{G}_{d,+}$ would have degree $p+1$, and we would have that

$$|\operatorname{Ver}(\mathcal{G}_{d,+})|(p+1) = 2|\operatorname{Ed}(\mathcal{G}_{d,+})|.$$

But on the other hand we know that the genus g_d of $\mathcal{Y}_{\Gamma_d}$ satisfies the relation $1 - g_d = |\operatorname{Ver}(\mathcal{G}_{d,+})| - |\operatorname{Ed}(\mathcal{G}_{d,+})|$. And when g_d is either 0 or 1, this is not compatible with the above relation. □

Next we translate the existence of a vertex in $\mathcal{G}_{d,+}$ fixed by w_m into the existence of solutions in $w_m\Gamma_d$ of certain quadratic equations. We do this in the following lemma, where $\mathcal{F}_{m,d}$ denotes the set of quadratic equations defined in the same way as we defined $\mathcal{F}_{p,d}$ in (3.23) replacing p by m.

LEMMA 3.63. *Let $m > 1$ be a divisor of D/p, and assume that $f_d = 1$ and $\varepsilon_d(m) = 1$. Then there is a vertex $v \in \operatorname{Ver}(\mathcal{G}_{d,+})$ such that $w_m(v) = v$ if and only if there exists an element $\alpha \in w_m\Gamma_d$ satisfying some quadratic equation in $\mathcal{F}_{m,d}$.*

PROOF. Suppose that there is a vertex $v \in \operatorname{Ver}(\mathcal{G}_{d,+})$ fixed by w_m, and let $\tilde{v} \in \operatorname{Ver}(\mathcal{T}_p)$ be a vertex above v. Then there is an element $\gamma \in \Gamma_d$ such that $\gamma w_m(\tilde{v}) = \tilde{v}$. Writing $\alpha = \gamma w_m \in \Gamma_d w_m = w_m \Gamma_d$, we have $\alpha(\tilde{v}) = \tilde{v}$. In particular, $\alpha^2(\tilde{v}) = \tilde{v}$ as well, but notice that

[2]The graph $\mathcal{G}_{d,+}$ is bipartite: its set of vertices admits a decomposition as a disjoint union of two sets of vertices V_d^1, V_d^2, of the same cardinality, and there is no edge between vertices in the same set V_d^i. Further, $w_p(V_d^1) = V_d^2$ and $w_p(V_d^2) = V_d^1$, whereas $w_m(V_d^i) = V_d^i$ for $i = 1, 2$, because $p \nmid m$. Then for every edge $y \in \operatorname{Ed}(\mathcal{G}_{d,+})$, if $o(y) \in V_d^1$ then $o(w_p(y)) \in V_d^2$ and $o(w_p w_m(\bar{y})) \in V_d^1$, so that $w_p(y)$ and $w_p w_m(\bar{y})$ cannot be the same edge (and analogously if $o(y) \in V_d^2$).

$\alpha^2 = \gamma w_m \gamma w_m = w_m^2 \gamma' = mu$ for some elements $\gamma', u \in \Gamma_d$, where we have used that $w_m^2 \in m\Gamma_d$. But therefore u fixes $\tilde{v}$ as well, because m acts trivially on $\mathcal{T}_p$. Then $u \in \mathrm{Stab}_{\Gamma_d}(\tilde{v}) = \mathcal{O}_{\tilde{v}}^\times$, and it thus follows that either $u = \pm 1$, $u^2 + 1 = 0$ or $u^2 \pm u + 1 = 0$. As in the proof of Lemma 3.28, we deduce that one of the following holds:

i) $u = -1$ and $\alpha^2 + m = 0$,
ii) $u^2 + 1 = 0$, $m = 2$, $4 \mid t_d$ and $\alpha^2 \pm 2\alpha + 2 = 0$,
iii) $u^2 - u + 1 = 0$, $m = 3$, $6 \mid t_d$ and $\alpha^2 \pm 3\alpha + 3 = 0$.

And this implies that α is a root of some equation in $\mathcal{F}_{m,d}$.

Conversely, assume that there exists a root α of some equation in $\mathcal{F}_{m,d}$ such that $\alpha \in w_m\Gamma_d$. Since $w_m\Gamma_d \subseteq \mathcal{O}_{D/p}$, we can choose a maximal order $\mathcal{O}_{\tilde{v}}$ corresponding to some vertex $\tilde{v}$ of $\mathcal{T}_p$ such that $\alpha \in \mathcal{O}_{\tilde{v}}$. But now notice that $\mathrm{n}(\alpha) = m$, and since $p \nmid m$ this implies that α is invertible in $\mathcal{O}_{\tilde{v}}$, thus it fixes $\tilde{v}$. In particular, writing $\alpha = \gamma w_m$ for some $\gamma \in \Gamma_d$ (recall that $w_m\Gamma_d = \Gamma_d w_m$), it follows that $\gamma w_m(\tilde{v}) = \tilde{v}$. If v denotes the image of $\tilde{v}$ in $\mathcal{G}_{d,+}$, then v is fixed by w_m. □

Finally, we conclude with the following criterion for the existence of $\mathbb{Q}_p$-rational points on $Y_d^{(pm)}$, which corresponds to part 2) of Theorem 3.3. It is a direct consequence of the previous lemmas: indeed, one only has to translate the existence of solutions in $w_m\Gamma_d$ of equations in the set $\mathcal{F}_{m,d}$ into explicit conditions by using Lemmas 3.55 and 3.56:

THEOREM 3.64. *Let $m > 1$ be a divisor of D/p, and assume that $f_d = 1$, $Y_d(\mathbb{Q}_p) = \emptyset$ and $\varepsilon_d(m) = 1$. Then $Y_d^{(pm)}(\mathbb{Q}_p)$ is not empty if and only if one of the following conditions holds:*

i) *$\mathbb{Q}(\sqrt{-m})$ splits $B_{D/p}$, and either*
   a) *$\ell \mid m$ or $4 \mid t_d$, or*
   b) *$m = 3$, $6 \mid t_d$ and $s_3 H_d$ contains a root of $x^2 + 3x + 3 = 0$, where $s_3 \in \mathbb{F}_{\ell^2}^\times$ is a square root of 3.*
ii) *$m = 2$, $4 \mid t_d$, $\mathbb{Q}(\sqrt{-1})$ splits $B_{D/p}$ and $s_2 H_d$ contains a root of $x^2 + 2x + 2 = 0$, where s_2 is a square root of 2 in $\mathbb{F}_{\ell^2}^\times$.*

CHAPTER 4

Galois representations over fields of moduli

The purpose of this chapter is to introduce a method for proving the non-existence of rational points on a coarse moduli space X of abelian varieties over a given number field K, in cases where the moduli problem is not fine and points in $X(K)$ may not be represented by abelian varieties (with additional structure) admitting models rational over the field K. This is typically the case when the abelian varieties that are being classified have even dimension (see [**Shi72**]).

The main idea, inspired by the work of Ellenberg and Skinner on the modularity of $\mathbb{Q}$-curves, is that one may still attach a Galois representation of $G_K := \mathrm{Gal}\,(\bar{K}/K)$ with values in the quotient group $\mathrm{GL}(T_p(A))/\mathrm{Aut}(A)$ to a point $P = [A] \in X(K)$ represented by an abelian variety $A/\bar{K}$, provided $\mathrm{Aut}(A)$ lies in the centre of $\mathrm{GL}(T_p(A))$. By exploiting this idea, we define what we call *Galois representations over fields of moduli*. These representations are introduced in some generality in the first two sections of the chapter, and next we exemplify in detail their construction in the cases where X is a Shimura curve over an imaginary quadratic field or an Atkin-Lehner quotient over $\mathbb{Q}$ in Sections 3 and 4, respectively. The representations obtained in this way, attached to points on Shimura curves rather than to single abelian surfaces, will be one of the key ingredients in the proof of the main results of Chapter 5.

The original idea of Ellenberg and Skinner arose while proving the modularity of $\mathbb{Q}$-curves (see [**ES01**]). Given a number field K, a $\mathbb{Q}$-curve over K is an elliptic curve E/K (without complex multiplication) such that there exists a K-isogeny $\mu_\sigma : {}^\sigma E \to E$ for every $\sigma \in G_\mathbb{Q}$. Using these isogenies, Ellenberg and Skinner showed that for any prime p the usual Galois representation

$$\phi_{E,p} : G_K \longrightarrow \mathrm{Aut}(T_p(E)) \simeq \mathrm{GL}_2(\mathbb{Z}_p)$$

can be extended to a representation

$$\rho_{E,p} : G_\mathbb{Q} \longrightarrow \bar{\mathbb{Q}}_p^\times \mathrm{GL}_2(\mathbb{Q}_p)$$

such that $\mathbb{P}\rho_{E,p|G_K} \simeq \mathbb{P}\phi_{E,p}$. To do this, they considered the cohomology class $[c_E] \in \mathrm{H}^2(G_\mathbb{Q}, \bar{\mathbb{Q}}^\times)$ of the 2-cocycle on $G_\mathbb{Q}$ with values on the trivial $G_\mathbb{Q}$-module $\bar{\mathbb{Q}}^\times$ given by

$$c_E(\sigma,\tau) = \mu_\sigma \cdot {}^\sigma\mu_\tau \cdot \mu_{\sigma\tau}^{-1} \in (\mathrm{Hom}(E,E) \otimes \mathbb{Q})^\times = \mathbb{Q}^\times.$$

According to a theorem of Tate (see [**Rib92**, Theorem 6.3]), the cohomology class $[c_E]$ is trivial and hence there exists a continuous map

$$\alpha : G_\mathbb{Q} \longrightarrow \bar{\mathbb{Q}}^\times$$

such that $c_E(\sigma,\tau) = \alpha(\sigma)\alpha(\tau)\alpha(\sigma\tau)^{-1}$ for all $\sigma,\tau \in G_\mathbb{Q}$. Then the rule

$$\rho_{E,p}(\sigma)(1 \otimes x) = \alpha(\sigma)^{-1} \otimes \mu_\sigma({}^\sigma x)$$

gives rise to an action of $G_\mathbb{Q}$ on $\bar{\mathbb{Q}}_p^\times \otimes T_p(E)$ which extends the one of G_K given by $\phi_{E,p}$. Note that if E is already defined over $\mathbb{Q}$, we can choose $\mu_\sigma = \mathrm{id}$ for all $\sigma \in G_\mathbb{Q}$ and $\alpha = 1$, so that this action is nothing but the usual one.

The role of the representation $\rho_{E,p}$ regarding modularity relies on the fact that a $\mathbb{Q}$-curve E/K is modular if and only if there exists a normalised eigenform f and a prime p such that $\rho_{E,p} \simeq \rho_{f,p}$.

1. Galois representations attached to abelian varieties

We turn now to a scenario which is more germane to the goals of this chapter. Let k be a field of characteristic zero and A be a polarised abelian variety of dimension g defined over a field L/k, regarded as always as a subfield of a fixed algebraic closure $\bar{k}$ of k. Unless needed, we will not make explicit the choice of polarisation on A.

For any prime p, the action of $G_L = \mathrm{Gal}\,(\bar{k}/L)$ on the p-adic Tate module $T_p(A)$ of A gives rise to a Galois representation

$$\varrho_A = \varrho_{A,p} : G_L \longrightarrow \mathrm{Aut}(T_p(A)).$$

If we consider the $\mathbb{Q}_p$-vector space

$$V_p(A) := T_p(A) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p,$$

equipped with the alternate pairing induced by the Weil pairing and the choice of polarisation on A, then ϱ_A provides a Galois representation

$$G_L \longrightarrow \mathrm{Aut}(V_p(A)) \simeq \mathrm{GSp}_{2g}(\mathbb{Q}_p),$$

which will be often denoted by $\varrho_A = \varrho_{A,p}$ as well. We will drop p from the notations whenever it is clear from the context.

If the abelian variety A is endowed with extra endomorphism structure, this may be reflected in the above Galois representations. Indeed, let R be a finite $\mathbb{Z}$-algebra and assume that A is equipped with a monomorphism of $\mathbb{Z}$-algebras $i : R \hookrightarrow \mathrm{End}(A)$. That is to say, assume A has *multiplication by R*.

Definition 4.1. *Let*

$$C_R(A) := \{\varphi \in \mathrm{End}^0(A) : \varphi \circ i(r) = i(r) \circ \varphi \text{ for all } r \in R\}$$

denote the $\mathbb{Q}$-subalgebra of endomorphisms of A which commute with the action of R.

Similarly, define the $\mathbb{Z}_p$-algebra $C_R(T_p(A))$ to be the commutator of $R \otimes_{\mathbb{Z}} \mathbb{Z}_p$ in $\mathrm{End}(T_p(A))$, that is,

$$C_R(T_p(A)) := \{\varphi \in \mathrm{End}(T_p(A)) : \varphi \circ i(r) = i(r) \circ \varphi \text{ for all } r \in R\}.$$

The $\mathbb{Q}$-subalgebra $C_R(A) \subseteq \mathrm{End}^0(A)$ is sometimes denoted by $\mathrm{End}^0_R(A)$. And similarly, $C_R(T_p(A))$ can be also written as $\mathrm{End}_R(T_p(A))$. Observe that $C_R(A) \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is a $\mathbb{Q}_p$-subalgebra of $C_R(T_p(A)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

Definition 4.2. *Let*

$$G_p := C_R(T_p(A))^\times \quad \text{and} \quad \bar{G}_p := (C_R(T_p(A))/pC_R(T_p(A)))^\times$$

denote the group of units of $C_R(T_p(A))$ and $C_R(T_p(A))/pC_R(T_p(A))$, respectively.

In the alternative notations quoted above, notice that

$$G_p = \mathrm{Aut}_R(T_p(A)) \quad \text{and} \quad \bar{G}_p = \mathrm{Aut}_R(A[p]).$$

Now assume that not only A is defined over L, but so is the pair (A, i). That is to say, the endomorphism structure given by $i : R \hookrightarrow \mathrm{End}(A)$ is also defined over L, which means that every single endomorphism $i(r)$, for $r \in R$, is defined over L. Then the action of G_L on the Tate module $T_p(A)$ of A commutes with the action of R induced by the embedding i, hence ϱ_A gives rise actually to a Galois representation

$$\varrho_{(A,i)} = \varrho_{(A,i),p} : G_L \longrightarrow G_p$$

attached to the pair (A, i) and the prime p.

The reduction of $\varrho_{(A,i)}$ modulo p corresponds to the Galois representation given by the action of G_L on the p-torsion subgroup $A[p] = T_p(A)/pT_p(A)$ of A. From the definitions, this Galois representation takes values on $\bar{G}_p$, thus we write

$$\bar{\varrho}_{(A,i)} = \bar{\varrho}_{(A,i),p} : G_L \longrightarrow \bar{G}_p.$$

2. Galois representations attached to points on Shimura varieties

Let k be a field of characteristic zero as before, and let R be a finite $\mathbb{Z}$-algebra such that $\mathbb{Q} \otimes R$ is a semisimple algebra. Let X be the moduli space parametrising isomorphism classes of pairs (A, i), where A is a polarised abelian variety and $i : R \hookrightarrow \mathrm{End}(A)$ is a monomorphism of $\mathbb{Z}$-algebras. We omit here the technicalities concerning the compatibility between the polarisation and i; we shall treat this with care only in the cases under study in this thesis.

The theory of Shimura varieties of PEL type (cf. e.g. [**Mil04**, §8 and 14]) yields a canonical model of X over $\mathbb{Q}$ -that we still denote X by a slight abuse of notation- so that a point $P \in X(\bar{k})$ corresponds to the $\bar{k}$-isomorphism class

$$P = [(A, i)] = \{(A', i')/\bar{k} : \text{ there exists an isomorphism of pairs } (A, i) \simeq (A', i')\}$$

of a polarised abelian variety $(A, i)/\bar{k}$ with multiplication by R. Here, two pairs (A, i) and (A', i') are said to be isomorphic if there exists an isomorphism $f : A \to A'$ of the underlying abelian surfaces such that the diagram

$$\begin{array}{ccc} A & \xrightarrow{f} & A' \\ {\scriptstyle i(r)}\downarrow & & \downarrow{\scriptstyle i'(r)} \\ A & \xrightarrow{f} & A' \end{array}$$

commutes for every $r \in R$.

Let us recall two definitions concerning the rationality of the point P and the pair (A, i), which play a fundamental role in this chapter.

Definition 4.3. *We say that the pair* $(A, i)/\bar{k}$ admits a model rational over a field L/k *if there exists a pair* (A', i') *defined over* L *such that*

$$(A' \times \bar{k}, i' \times \bar{k}) \simeq (A, i).$$

When this is the case, we say that L *is a* field of definition *for* (A, i).

Definition 4.4. *The* field of moduli $k_P = k_{(A,i)}$ *of* (A, i) *is the minimal field extension* k_P/k *such that there is an isomorphism of pairs*

$$f_s : {}^s(A, i) \xrightarrow{\simeq} (A, i)$$

for each $s \in G_{k_P}$.

The notions of field of moduli and field of definition are closely related. From the very definitions, it is clear that the field of moduli of a pair $(A, i)/\bar{k}$ is unique, and it is contained in every field of definition of (A, i). Further, as our notation already suggests, the field of moduli of (A, i) depends only on the point $P = [(A, i)] \in X(\bar{k})$. In view of this, we often say that k_P is the field of moduli of P as well. In contrast, (A, i) may admit many fields of definition, for if L/k is a field of definition for (A, i), then every extension L'/L is again a field of definition for (A, i). The most pleasant situation would be if every abelian variety parametrised by X could be defined over its field of moduli. In particular, there would be a unique minimal field of definition for each abelian variety parametrised by X. However, this does not occur in general, and deciding whether the field of moduli is a field of definition or not can be an interesting and difficult question. In the next series of examples, we collect some results in this direction:

Example 4.5. Every elliptic curve can be defined over its field of moduli.

Example 4.6. A generic odd-dimensional, principally polarised abelian variety can be defined over its field of moduli. In contrast, no generic even-dimensional, principally polarised abelian variety can be defined over its field of moduli (see [**Shi72**]). Besides, every abelian variety with CM can be defined over its field of moduli ([**Mil72, Mil74**]).

EXAMPLE 4.7. Let $C/\bar{k}$ be a genus 2 curve with field of moduli k and whose only non-trivial automorphism is the hyperelliptic involution. The obstruction for C to admit a model rational over k is an element in the two-torsion subgroup $\mathrm{Br}(k)[2]$ of the Brauer group of k, which was computed by Mestre [**Mes91**]. If the automorphism group of C is larger, then C can be defined over its field of moduli (see [**CQ05**]).

Back to our general discussion, notice that the set $X(L)$ of points on X rational over a field extension L/k (the set of *L-rational points on X*) can therefore be described as

$$X(L) = \{P \in X(\bar{k}) : k_P \subseteq L\}.$$

In particular, note that if (A, i) admits a model rational over L, then $P = [(A, i)]$ belongs to $X(L)$. However, the converse is not true in general.

Fix a point $P = [(A, i)]$ on X and assume without loss of generality that $k_P = k$ (if $k_P \supsetneq k$, replace k by k_P). For the rest of this section, we shall assume the following hypothesis:

HYPOTHESIS 4.8. *$C_R(A)$ is a field whose only roots of unity are ± 1.*

LEMMA 4.9. *Let $\mathrm{Aut}(A, i)$ denote the group of automorphisms of a polarised abelian variety (A, i) with multiplication by R. If Hypothesis 4.8 holds, then $\mathrm{Aut}(A, i) = \{\pm 1\}$.*

PROOF. From the definitions, the group $\mathrm{Aut}(A, i)$ of automorphisms of the pair (A, ι) is contained in the multiplicative group $C_R(A)^\times$ of the invertible elements in $C_R(A)$. Since the automorphism group of a polarised abelian variety is finite (see [**Mil86**, Proposition 17.5]), it follows that $\mathrm{Aut}(A, i)$ consists of roots of unity in $C_R(A)$. By our assumption, $\mathrm{Aut}(A, i) = \{\pm 1\}$. □

Choose a collection of isomorphisms

$$\mathbf{f} = \{f_s : {}^s(A, i) \longrightarrow (A, i)\}_{s \in G_k},$$

which exists because k is the field of moduli of P. Moreover, we may (and we do) choose $\mathbf{f}$ to be locally trivial[1]. Then we attach to the point P a two-cocycle on G_k with values on $\mathrm{Aut}(A, i) = \{\pm 1\}$

$$c_P : G_k \times G_k \longrightarrow \mathrm{Aut}(A, i) = \{\pm 1\}, \quad (s, t) \longmapsto c_P(s, t),$$

just by setting

$$c_P(s, t) := f_s \cdot {}^s f_t \cdot f_{st}^{-1} \in \mathrm{Aut}(A, i) = \{\pm 1\}, \quad \text{for } s, t \in G_k.$$

LEMMA 4.10. *The class $[c_P] \in \mathrm{H}^2(G_k, \{\pm 1\})$ does not depend on the choice of $\mathbf{f}$.*

PROOF. Suppose that we have two distinct collections of isomorphisms, say

$$\mathbf{f} = \{f_s : {}^s(A, i) \longrightarrow (A, i)\}_{s \in G_k} \quad \text{and} \quad \mathbf{f}' = \{f'_s : {}^s(A, i) \longrightarrow (A, i)\}_{s \in G_k},$$

and let c_P and c'_P be the corresponding cocycles defined as above, associated to $\mathbf{f}$ and $\mathbf{f}'$, respectively. Then, for each $s \in G_k$,

$$\lambda_s := f'_s \cdot f_s^{-1} \in \mathrm{Aut}(A, i),$$

hence $\lambda_s = \pm 1$. Writing $f'_s = \lambda_s \cdot f_s$, we compute

$$c'_P(s, t) = (\lambda_s \cdot f_s) \cdot {}^s(\lambda_t \cdot f_t) \cdot (\lambda_{st} \cdot f_{st})^{-1} = \lambda_s \cdot \lambda_t \cdot \lambda_{st}^{-1} c_P(s, t),$$

so that c_P and c'_P define the same cohomology class in $\mathrm{H}^2(G_k, \{\pm 1\})$, as they differ by a coboundary. □

The cocycle c_P detects the fields of definition for the pair (A, i) via the restriction morphisms

$$\mathrm{H}^2(G_k, \{\pm 1\}) \longrightarrow \mathrm{H}^2(G_L, \{\pm 1\})$$

in cohomology. Indeed, the following lemma is consequence of a well-known result due to Weil (see [**Wei56**, Theorem 3]):

[1] By this we mean that there exists a finite extension L/k such that $f_s = \mathrm{id}$ for every $s \in G_L \subseteq G_k$. We can obviously do this, for example by taking L/k to be a field of definition for (A, i).

LEMMA 4.11. *A field L/k is a field of definition for (A,i) if and only if the restriction $c_{P,L}$ of c_P to G_L induces the trivial class in $\mathrm{H}^2(G_L,\{\pm 1\})$.*

Let $\mathcal{Q}_k$ denote the set of isomorphism classes of quaternion algebras over the field k. Class field theory provides an isomorphism

$$\mathrm{H}^2(G_k,\{\pm 1\}) \simeq \mathcal{Q}_k,$$

thus we can consider the quaternion algebra (up to isomorphism) corresponding to the cohomology class $[c_P]$ associated with a point $P \in X(\bar{k})$.

DEFINITION 4.12. *For each $P \in X(\bar{k})$, let $B_P \in \mathcal{Q}_k$ denote the quaternion algebra over k (up to isomorphism) corresponding to $[c_P] \in \mathrm{H}^2(G_k,\{\pm 1\})$ via the above isomorphism.*

EXAMPLE 4.13. If $g = 1$ and $R = \mathbb{Z}$, then $X \simeq \mathbb{A}^1/\mathbb{Q}$ is the j-line classifying elliptic curves. This moduli space is not fine, but it is nevertheless true that for any point $j \in X(k)$ there exists an elliptic curve E_j defined over k representing the isomorphism class given by j. If $j \neq 0, 1728$, then $\mathrm{Aut}(E_j) = \{\pm 1\}$ and the corresponding quaternion algebra B_j is the split algebra $\mathrm{M}_2(k)$.

If $g = 2$, $R = \mathbb{Z}$ and the polarisations are assumed to be principal, then the moduli space X is commonly referred to as *Igusa's threefold*. The generic point $P \in X(k)$ corresponds to the isomorphism class of a principally polarised abelian surface $A/\bar{k}$ such that $\mathrm{End}(A) = \mathbb{Z}$. In this case, Hypothesis 4.8 is fulfilled and an algorithm for computing the quaternion algebra B_P is due to Mestre [**Mes91**].

In general, it is a difficult problem to compute the class of the cocycle c_P and the quaternion algebra B_P. See Theorems 4.20 and 4.26 below for yet other instances.

In terms of B_P, Lemma 4.11 asserts that a field L/k is a field of definition for (A,i) if and only if $B_P \otimes_k L \simeq \mathrm{M}_2(L)$. Recall that when this holds, it is said that L *splits* the quaternion algebra B_P. As an immediate consequence of that we obtain the following.

COROLLARY 4.14. *There exist infinitely many quadratic extensions L/k which are a field of definition of (A,i).*

PROOF. Take those quadratic extensions L/k which split B_P. By Corollary 1.32, there are infinitely many of them. □

We are finally in position to construct representations of G_k attached to the point $P \in X(k)$. First, we choose a collection $\mathbf{f} = \{f_s : {}^s(A,i)) \to (A,i)\}_{s\in G_k}$ as before, and define

$$\varrho_P = \varrho_{P,p} : G_k \longrightarrow G_p/\{\pm 1\}$$

by the rule

$$x \in T_p(A) \longmapsto \varrho_P(s)(x) := f_s({}^s x), \quad s \in G_k. \tag{4.1}$$

By passing to the quotient we similarly define

$$\bar{\varrho}_P = \bar{\varrho}_{P,p} : G_k \longrightarrow \bar{G}_p/\{\pm 1\}.$$

Because of the next lemma, we do not keep track of the choice of $\mathbf{f}$ in the above representations:

LEMMA 4.15. *ϱ_P and $\bar{\varrho}_P$ are group homomorphisms which do not depend on the choice of $\mathbf{f}$.*

PROOF. Let $\mathbf{f} = \{f_s : {}^s(A,i) \to (A,i)\}_{s\in G_k}$ and $\mathbf{f}' = \{f'_s : {}^s(A,i) \to (A,i)\}_{s\in G_k}$ be two distinct collections of isomorphisms. As before, define

$$\lambda : G_k \to \mathrm{Aut}(A,i) = \{\pm 1\}, \quad s \mapsto \lambda_s := f'_s \cdot f_s^{-1}.$$

Then we have

$$\begin{aligned} \varrho_{P,\mathbf{f}'}(s) : x &\longmapsto f'_s({}^s x), \\ \lambda_s \cdot \varrho_{P,\mathbf{f}}(s) : x &\longmapsto f'_s \cdot f_s^{-1} \cdot f_s({}^s x) = f'_s({}^s x). \end{aligned}$$

This shows that $\varrho_{P,\mathbf{f}'} = \varrho_{P,\mathbf{f}}$, since λ takes values in $\{\pm 1\}$. In fact, for any collection $\mathbf{f}$ as above and any map $\lambda : G_k \to \{\pm 1\}$, $f'_s := \lambda_s \cdot f_s$ defines a second collection $\mathbf{f}'$ of isomorphisms satisfying the above relation. The statement for $\bar{\varrho}_P$ follows similarly.

Now let us prove that ϱ_P is indeed a group homomorphism (the same proof works for $\bar{\varrho}_P$). Since the definition of ϱ_P does not depend on the choice of the family $\mathbf{f}$, we can assume without loss of generality that $f_{\mathrm{id}} = \mathrm{id}_{(A,i)}$, hence $\varrho_P(\mathrm{id})$ is clearly the identity element[2] in $G_p/\{\pm 1\}$.

On the other hand, observe that for $s, t \in G_k$ and $x \in T_p(A)$ we have

$$\varrho_P(st)(x) = f_{st}({}^{st}x) = c_P(s,t)^{-1}(f_s({}^s f_t({}^s({}^t x)))) = c_P(s,t)^{-1}(\varrho_P(s)(\varrho_P(t)(x))),$$

which implies that $\varrho_P(st) = c_P(s,t)^{-1} \cdot \varrho_P(s) \cdot \varrho_P(t)$ in G_p. Therefore, $\varrho_P(st) = \varrho_P(s) \cdot \varrho_P(t)$ holds in $G_p/\{\pm 1\}$. A similar computation shows that $\varrho_P(s)\varrho_P(s^{-1}) = c_P(s, s^{-1})$ in G_p, thus $\varrho_P(s^{-1}) = \varrho_P(s)^{-1}$ in $G_p/\{\pm 1\}$. Hence, ϱ_P is a group homomorphism and the statement follows. □

Definition 4.16. *We call ϱ_P (resp. $\bar{\varrho}_P$) the* Galois representation over the field of moduli attached to P *induced by the Galois action on $T_p(A)$ (resp. $A[p]$).*

Remark 4.17. In view of Lemma 4.15, if (A,i) is defined over L/k, we can choose $f_s = \mathrm{id}$ for all $s \in G_L \subseteq G_k$. Then, the restrictions of ϱ_P and $\bar{\varrho}_P$ to G_L clearly coincide with the reduction modulo ± 1 of $\varrho_{(A,i)}$ and $\bar{\varrho}_{(A,i)}$, respectively.

Remark 4.18. While Hypothesis 4.8 is fulfilled in the two scenarios we treat in detail, it could probably be relaxed by asking that $\mathrm{Aut}(A,i)$ be contained in the centre of $C_R(T_p(A))$, and working with Galois representations with values in $G_p/\mathrm{Aut}(A,i)$ and $\bar{G}_p/\mathrm{Aut}(A,i)$.

3. The case of Shimura curves

As in previous chapters, let $X_D/\mathbb{Q}$ be the Shimura curve associated with the choice of a maximal order $\mathcal{O}_D$ (unique up to conjugation) in an indefinite rational quaternion algebra B_D of discriminant $D > 1$. It is the coarse moduli scheme classifying (A,ι), where A is an abelian surface and $\iota : \mathcal{O}_D \hookrightarrow \mathrm{End}(A)$ is a monomorphism of rings. Recall that we call these pairs QM-abelian surfaces, or fake elliptic curves. If $\mathcal{O}_D^1$ denotes the group of units of $\mathcal{O}_D$ of norm 1 and we fix an isomorphism $B_D \otimes \mathbb{R} \simeq \mathrm{M}_2(\mathbb{R})$, $\mathcal{O}_D^1$ acts by conformal transformations on the complex upper half plane $\mathcal{H}$ through its image in $\mathrm{SL}_2(\mathbb{R})$, and Shimura's uniformisation (1.17) provides an isomorphism of complex analytic curves

$$X_D(\mathbb{C})^{an} \simeq \mathcal{O}_D^1 \setminus \mathcal{H}.$$

Considering again the canonical model X_D over $\mathbb{Q}$, in this section we exemplify our construction of Galois representations over fields of moduli attached to points on X_D rational over fields of arithmetic interest (the reader may keep in mind number fields and their completions at non-archimedean places). So fix a field k of characteristic zero, and let $P \in X_D(k)$ be a k-rational point on X_D. By the moduli interpretation of X_D, P corresponds to a pair $(A,\iota)/\bar{k}$ whose field of moduli is k. This amounts to saying that there exists a collection

$$\mathbf{f} = \{f_s : {}^s(A,\iota) \longrightarrow (A,\iota)\}_{s \in G_k}$$

of isomorphisms of pairs, indexed by the elements of the absolute Galois group of k. In other words, we have isomorphisms of abelian surfaces $f_s : {}^sA \to A$, one for each $s \in G_k$, such that the diagrams

$$\begin{array}{ccc} {}^sA & \xrightarrow{f_s} & A \\ {\scriptstyle {}^s\iota(\beta)}\downarrow & & \downarrow{\scriptstyle \iota(\beta)} \\ {}^sA & \xrightarrow{f_s} & A \end{array} \tag{4.2}$$

[2]Without the assumption $f_{\mathrm{id}} = \mathrm{id}_{(A,i)}$, we can still ensure that $f_{\mathrm{id}} = \pm\mathrm{id}_{(A,i)}$, since by Hypothesis 4.8 we have $\mathrm{Aut}(A,i) = \{\pm 1\}$; it follows immediately that that $\varrho_P(\mathrm{id})$ is the identity element, because ϱ_P takes values on $G_p/\{\pm 1\}$.

commute for every $\beta \in \mathcal{O}_D$. This is the case, for instance, when the pair (A, ι) admits a model rational over k.

LEMMA 4.19. *If (A, ι) does not have complex multiplication by $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$, then Hypothesis 4.8 holds for (A, ι).*

PROOF. Indeed, if (A, ι) has no complex multiplication, so that $\iota : \mathcal{O}_D \xrightarrow{\sim} \mathrm{End}(A)$ is an isomorphism, then the commutator of $\mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{Q} \simeq B_D$ in $\mathrm{End}^0(A) \simeq B_D$ is $\mathbb{Q}$, hence Hypothesis 4.8 is clearly satisfied.

Otherwise, suppose that A has complex multiplication by an order in an imaginary quadratic field $M/\mathbb{Q}$. Then, $B_D \hookrightarrow \mathrm{End}^0(A) \simeq \mathrm{M}_2(M)$, and the commutator of $\mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{Q} \simeq B_D$ in $\mathrm{End}^0(A)$ is M. Whenever $M \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, the only roots of unity in $M^\times$ are ± 1, hence Hypothesis 4.8 is still satisfied and the statement follows. □

The obstruction for the abelian surfaces parametrised by X_D to admit a model rational over their field of moduli was characterised by Jordan in [**Jor86**, Theorem 1.1], which can be rephrased in our setting as follows:

THEOREM 4.20 (Jordan). *Let $P \in X_D(k)$ be a k-point on X_D and assume that it does not have complex multiplication by $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$. Then $B_P = B_D \otimes k$.*

In other words, for a given field extension L/k, there exists a QM-abelian surface (A, ι) over L such that $P = [(A, \iota) \times \bar{k}]$ if and only if L splits B_D.

REMARK 4.21. It is important to notice that B_P does not depend actually on the point P, and in fact, it does not depend on the field k either, in the sense that B_P arises as the extension of scalars from the rational quaternion algebra B_D. In this regard, the reader may compare the previous theorem with Theorem 4.26 below.

By virtue of Lemma 4.19, under Hypothesis 4.8 we can attach Galois representations to points $P \in X_D(k)$ corresponding to pairs $(A, i)/\bar{k}$ with no complex multiplication by $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$, where k is a field of characteristic zero.

Towards the proof of Theorem 5.1 in the next chapter, we focus now on local points on the Shimura curve X_D over imaginary quadratic fields. In particular, we may regard X_D as a curve over the completion of $\mathbb{Q}$ at finite rational places (by base change) rather than over $\mathbb{Q}$, although we still write X_D for ease of notation.

So fix at the outset a quadratic extension $K'/\mathbb{Q}$ splitting B_D, and let $K/\mathbb{Q}$ be an imaginary quadratic field. Let v and v' be places of K and K', respectively, above the same rational prime ℓ, and let us denote by w the unique extension of the ℓ-adic valuation on $\mathbb{Q}_\ell$ to the composite field $L_w := K_v \cdot K'_{v'}$. Since $K'_{v'}$ splits B_D, also L_w does. Let $P_v \in X_D(K_v)$ be a K_v-rational point. By Theorem 4.20, we can choose a pair (A_v, ι_v) defined over L_w such that $P_v = [(A_v, \iota_v)]$.

Fix a rational prime p dividing D. As in Section 1, there is a Galois representation

$$\varrho_{(A_v,\iota_v)} = \varrho_{(A_v,\iota_v),p} : G_{L_w} \longrightarrow \mathrm{Aut}_{\mathcal{O}_D}(T_p(A_v)) = C_{\mathcal{O}_D}(T_p(A_v))^\times$$

arising from the action of G_{L_w} on the p-adic Tate module $V_p(A_v) = T_p(A_v) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ of A_v. By [**Oht74**], the assumption that p divides D provides an isomorphism

$$\mathrm{Aut}_{\mathcal{O}_D}(T_p(A_v)) \simeq (\mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times,$$

hence the above Galois representation can actually be regarded as

$$\varrho_{(A_v,\iota_v)} = \varrho_{(A_v,\iota_v),p} : G_{L_w} \longrightarrow \mathrm{Aut}_{\mathcal{O}_D}(T_p(A_v)) \simeq (\mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times \subseteq (B_D \otimes_{\mathbb{Q}} \mathbb{Q}_p)^\times.$$

By reduction modulo p, we find that the Galois representation arising from the action of G_{L_w} on $A_v[p]$ associated to the pair (A_v, ι_v) then takes the form

$$\bar{\varrho}_{(A_v,\iota_v)} = \bar{\varrho}_{(A_v,\iota_v),p} : G_{L_w} \longrightarrow \mathrm{Aut}_{\mathcal{O}_D}(A_v[p]) \simeq (\mathcal{O}_D/p\mathcal{O}_D)^\times \subseteq \mathrm{GL}_2(\mathbb{F}_{p^2}).$$

Along with these two representations, Jordan attached to the pair (A_v, ι_v) a finite order character arising from the Galois action on the canonical torsion subgroup of (A_v, ι_v) at p, which recall that it is defined as

$$C_p := A_v[I(p)] \simeq \mathcal{O}_D/I(p) \subseteq A_v[p],$$

where $I(p)$ denotes the unique two-sided $\mathcal{O}_D$-ideal of reduced norm p and

$$A_v[I(p)] = \{x \in A_v(\bar{L}_w) : \iota_v(\gamma)(x) = 0 \text{ for all } \gamma \in I(p)\} \subseteq A_v[p].$$

Working locally at p, and fixing a choice of a Nebentypus character as in (2.6), there is a (non-canonical) isomorphism

$$C_p \simeq \mathcal{O}_D/I(p) \simeq \mathbb{F}_{p^2}$$

between the torsion $\mathcal{O}_D$-submodule C_p of $A_v[p]$ and $\mathbb{F}_{p^2}$. Moreover, the canonical torsion subgroup C_p is rational over L_w because of its uniqueness: indeed, ${}^{\sigma}C_p$ is a torsion $\mathcal{O}_D$-submodule of $A_v[p]$ for every $\sigma \in G_{L_w}$, hence it is necessarily C_p.

In particular, from the isomorphism $C_p \simeq \mathbb{F}_{p^2}$ it follows that

$$\mathrm{Aut}_{\mathcal{O}_D}(C_p) \simeq \mathbb{F}_{p^2}^{\times},$$

hence the action of G_{L_w} on C_p gives rise to the so-called *canonical isogeny character at p*:

$$\alpha_{(A_v,\iota_v)} = \alpha_{(A_v,\iota_v),p} : G_{L_w} \longrightarrow \mathrm{Aut}_{\mathcal{O}_D}(C_p) \simeq \mathbb{F}_{p^2}^{\times}.$$

Changing the isomorphism between C_p and $\mathbb{F}_{p^2}$ has the effect of replacing the character $\alpha_{(A_v,\iota_v)}$ by $\alpha^p_{(A_v,\iota_v)}$.

We shall sometimes regard $\alpha_{(A_v,\iota_v)}$ as a character on

$$G^{ab}_{L_w} := \mathrm{Gal}\,(L^{ab}_w/L_w),$$

where L^{ab}_w is the abelian closure of L_w in $\bar{L}_w$. This character is closely related to the Galois representation $\varrho_{(A_v,\iota_v)}$. Indeed:

PROPOSITION 4.22. *With notations as before:*

(a) *There is a $\mathbb{F}_{p^2}$-basis of $A_v[p]$ with respect to which*

$$\bar{\varrho}_{(A_v,\iota_v)} = \begin{pmatrix} (\alpha_{(A_v,\iota_v)})^p & 0 \\ * & \alpha_{(A_v,\iota_v)} \end{pmatrix}.$$

For any $\sigma \in G_{L_w}$, the characteristic polynomial of $\varrho_{(A_v,\iota_v)}(\sigma) \in \mathrm{Aut}_{\mathbb{F}_p}(A_v[p])$ is

$$[(T - \alpha_{(A_v,\iota_v)}(\sigma))(T - \alpha_{(A_v,\iota_v)}(\sigma)^p)]^2.$$

(b) *If $p \neq \ell$, $\varrho^{12}_{(A_v,\iota_v)}$ and $\alpha^{12}_{(A_v,\iota_v)}$ are unramified.*

PROOF. Statement (a) is [**Jor81**, Proposition 4.3.10], and (b) follows from [**Jor86**, §3]. □

Also, as in [**Jor86**, Proposition 4.6], we have the following:

LEMMA 4.23. *If we denote the reduction of the p-th cyclotomic character by*

$$\bar{\chi}_p : G_{K_v} \longrightarrow \mathrm{Aut}(\mu_p) \simeq \mathbb{F}_p^{\times},$$

then it holds

$$N_{\mathbb{F}_{p^2}/\mathbb{F}_p} \circ \alpha_{(A_v,\iota_v)} = \bar{\chi}_{p|G_{L_w}}.$$

Let us assume now that A_v does not have complex multiplication by $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$, and let $P_v \in X_D(K_v)$ denote the point on X_D parametrising the pair (A_v, ι_v). By virtue of Lemma 4.19, Hypothesis 4.8 holds and therefore, as explained in Section 2, we can attach to the point P_v Galois representations

$$\varrho_{P_v} = \varrho_{P_v,p} : G_{K_v} \longrightarrow \mathrm{Aut}_{\mathcal{O}_D}(T_p(A_v))/\{\pm 1\} \subseteq \mathrm{GL}_4(\mathbb{Z}_p)/\{\pm 1\},$$

$$\bar{\varrho}_{P_v} = \bar{\varrho}_{P_v,p} : G_{K_v} \longrightarrow \mathrm{Aut}_{\mathcal{O}_D}(A_v[p])/\{\pm 1\} \subseteq \mathrm{GL}_2(\mathbb{F}_{p^2})/\{\pm 1\}$$

and, in the same way, a character

$$\alpha_{P_v} = \alpha_{P_v,p} : G_{K_v} \longrightarrow \mathrm{Aut}_{\mathcal{O}_D}(C_p)/\{\pm 1\} \simeq \mathbb{F}_{p^2}^\times/\{\pm 1\}.$$

By Remark 4.17, the restrictions of these representations to $G_{L_w} \subseteq G_{K_v}$ coincide with the reduction modulo ± 1 of $\varrho_{(A_v,\iota_v)}$, $\bar{\varrho}_{(A_v,\iota_v)}$ and $\alpha_{(A_v,\iota_v)}$, respectively.

We conclude this section by collecting a few basic properties of the character α_{P_v}, which we will later use in the proof of Theorem 5.1 in Chapter 5. To begin with, note that from Proposition 4.22 we deduce the following

COROLLARY 4.24. *For $p \neq \ell$, $\alpha_{P_v,p}^{12}$ is unramified.*

Secondly, let us write

$$\tilde{\varrho}_{P_v} : G_{K_v} \longrightarrow \mathrm{Aut}_{\mathcal{O}_D}(T_p(A_v)) \quad \text{and} \quad \tilde{\alpha}_{P_v} : G_{K_v} \longrightarrow \mathbb{F}_{p^2}^\times$$

for the lifts of ϱ_{P_v} and α_{P_v}, respectively, associated to a choice of $\mathbf{f}$ as defined in (4.1). These lifts are not homomorphisms in general, but it is easy to check that for any $\sigma \in G_{K_v}$ we have

$$\tilde{\varrho}_{P_v}(\sigma^2) = \pm\tilde{\varrho}_{P_v}(\sigma)^2 \quad \text{and} \quad \tilde{\alpha}_{P_v}(\sigma^2) = \pm\tilde{\alpha}_{P_v}(\sigma)^2.$$

It is also important to notice that while α_{P_v} factors through the maximal abelian quotient $G_{K_v}^{ab}$ of G_{K_v}, the same is not true for the lift $\tilde{\alpha}_{P_v}$: it does not necessarily descend to a map on $G_{K_v}^{ab}$. However, it will suffice for our purposes the obvious observation that for every $\sigma \in G_{K_v}$, the value $\tilde{\alpha}_{P_v}(\sigma)^2 \in \mathbb{F}_{p^2}^\times$ depends only on the class of σ in $G_{K_v}^{ab}$.

Finally, using the fact that $\tilde{\alpha}_{P_v|G_{L_w}}$ coincides with $\alpha_{(A_v,\iota_v)}$, Lemma 4.23 implies that

$$N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\tilde{\alpha}_{P_v|G_{L_w}}(\sigma)) = \chi_{p|G_{L_w}}(\sigma), \quad \text{for all } \sigma \in G_{L_w}.$$

Since L_w has at most degree 2 over K_v, we can write

$$N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\tilde{\alpha}_{P_v|G_{L_w}}(\sigma^2)) = \chi_{p|G_{L_w}}(\sigma^2) = \chi_p(\sigma)^2, \quad \text{for all } \sigma \in G_{K_v}.$$

And, using that $\tilde{\alpha}_{P_v|G_{L_w}}(\sigma^2) = \pm\tilde{\alpha}_{P_v}(\sigma)^2$ for all $\sigma \in G_{K_v}$, we get that

$$N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\tilde{\alpha}_{P_v}(\sigma)^2) = \chi_p(\sigma)^2, \quad \text{for all } \sigma \in G_{K_v}. \tag{4.3}$$

4. The case of Atkin-Lehner quotients of Shimura curves

Keeping the same notations as in the previous section, let now m be a positive divisor of D, and consider the Atkin-Lehner quotient $X_D^{(m)}$ of the Shimura curve X_D by the action of the Atkin-Lehner involution ω_m associated with m. In this section we show how to attach Galois representations over fields of moduli to points on $X_D^{(m)}$ rational over fields of characteristic zero.

Our ultimate goal is to apply these representations to study the set of rational points on $X_D^{(m)}$. More precisely, Theorem 5.2 in Chapter 5 combines these Galois representations with the coverings introduced in Chapter 2 to give sufficient conditions for the emptiness of the set $X_D^{(m)}(\mathbb{Q})$. As we can only apply our methods when D is odd and $m \neq D$, it is harmless to assume that $D = pm$ for some odd prime p such that $(\frac{m}{p}) = -1$, as otherwise [**RSY05**, Theorem 3.1] implies that $X_D^{(m)}(\mathbb{A}_\mathbb{Q}) = \emptyset$. In view of this, we make the following assumption for the rest of this section:

ASSUMPTION 4.25. *D is odd, and $D = pm$ for some prime p with $(\frac{m}{p}) = -1$.*

This assumption endows $X_D^{(m)}$ with a moduli interpretation inherited from X_D as we now recall (cf. Section 3.4 of Chapter 1). By virtue of Lemma 1.45, Assumption 4.25 implies that $\mathcal{O}_D$ admits a twist of some degree $\delta \geq 1$ and norm m, hence we can choose elements $\mu, \chi \in \mathcal{O}_D$ with $\mu^2 + D\delta = 0$, $\chi^2 = m$ and $\mu\chi = -\chi\mu$, for some integer $\delta \geq 1$. The element χ determines an optimal embedding

$$\vartheta_\chi : R_m \hookrightarrow \mathcal{O}_D,$$

where R_m denotes the ring of integers of the real quadratic field $E = \mathbb{Q}(\sqrt{m})$, which in turn induces a forgetful map

$$\pi_{R_m} : X_D \longrightarrow \mathcal{H}_m$$

from X_D onto the Hilbert modular surface parametrising abelian surfaces with real multiplication by R_m (cf. Section 3.4 of Chapter 1). In moduli-theoretic terms, the forgetful map π_{R_m} is described by the rule

$$[(A,\iota)] \longmapsto [(A,\iota_{|R_m})], \quad \text{where } \iota_{|R_m} := \iota \circ \vartheta_\chi.$$

Further, π_{R_m} is a quasi-finite map that factors over $\mathbb{Q}$ into the natural projection $\pi_m : X_D \to X_D^{(m)}$ composed by a birrational morphism

$$b_m : X_D^{(m)} \dashrightarrow \pi_{R_m}(X_D) \subseteq \mathcal{H}_m$$

which has an inverse defined on the whole $\pi_{R_m}(X_D)$ except for a finite set of CM points (cf. Proposition 1.46).

This way, the Atkin-Lehner quotient $X_D^{(m)}/\mathbb{Q}$ is the coarse moduli scheme classifying isomorphism classes of abelian surfaces with real multiplication (RM) by E and admitting QM by $\mathcal{O}_D$.

If k is a field of characteristic zero, the above moduli interpretation implies that a k-rational point Q in $X_D^{(m)}(\bar{k})$ corresponds to the isomorphism class of a pair $(A,i)/\bar{k}$ where:

- A is an abelian surface such that the ring $\mathrm{End}(A)$ contains $\mathcal{O}_D$,
- $i : R_m \hookrightarrow \mathrm{End}(A)$ is a ring monomorphism and
- there exists a collection

$$\mathbf{f} = \{f_s : {}^s(A,i) \longrightarrow (A,i)\}_{s\in G_k}$$

of isomorphisms of pairs, one for each Galois automorphism of G_k.

Notice that the third condition means that for each $s \in G_k$ there is an isomorphism $f_s : {}^sA \to A$ such that the diagram

$$\begin{array}{ccc} {}^sA & \xrightarrow{f_s} & A \\ {\scriptstyle {}^{s}i(\alpha)}\downarrow & & \downarrow{\scriptstyle i(\alpha)} \\ {}^sA & \xrightarrow{f_s} & A \end{array} \tag{4.4}$$

commutes for every $\alpha \in R_m$.

The obstruction for a representative $(A,i)/\bar{k}$ of Q to admit a model rational over k, its field of moduli, is given by the next theorem (see [**BFGR06**, Theorem 4.1]):

Theorem 4.26 (Bruin-Flynn-González-Rotger). *Let $Q = [(A,i)] \in X_D^{(m)}(k)$ be a non-CM point and K/k be the (at most quadratic) extension of k generated by the coordinates of $\pi_m^{-1}(Q)$. Write $K = k(\sqrt{\delta})$ for some $\delta \in k^\times$. Then*

$$B_Q = (B_D \otimes_{\mathbb{Q}} k) \otimes (\frac{\delta, m}{k}).$$

That is to say, (A,i) admits a model rational over a field L/k if and only if $B_D \otimes_{\mathbb{Q}} L \simeq (\frac{\delta,m}{L})$.

The reader may compare this result with Theorem 4.20; observe that now the obstruction for the field of moduli of a pair $(A,i)/\bar{k}$ to be a field of definition does depend on the point $Q = [(A,\iota)] \in X_D^{(m)}(\bar{k})$.

The main ingredient in the proof of Theorem 5.2 is the study of the Galois representations attached to rational points on $X_D^{(m)}$ over a local field, thus we now focus on exemplifying the method explained in Section 2 in this setting.

Let ℓ be a prime, $Q_\ell \in X_D^{(m)}(\mathbb{Q}_\ell)$ be a $\mathbb{Q}_\ell$-rational point on $X_D^{(m)}$ and $(A_\ell, i_\ell)/L$ be a pair as above, defined over some finite extension $L/\mathbb{Q}_\ell$, such that $Q_\ell = [(A_\ell, i_\ell)]$. The action of G_L on $T_p(A_\ell)$ gives rise to a Galois representation

$$\varrho_{(A_\ell,i),p} : G_L \longrightarrow \mathrm{Aut}_{R_m}(T_p(A_\ell)) \subseteq \mathrm{Aut}(T_p(A_\ell)) \simeq \mathrm{GSp}_4(\mathbb{Z}_p).$$

Recall our running assumption that the prime p be inert in E, let $\mathfrak{p} = pR_m$ denote the unique prime of E above p and $R_{m,\mathfrak{p}} = R_m \otimes \mathbb{Z}_p$ the completion of R_m along $\mathfrak{p}$.

The Galois group G_L acts on $T_p(A_\ell)$ by $R_{m,\mathfrak{p}}$-linear transformations, giving rise to a Galois representation

$$\varrho_{(A_\ell,i_\ell),\mathfrak{p}} : G_L \longrightarrow \mathrm{Aut}_{R_m}(T_p(A_\ell)) \simeq \mathrm{GL}_2(R_{m,\mathfrak{p}}),$$

which may be regarded as a subrepresentation of $\varrho_{(A_\ell,i_\ell),p}$. Likewise, the reduction of $\varrho_{(A_\ell,i_\ell),\mathfrak{p}}$ modulo $\mathfrak{p}$ yields a residual Galois representation

$$\bar{\varrho}_{(A_\ell,i_\ell),\mathfrak{p}} : G_L \longrightarrow \mathrm{Aut}_{R_m}(A_\ell[\mathfrak{p}]) \simeq \mathrm{GL}_2(\mathbb{F}_{p^2}).$$

Finally, consider again the canonical torsion subgroup $C_p = A_\ell[I(p)]$ of A_ℓ at p, now regarded as a subgroup of

$$A_\ell[\mathfrak{p}] = \{x \in A_\ell(\bar{\mathbb{Q}}_p) : \iota_\ell(\gamma)(x) = 0 \text{ for all } \gamma \in \mathfrak{p} \subseteq R_m\}.$$

The local quaternion algebra $B_{D,p} := B_D \otimes_{\mathbb{Q}} \mathbb{Q}_p$ can be written as

$$B_{D,p} = E_{\mathfrak{p}} + E_{\mathfrak{p}} \cdot \pi,$$

where $\pi^2 = p$ and $\pi\beta = {}^\tau\beta\pi$ for any $\beta \in E_{\mathfrak{p}}$, with τ the non-trivial element in $\mathrm{Gal}\,(E_{\mathfrak{p}}/\mathbb{Q}_p)$. Moreover, the local maximal order of $B_{D,p}$ is

$$\mathcal{O}_{D,p} = R_{m,\mathfrak{p}} + R_{m,\mathfrak{p}}\pi$$

(cf. [**Vig80**, p. 33]) and we also have

$$I(p)_p := I(p) \otimes \mathbb{Z}_p = \mathfrak{p}R_{m,\mathfrak{p}} + R_{m,\mathfrak{p}}\pi,$$

whereas $I(p)_q = \mathcal{O}_{D,q}$ at every rational prime $q \neq p$.

Since $T_p(A_\ell)$ is a principal $\mathcal{O}_{D,p}$-module, we have

$$A_\ell[\mathfrak{p}] = T_p(A_\ell)/\mathfrak{p}T_p(A_\ell) \simeq \mathcal{O}_{D,p}/\mathfrak{p}\mathcal{O}_{D,p}$$

and

$$C_p = \mathcal{O}_{D,p}/I(p)_p \simeq R_{m,\mathfrak{p}}/\mathfrak{p}R_{m,\mathfrak{p}} \simeq \mathbb{F}_{p^2}.$$

Since $I(p)$ is the unique two-sided $\mathcal{O}_D$-ideal of reduced norm p, the action of G_L leaves $I(p)$ invariant. Moreover, G_L acts R_m-linearly on C_p, giving rise to a character

$$\alpha_{(A_\ell,i_\ell),\mathfrak{p}} : G_L \longrightarrow \mathrm{Aut}_{R_m}(C_p) \simeq \mathbb{F}_{p^2}^\times.$$

Let $P_\ell \in X_D(K_\ell)$ be a preimage of Q_ℓ under the projection π_m, rational over some extension $K_\ell/\mathbb{Q}_\ell$ of degree $[K_\ell : \mathbb{Q}_\ell] \leq 2$. In terms of moduli, P_ℓ may be represented by the pair $(A_\ell, \iota_\ell)/\bar{\mathbb{Q}}_\ell$, where $\iota_\ell : \mathcal{O}_D \hookrightarrow \mathrm{End}(A_\ell)$ is a monomorphism such that $\iota_{\ell|R_m} = i_\ell$.

LEMMA 4.27. *If D is odd, $[K_\ell : \mathbb{Q}_\ell] = 2$ and $B_P = B_D \otimes_{\mathbb{Q}_\ell} K_\ell \simeq \mathrm{M}_2(K_\ell)$.*

PROOF. The hypothesis $2 \nmid D$ implies, by the results in [**JL85**], that $X_D(\mathbb{Q}_\ell) = \emptyset$. This implies that K_ℓ is quadratic over $\mathbb{Q}_\ell$.

As for the second assertion, note first that $B_P = B_D \otimes_{\mathbb{Q}_\ell} K_\ell$ by Theorem 4.20. For primes $\ell \nmid D$, it is plain that $B_D \otimes_{\mathbb{Q}_\ell} K_\ell$ is isomorphic to the split algebra $\mathrm{M}_2(K_\ell)$. Assume therefore that $\ell \mid D$, and choose an element e in $\mathbb{Z}_\ell^\times \setminus \mathbb{Z}_\ell^{\times 2}$, so that the only quadratic extensions of $\mathbb{Q}_\ell$ are $\mathbb{Q}_\ell(\sqrt{e})$, $\mathbb{Q}_\ell(\sqrt{\ell})$ and $\mathbb{Q}_\ell(\sqrt{e\ell})$. The three of them are subfields of $B_{D,\ell}$, because

$$B_{D,\ell} \simeq \mathbb{Q}_\ell(\sqrt{e}) + \mathbb{Q}_\ell(\sqrt{e})\pi,$$

where $\pi^2 = \ell$ and $\pi\beta = {}^\tau\beta\pi$ for all $\beta \in \mathbb{Q}_\ell(\sqrt{e})$, with $\tau \in \mathrm{Gal}\,(\mathbb{Q}_\ell(\sqrt{e})/\mathbb{Q}_\ell)$ the non-trivial automorphism (see [**Vig80**, Théorème II.1.3]). Hence K_ℓ necessarily splits B_D. □

Since we are assuming D is odd, by Theorem 4.20 we can choose the pairs (A_ℓ, ι_ℓ) and $(A_\ell, i_\ell = \iota_{\ell|R_m})$ representing P_ℓ and Q_ℓ to be defined over K_ℓ. With these choices, the following is an immediate consequence of Proposition 4.22 and Lemma 4.23.

PROPOSITION 4.28. *With notations as before:*

(a) *There is a $\mathbb{F}_{p^2}$-basis of $A_\ell[\mathfrak{p}]$ with respect to which*

$$\bar{\varrho}_{(A_\ell,i_\ell),\mathfrak{p}} = \begin{pmatrix} (\alpha_{(A_\ell,i_\ell),\mathfrak{p}})^p & 0 \\ * & \alpha_{(A_\ell,i_\ell),\mathfrak{p}} \end{pmatrix}.$$

(b) *If $p \neq \ell$, then $\varrho^{12}_{(A_\ell,i_\ell),\mathfrak{p}}$ is unramified. In particular, $\alpha^{12}_{(A_\ell,i_\ell),\mathfrak{p}}$ is unramified.*

(c) *If $\bar{\chi}_p : G_{\mathbb{Q}_\ell} \to \mathrm{Aut}(\mu_p) \simeq \mathbb{F}_p^\times$ denotes the reduction of the p-cyclotomic character, then $N_{\mathbb{F}_{p^2}/\mathbb{F}_p} \circ \alpha_{(A_\ell,i_\ell),\mathfrak{p}} = \bar{\chi}_{p|G_{K_\ell}}$. Hence, $\det(\bar{\varrho}_{(A_\ell,i_\ell),\mathfrak{p}}) = \bar{\chi}_{p|G_{K_\ell}}$.*

As in the previous section, we can apply now the machinery introduced in Section 2 to attach Galois representations to the points in $X_D^{(m)}(\mathbb{Q}_\ell)$, even if they cannot be represented by an abelian surface defined over $\mathbb{Q}_\ell$.

LEMMA 4.29. *Assume that A_ℓ does not have complex multiplication by $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$. Then the pair (A_ℓ, i_ℓ) satisfies Hypothesis 4.8.*

PROOF. Suppose first that A_ℓ has no complex multiplication. In this case, the commutator of $R_m \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \mathbb{Q}(\sqrt{m}) = E$ in $\mathrm{End}^0(A_\ell) \simeq B_D$ is E itself because it is a maximal subfield of B_D. Since E is a real quadratic field, its only units are ± 1.

Assume now that A_ℓ has complex multiplication by an order in an imaginary quadratic field $M/\mathbb{Q}$. We have $B_D \hookrightarrow \mathrm{End}^0(A_\ell) \simeq \mathrm{M}_2(M)$, and the commutator of $R_m \otimes_{\mathbb{Z}} \mathbb{Q} = E$ in $\mathrm{End}^0(A_v)$ is ME. It is easy to check that the only roots of unity in ME are ± 1, unless $M = \mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$. □

From now on, we assume that A_ℓ does not have complex multiplication by $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$. In light of Lemma 4.29, we can attach to the point $Q_\ell = [(A_\ell, i_\ell)] \in X_D^{(m)}(\mathbb{Q}_\ell)$ Galois representations

$$\begin{aligned} \varrho_{Q_\ell,\mathfrak{p}} : G_{\mathbb{Q}_\ell} &\longrightarrow \mathrm{Aut}_{R_m}(T_p(A_\ell))/\{\pm 1\} \simeq \mathrm{GL}_2(R_{m,\mathfrak{p}})/\{\pm 1\}, \\ \bar{\varrho}_{Q_\ell,\mathfrak{p}} : G_{\mathbb{Q}_\ell} &\longrightarrow \mathrm{Aut}_{R_m}(A_\ell[\mathfrak{p}])/\{\pm 1\} \simeq \mathrm{GL}_2(\mathbb{F}_{p^2})/\{\pm 1\} \end{aligned}$$

and

$$\alpha_{Q_\ell,\mathfrak{p}} : G_{\mathbb{Q}_\ell} \longrightarrow \mathrm{Aut}_{R_m}(C_p)/\{\pm 1\} \simeq \mathbb{F}_{p^2}^\times/\{\pm 1\},$$

extending $\varrho_{(A_\ell,i_\ell),\mathfrak{p}}$, $\bar{\varrho}_{(A_\ell,i_\ell),\mathfrak{p}}$ and $\alpha_{(A_\ell,i_\ell),\mathfrak{p}}$, respectively.

As before, we write

$$\tilde{\varrho}_{Q_\ell,\mathfrak{p}} : G_{\mathbb{Q}_\ell} \longrightarrow \mathrm{Aut}_{R_m}(T_p(A_\ell)) \quad \text{and} \quad \tilde{\alpha}_{Q_\ell,\mathfrak{p}} : G_{\mathbb{Q}_\ell} \longrightarrow \mathbb{F}_{p^2}^\times$$

for the lifts of $\varrho_{Q_\ell,\mathfrak{p}}$ and $\alpha_{Q_\ell,\mathfrak{p}}$ associated to a choice of $\mathbf{f}$ by (4.1). Again, these lifts are not homomorphisms in general, but their restrictions to G_{K_ℓ} coincide with $\varrho_{(A_\ell,i_\ell),\mathfrak{p}}$ and $\alpha_{(A_\ell,i_\ell),\mathfrak{p}}$, respectively, and for any $\sigma \in G_{\mathbb{Q}_\ell}$ it is easy to see that

$$\tilde{\varrho}_{Q_\ell}(\sigma^2) = \pm\tilde{\varrho}_{Q_\ell}(\sigma)^2 \quad \text{and} \quad \tilde{\alpha}_{Q_\ell}(\sigma^2) = \pm\tilde{\alpha}_{Q_\ell}(\sigma)^2.$$

While both $\alpha_{(A_\ell,i_\ell),\mathfrak{p}}$ and $\alpha_{Q_\ell,\mathfrak{p}}$ descend to characters on $G_{K_\ell}^{ab}$ and $G_{\mathbb{Q}_\ell}^{ab}$, respectively, the map $\tilde{\alpha}_{Q_\ell,\mathfrak{p}}$ does not necessarily factor through $G_{K_\ell}^{ab}$, though $\tilde{\alpha}^2_{Q_\ell,\mathfrak{p}}$ does.

From Proposition 4.28 we deduce the following:

COROLLARY 4.30. *With the above notations:*

(a) *If $\ell \neq p$, $\alpha^{12}_{Q_\ell,\mathfrak{p}}$ is unramified. More precisely, we have $\tilde{\alpha}_{Q_\ell,\mathfrak{p}}(I_\ell)^{24} = \{1\}$.*

(b) *$\det(\bar{\varrho}_{Q_\ell,\mathfrak{p}}(\sigma)) = \pm\bar{\chi}_p(\sigma)$ for every $\sigma \in G_{\mathbb{Q}_\ell}$.*

To conclude with the basic properties of these representations, we now turn to give an explicit description of $\bar{\varrho}_{Q_\ell,\mathfrak{p}}$ in terms of the character $\alpha_{Q_\ell,\mathfrak{p}}$. To do so, choose a family of isomorphisms

$$\mathbf{f} = \{f_\sigma : {}^\sigma(A_\ell, i_\ell) \longrightarrow (A_\ell, i_\ell)\}_{\sigma \in G_{\mathbb{Q}_\ell}}$$

satisfying (4.4); this is possible because the field of moduli of (A_ℓ, i_ℓ) is $\mathbb{Q}_\ell$. For each $\sigma \in G_{\mathbb{Q}_\ell}$, the automorphism $B_D \to B_D$ given by the rule

$$\beta \mapsto f_\sigma {}^\sigma\beta f_\sigma^{-1}$$

is inner by the Noether-Skolem Theorem, hence there exists an element $\omega_\sigma \in \mathcal{O}_D$ such that

$$f_\sigma{}^\sigma \beta f_\sigma^{-1} = \omega_\sigma \beta \omega_\sigma^{-1}$$

for all $\beta \in B_D$. Moreover, by the commutativity of (4.4), $\beta = \omega_\sigma \beta \omega_\sigma^{-1}$ for every $\beta \in E$, so that ω_σ belongs to the commutator of E in B_D, which is E itself because it is a maximal subfield of B_D. This shows that, for every $\sigma \in G_{\mathbb{Q}_\ell}$, ω_σ lies in $R_m = \mathcal{O}_D \cap E$, and in this way we obtain a character

$$\psi : G_{\mathbb{Q}_\ell} \longrightarrow E^\times/\mathbb{Q}^\times, \quad \sigma \longmapsto \omega_\sigma.$$

Actually, write $\mathrm{Gal}\,(K_\ell/\mathbb{Q}_\ell) = \{1, \sigma_0\}$ and fix an isomorphism of pairs

$$f_0 : ({}^{\sigma_0}A_\ell, {}^{\sigma_0}i_\ell) \longrightarrow (A_\ell, i_\ell).$$

We can extend f_0 to a collection of isomorphisms $\mathbf{f} = \{f_\sigma\}_{\sigma \in G_{\mathbb{Q}_\ell}}$ by setting $f_\sigma = \mathrm{id}$ if $\sigma \in G_{K_\ell}$ and $f_\sigma = f_0$ otherwise, and note that $\mathbf{f}$ satisfies (4.4). Accordingly, set $\omega_\sigma = 1$ if $\sigma \in G_{K_\ell}$ and $\omega_\sigma = \omega_0$ otherwise. Then the character ψ factors through the quotient $\mathrm{Gal}\,(K_\ell/\mathbb{Q}_\ell)$, thus we can regard

$$\psi : G_{\mathbb{Q}_\ell} \longrightarrow \{\pm 1\}$$

as a character with values in $\{\pm 1\}$ which is trivial on $G_{K_\ell} \subseteq G_{\mathbb{Q}_\ell}$.

LEMMA 4.31. *There exists a $\mathbb{F}_{p^2}$-basis of $A_\ell[\mathfrak{p}]$ with respect to which*

$$\begin{array}{rccc} \bar{\varrho}_{Q_\ell,\mathfrak{p}} : & G_{\mathbb{Q}_\ell} & \longrightarrow & \mathrm{GL}_2(\mathbb{F}_{p^2})/\{\pm 1\} \\ & \sigma & \longmapsto & \begin{pmatrix} \psi(\sigma)\tilde{\alpha}_{Q_\ell,\mathfrak{p}}(\sigma)^p & 0 \\ * & \tilde{\alpha}_{Q_\ell,\mathfrak{p}}(\sigma) \end{pmatrix} \mod \pm 1. \end{array}$$

PROOF. Write $\mathcal{O}_{D,p} = R_{m,\mathfrak{p}} + R_{m,\mathfrak{p}} \cdot \pi$, and let $x \in A_\ell[\mathfrak{p}]$ be such that

$$A_\ell[\mathfrak{p}] = \mathcal{O}_{D,p}/\mathfrak{p}\mathcal{O}_{D,p} \cdot x = R_{m,\mathfrak{p}}/\mathfrak{p}R_{m,\mathfrak{p}} \cdot x + R_{m,\mathfrak{p}}/\mathfrak{p}R_{m,\mathfrak{p}} \cdot \pi(x).$$

We shall compute $\bar{\varrho}_{Q_\ell,\mathfrak{p}}$ with respect to the $\mathbb{F}_{p^2}$-basis $\{x, \pi(x)\}$ of $A_\ell[\mathfrak{p}]$. Fix an element $\sigma \in G_{\mathbb{Q}_\ell}$ and write

$$\tilde{\varrho}_{Q_\ell,\mathfrak{p}}(\sigma)(x) = f_\sigma({}^\sigma x) = u_\sigma \cdot x + v_\sigma \cdot \pi(x)$$

for some $u_\sigma, v_\sigma \in R_{m,\mathfrak{p}}$, which are uniquely determined modulo $\mathfrak{p}$. In order to compute $\tilde{\varrho}_{Q_\ell,\mathfrak{p}}(\sigma)(\pi(x))$, first note that

$$f_\sigma{}^\sigma \pi f_\sigma^{-1} = \omega_\sigma \pi \omega_\sigma^{-1} = \pi^\tau \omega_\sigma \omega_\sigma^{-1} = \psi(\sigma)\pi,$$

where $\tau \in \mathrm{Gal}\,(E_\mathfrak{p}/\mathbb{Q}_p)$ denotes the non-trivial automorphism. This shows that

$$f_\sigma({}^\sigma(\pi(x))) = \psi(\sigma)\pi(f_\sigma({}^\sigma x)) = \psi(\sigma)\pi(u_\sigma \cdot x + v_\sigma \cdot \pi(x)) = \psi(\sigma)^\tau u_\sigma \cdot \pi(x).$$

Switching u_σ and $\psi(\sigma)^\tau u_\sigma$ for ease of notation and reducing modulo ± 1 and then modulo $\mathfrak{p}$, we finally obtain that

$$\bar{\varrho}_{Q_\ell,\mathfrak{p}}(\sigma) = \begin{pmatrix} \psi(\sigma)u_\sigma^p & 0 \\ v_\sigma & u_\sigma \end{pmatrix} \mod \pm 1.$$

We deduce that $\alpha_{Q_\ell,\mathfrak{p}}(\sigma) = u_\sigma \mod \pm 1$, so the lemma follows. □

Notice that the proof of this lemma recovers Proposition 4.28 (a), since the restrictions of $\tilde{\varrho}_{Q_\ell,\mathfrak{p}}$ and $\tilde{\alpha}_{Q_\ell,\mathfrak{p}}$ to G_{K_ℓ} coincide with $\varrho_{(A_\ell,i_\ell),\mathfrak{p}}$ and $\alpha_{(A_\ell,i_\ell),\mathfrak{p}}$, respectively. We can thus rewrite Proposition 4.28 (a) by saying that, in a suitable $\mathbb{F}_{p^2}$-basis of $A_\ell[\mathfrak{p}]$:

$$\begin{array}{rccc} \bar{\varrho}_{(A_\ell,i_\ell),\mathfrak{p}} : & G_{K_\ell} & \longrightarrow & \mathrm{GL}_2(\mathbb{F}_{p^2}) \\ & \sigma & \longmapsto & \begin{pmatrix} \tilde{\alpha}_{Q_\ell,\mathfrak{p}}(\sigma)^p & 0 \\ * & \tilde{\alpha}_{Q_\ell,\mathfrak{p}}(\sigma) \end{pmatrix}. \end{array}$$

Let now $\sigma_\ell \in G_{\mathbb{Q}_\ell}$ be a Frobenius element at ℓ, i.e. whose reduction coincides with the Frobenius automorphism $\mathrm{Fr}_\ell \in \mathrm{Gal}\,(\bar{\mathbb{F}}_\ell/\mathbb{F}_\ell)$.

COROLLARY 4.32. *If $\ell \neq p$ and $\sigma_\ell \in G_{K_\ell}$, then the characteristic polynomial $\Phi_\ell(T) \in R_m[T]$ of $\varrho_{(A_\ell,i_\ell),\mathfrak{p}}(\sigma_\ell)$ satisfies the congruence*

$$\Phi_\ell(T) \equiv T^2 - (\tilde{\alpha}_{Q_\ell,\mathfrak{p}}(\sigma_\ell) + \ell\tilde{\alpha}_{Q_\ell,\mathfrak{p}}(\sigma_\ell)^{-1})T + \ell \mod \mathfrak{p}.$$

PROOF. If $\sigma_\ell \in G_{K_\ell}$, by the above observation $\Phi_\ell(T)$ satisfies the congruence

$$\Phi_\ell(T) \bmod \mathfrak{p} \equiv T^2 - (\tilde{\alpha}_{Q_\ell,\mathfrak{p}}(\sigma_\ell) + \tilde{\alpha}_{Q_\ell,\mathfrak{p}}(\sigma_\ell)^p)T + N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\tilde{\alpha}_{Q_\ell,\mathfrak{p}}(\sigma_\ell)).$$

Also, from Proposition 4.28 (c), $\det(\bar{\varrho}_{(A_\ell,i_\ell),\mathfrak{p}}(\sigma_\ell)) = \ell$, so we can write

$$\tilde{\alpha}_{Q_\ell,\mathfrak{p}}(\sigma_\ell)^p \tilde{\alpha}_{Q_\ell,\mathfrak{p}}(\sigma_\ell) = \ell \in \mathbb{F}_{p^2}^\times,$$

and therefore the lemma follows noting that

$$\tilde{\alpha}_{Q_\ell,\mathfrak{p}}(\sigma_\ell) + \tilde{\alpha}_{Q_\ell,\mathfrak{p}}(\sigma_\ell)^p \equiv \tilde{\alpha}_{Q_\ell,\mathfrak{p}}(\sigma_\ell) + \ell\tilde{\alpha}_{Q_\ell,\mathfrak{p}}(\sigma_\ell)^{-1} \mod \mathfrak{p}.$$

□

REMARK 4.33. We have already seen that, for every prime $\ell \neq p$, the character $\alpha^{12}_{Q_\ell,\mathfrak{p}}$ is unramified. We now make an observation for the case $\ell = p$. First, recall that the local Artin reciprocity map gives us an isomorphism

$$w_p : \mathbb{Z}_p^\times \xrightarrow{\simeq} I_p^{ab} \subseteq G_{\mathbb{Q}_p}^{ab},$$

where I_p^{ab} denotes the inertia subgroup of $G_{\mathbb{Q}_p}^{ab}$. Also, since the character $\alpha_{Q_p,\mathfrak{p}}$ takes values on an abelian group, it factors through the quotient $G_{\mathbb{Q}_p}^{ab} := \mathrm{Gal}\,(\mathbb{Q}_p^{ab}/\mathbb{Q}_p)$ of $G_{\mathbb{Q}_p}$, hence we can write

$$\alpha_{Q_p,\mathfrak{p}} : G_{\mathbb{Q}_p}^{ab} \longrightarrow \mathbb{F}_{p^2}^\times/\{\pm 1\}.$$

Therefore, we can consider the composition

$$\alpha_{Q_p,\mathfrak{p}} \circ w_p : \mathbb{Z}_p^\times \underset{\simeq}{\xrightarrow{w_p}} I_p^{ab} \subseteq G_{\mathbb{Q}_p}^{ab} \xrightarrow{\alpha_{Q_p,\mathfrak{p}}} \mathbb{F}_{p^2}^\times/\{\pm 1\},$$

which is a continuous homomorphism. The image of

$$\mathbb{Z}_p^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$$

under $\alpha_{Q_p,\mathfrak{p}} \circ w_p$ is then a cyclic subgroup of $\mathbb{F}_{p^2}^\times/\{\pm 1\}$, but since $\alpha_{Q_p,\mathfrak{p}} \circ w_p$ must be trivial on the pro-p-part, $\alpha_{Q_p,\mathfrak{p}} \circ w_p(\mathbb{Z}_p^\times)$ is indeed a cyclic subgroup of

$$\mathbb{Z}/\frac{p-1}{2}\mathbb{Z} \simeq \mathbb{F}_p^\times/\{\pm 1\},$$

which we identify with the unique subgroup of index 2 of $\mathbb{Z}/(p-1)\mathbb{Z}$. Therefore, for any $x \in \mathbb{Z}_p^\times$, it holds

$$\alpha_{Q_p,\mathfrak{p}}(w_p(x))^2 = \alpha_{Q_p,\mathfrak{p}}(w_p(x^2)) \in \mathbb{F}_p^\times/\{\pm 1\}.$$

If we take any representative $\tau \in I_p$ of $w_p(x) \in I_p^{ab}$, this implies that $\alpha_{Q_p,\mathfrak{p}}(\tau^2) \in \mathbb{F}_p^\times/\{\pm 1\}$. As a consequence,

$$\tilde{\alpha}_{Q_p,\mathfrak{p}}(\tau^2) \in \mathbb{F}_p^\times \quad \text{for any } \tau \in I_p \subseteq G_{\mathbb{Q}_p}.$$

CHAPTER 5

Rational points on Shimura curves via Galois representations

The goal of this chapter is to combine the study of Galois representations over fields of moduli attached to points on Shimura curves from Chapter 4 together with the étale coverings analysed in Chapter 2. As a result, we provide sufficient conditions for the non-existence of rational points on Shimura curves over imaginary quadratic fields and for the non-existence of rational points on Atkin-Lehner quotients of Shimura curves.

As usual, let X_D be the Shimura curve defined by an indefinite rational quaternion algebra B_D of reduced discriminant D. If k is a field of characteristic zero, a k-rational point P on X_D corresponds to the isomorphism class of a QM-abelian surface $(A,\iota)/\bar{k}$ which is isomorphic to all its $\mathrm{Gal}\,(\bar{k}/k)$-conjugates. However, the pair $(A,\iota)/\bar{k}$ does not necessarily admit a model rational over k, because the moduli problem associated to X_D is not fine. As we have seen in the previous chapter, this issue was studied by Jordan, who proved that (A,ι) admits a model over k if and only if k splits B_D.

Assuming this condition for an imaginary quadratic field $K/\mathbb{Q}$, Jordan gave sufficient conditions for the emptiness of $X_D(K)$ or, in other words, for the non-existence of abelian surfaces with multiplication by $\mathcal{O}_D$ defined over K (cf. [**Jor86**, Theorem 6.3]). However, there is no reason to expect the hypothesis that K splits B to be correlated with the failure of X_D to admit points over K, and in fact standard conjectures predict that $X_D(K)$ should be empty when both D and $\mathrm{disc}(K)$ are large enough.

The first main result of this chapter provides sufficient conditions for the set $X_D(K)$ to be empty, without assuming that hypothesis. The method of our proof pushes the original one of Jordan, as strengthened by Skorobogatov in [**Sko05**] in order to prove that the non-existence of points in $X_D(K)$ is actually accounted for by the Brauer-Manin obstruction. The novelty in our setting is that a pair $(A,\iota)/\bar{K}$ represented by a point $P \in X_D(K)$ may not admit a model over K, and we overcome this by attaching to P the Galois representations over K (its field of moduli) introduced in the previous chapter.

In order to precisely state this result, let us fix some notations. For a given rational prime q, let us define $\mathcal{P}_1(q)$ to be the (finite) set of all primes appearing as a factor of some non-zero integer in the set

$$\bigcup_{|a|\leq 2q}\bigcup_{s=0}^{4}\{a^2-sq^2, a^4-4a^2q^2+q^4\},$$

For $q\neq 2$, define also $\mathcal{B}_1(q)$ to be the set of indefinite rational quaternion algebras which are not split by $\mathbb{Q}(\sqrt{-q})$. Similarly, define $\mathcal{B}_1(2)$ as the set of indefinite rational quaternion algebras which are split by neither $\mathbb{Q}(\sqrt{-2})$ nor $\mathbb{Q}(\sqrt{-1})$.

We say that a point $P\in X_D(\bar{\mathbb{Q}})$ has CM (by an imaginary quadratic field K) if the abelian surfaces in the isomorphism class corresponding to P have complex multiplication (by K).

As in Chapter 1, we write $X_D(\mathbb{A}_K)^{\mathrm{Br}}$ for the Brauer set of X_D, that is, the subset of the set $X_D(\mathbb{A}_K)$ of adèlic points on $X_D\times_{\mathbb{Q}} K$ cut out by the Brauer-Manin conditions; recall that $X_D(\mathbb{A}_K)^{\mathrm{Br}}$ always contains the set of global points $X_D(K)$ and when $X_D(\mathbb{A}_K)^{\mathrm{Br}}=\emptyset$ one says that the emptiness of $X_D(K)$ is explained by the Brauer-Manin obstruction.

THEOREM 5.1. *Let K be an imaginary quadratic field in which a prime q is ramified. If $B_D \in \mathcal{B}_1(q)$ is such that D is divisible by a prime $p \notin \mathcal{P}_1(q)$, $p \geq 5$, and p is not split in K, then $X_D(K)$ consists only of CM-points.*

If in addition $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, then $X_D(K) = X_D(\mathbb{A}_K)^{\mathrm{Br}} = \emptyset$.

Similar techniques to those used in the proof of Theorem 5.1 should still be useful to tackle the questions addressed in this note over larger number fields, although we have made no attempt of generalisation in this direction.

Let us say that a pair (D, K) is *exceptional* if the imaginary quadratic field K fails to split B_D and $X_D(K_v) \neq \emptyset$ for every place v of K; this terminology was adopted by Jordan in [**Jor86**], and these are precisely the pairs for which the results in *ibid.* and [**Sko05**] do not apply. As pointed out in [**Jor86**, p. 93-94], if (D, K) is an exceptional pair, then either $D = 2p$ for some prime $p \equiv 1 \pmod 4$ or $D = 2q_1 \cdots q_{2r-1}$ with primes q_i satisfying $q_i \equiv 3 \pmod 4$, $1 \leq i \leq 2r-1$. Let us list in Table 1 below some examples of exceptional pairs (D, K) for which Theorem 5.1 applies to show that $X_D(K) = X_D(\mathbb{A}_K)^{\mathrm{Br}} = \emptyset$. In particular, for every pair (D, K) in the Table 1, X_D is a counterexample to the Hasse principle over K accounted for by the Brauer-Manin obstruction.

$D = 2 \cdot p$	$K = \mathbb{Q}(\sqrt{d})$
$2 \cdot 19$	$\mathbb{Q}(\sqrt{-39})$, $\mathbb{Q}(\sqrt{-87})$, $\mathbb{Q}(\sqrt{-111})$, $\mathbb{Q}(\sqrt{-159})$
$2 \cdot 29$	$\mathbb{Q}(\sqrt{-15})$, $\mathbb{Q}(\sqrt{-55})$, $\mathbb{Q}(\sqrt{-95})$, $\mathbb{Q}(\sqrt{-119})$
$2 \cdot 31$	$\mathbb{Q}(\sqrt{-39})$, $\mathbb{Q}(\sqrt{-87})$, $\mathbb{Q}(\sqrt{-111})$, $\mathbb{Q}(\sqrt{-159})$, $\mathbb{Q}(\sqrt{-183})$
$2 \cdot 37$	$\mathbb{Q}(\sqrt{-15})$, $\mathbb{Q}(\sqrt{-39})$, $\mathbb{Q}(\sqrt{-87})$, $\mathbb{Q}(\sqrt{-111})$, $\mathbb{Q}(\sqrt{-183})$
$2 \cdot 43$	$\mathbb{Q}(\sqrt{-15})$, $\mathbb{Q}(\sqrt{-87})$, $\mathbb{Q}(\sqrt{-95})$, $\mathbb{Q}(\sqrt{-111})$, $\mathbb{Q}(\sqrt{-183})$
$2 \cdot 47$	$\mathbb{Q}(\sqrt{-55})$, $\mathbb{Q}(\sqrt{-95})$
$2 \cdot 53$	$\mathbb{Q}(\sqrt{-39})$, $\mathbb{Q}(\sqrt{-55})$
$2 \cdot 59$	$\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-119})$
$2 \cdot 61$	$\mathbb{Q}(\sqrt{-55})$, $\mathbb{Q}(\sqrt{-87})$, $\mathbb{Q}(\sqrt{-111})$, $\mathbb{Q}(\sqrt{-159})$, $\mathbb{Q}(\sqrt{-183})$

TABLE 1. Some exceptional pairs (D, K) with $X_D(\mathbb{A}_K)^{\mathrm{Br}} = \emptyset$.

Let us now introduce the second main result of this chapter, which concerns the existence of rational points on the Atkin-Lehner quotients $X_D^{(m)}$ of a Shimura curve X_D. Although $X_D(\mathbb{Q}) = \emptyset$, thanks to a theorem of Shimura (cf. Theorem 1.40), one may ask whether the quotient of X_D by an Atkin-Lehner involution ω_m has rational points or not.

In [**RSY05**], Rotger, Skorobogatov and Yafaev established a criterion for the existence of local points on $X_D^{(m)}$ at every place of $\mathbb{Q}$, using previous work of Ogg. This allowed them to exhibit that $X_{23\cdot 107}^{(107)}$ is a counterexample to the Hasse principle over $\mathbb{Q}$.

On the other hand, Parent and Yafaev [**PY07**] have given a method to study global rational points on certain Atkin-Lehner quotients of Shimura curves. They study the case where $D = pm$ is the product of two odd primes with $p \equiv 1 \bmod 4$ and $m \equiv 3 \bmod 4$, which corresponds to the "non-ramifié" case in the terminology of Ogg (see [**Ogg85**]). In [**PY07**], explicit conditions for rational points on these quotients to be "trivial" (arising from CM-points) are given, and they also find an infinite family of such quotients satisfying them. This work has recently been taken a step further by Gillibert in [**Gil13**], where Parent-Yafaev conditions are made explicit.

As in Theorem 5.1, we will exploit the moduli interpretation of $X_D^{(m)}$ as the classifying space of abelian surfaces with real multiplication by $\mathbb{Q}(\sqrt{m})$ whose endomorphism algebras contain the maximal order $\mathcal{O}_D$ (cf. Proposition 1.46 below for more details) and the Galois representations of $\mathrm{Gal}\,(\bar{\mathbb{Q}}/\mathbb{Q})$ with values in $\mathrm{GL}_2(\mathbb{Q}(\sqrt{m}) \otimes \mathbb{Q}_p)/\{\pm 1\}$ that we can attach to these abelian surfaces, in the same fashion as in Chapter 4.

As a result, we are able to prove the following statement. For a given rational prime q we now define $\mathcal{P}_2(q)$ to be the set of all primes appearing as a factor of some non-zero integer in the set

$$\bigcup_{|a|\leq 2\sqrt{q}} \bigcup_{s=0}^{4} \{a^2 - sq, a^4 - 4a^2q + q^2\},$$

If $\mathcal{Q} = \mathcal{Q}_{\mathbb{Q}}$ denotes the set of indefinite rational quaternion algebras, define

$$\mathcal{B}_2(q) := \left\{ B \in \mathcal{Q} \;\middle|\; \begin{array}{l} B \in \mathcal{B}_1(q) \text{ and } q \text{ is not inert in any imaginary} \\ \text{quadratic field } K \text{ such that } \underline{\text{disc}}(K) | \operatorname{disc}(B) \end{array} \right\} \subset \mathcal{Q},$$

where $\underline{\text{disc}}(K)$ is the (square-free) product of the primes ramifying in K.

THEOREM 5.2. *Let B_D be an indefinite quaternion algebra of odd discriminant $D = pm$, with $p \geq 7$ a prime such that $p \equiv 3 \mod 4$. If there is a prime q such that $B_D \in \mathcal{B}_2(q)$ and $p \notin \mathcal{P}_2(q)$, then $X_D^{(m)}(\mathbb{Q}) = \emptyset$.*

Using the criterion given in [**RSY05**, Theorem 3.1] we can check whether a pair (p, m) satisfying the hypotheses of Theorem 5.2 gives rise to a curve $X_D^{(m)}$ which has points everywhere locally and thus violates the Hasse principle over $\mathbb{Q}$; Table 2 below lists some of such pairs (p, m).

Some pairs (p, m) such that $X_{pm}^{(m)}$ violates the Hasse principle over $\mathbb{Q}$.
(23, 17), (31, 17), (31, 29), (31, 37), (31, 53), (31, 61), (47, 13), (47, 41), (59, 13), (71, 13), (71, 17), (79, 17), (83, 5), (83, 13), (103, 5), (107, 5), (107, 17), (127, 5), (151, 13), (167, 5), (223, 5), (227, 5), (263, 5), (283, 5), (307, 5), (347, 5), (367, 5), (383, 5)

TABLE 2.

As opposite to the approach taken in [**PY07**] and [**Gil13**], observe that if we consider discriminants of the form $D = pm$ with p, m different odd primes, the conditions on the above theorem place us in Ogg's "ramifié" case (see [**Ogg85**]). Therefore, our results are complementary to those in [**PY07**] and [**Gil13**].

In addition to the ideas mentioned above, our proof of Theorem 5.2 also borrows the descent techniques from [**Sko05**] together with some ideas from [**Rot08**].

1. Proof of Theorem 5.1

Let $\mathcal{O}_D$ be a maximal order in an indefinite rational quaternion algebra B_D of reduced discriminant D, and let X_D be the associated Shimura curve. Fix an odd prime p dividing D and consider the cyclic Galois covering $X_{D,p} \to X_D$ from Chapter 2, whose moduli interpretation has been described in Section 6 of Chapter 2.

Recall that the Shimura curve $X_{D,p}/\mathbb{Q}$ is not geometrically connected: its $p-1$ geometric connected components are only defined over the p-th cyclotomic field $\mathbb{Q}(\mu_p)$, and conjugated by the action of $\operatorname{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ (cf. Chapter 2). Moreover, the automorphism group $\Delta = \operatorname{Aut}(X_{D,p}/X_D)$ of this covering is cyclic of order $(p^2-1)/2$, and its maximal étale quotient (the *Shimura covering of X_D at p*) arises as the quotient of $X_{D,p}$ by the action of the unique (cyclic) subgroup of Δ of order $e = e(D)$. In particular, following the notations of Chapter 2, the covering

$$g_{(p^2-1)/12} : Y_{(p^2-1)/12} \longrightarrow X_D$$

is étale and cyclic of degree $(p^2-1)/12$. For simplicity, we define $Y_{D,p} := Y_{(p^2-1)/12}$ and write this covering by

$$g_p : Y_{D,p} \longrightarrow X_D.$$

This way, $Y_{D,p}$ is an X_D-torsor under the constant group scheme $\mathbb{F}_{p^2}^{\times 12} \simeq \mathbb{Z}/\frac{p^2-1}{12}\mathbb{Z}$ (cf. [**Sko05**, Corollary 1.2]). Therefore, if k is a field of characteristic zero, each k-rational point $P \in X_D(k)$ gives rise by specialisation of $Y_{D,p}$ to a continuous character

$$\phi_P : G_k \longrightarrow \mathbb{F}_{p^2}^{\times 12},$$

by which the Galois group G_k acts on the fibre of $g_p : Y_{D,p} \to X_D$ at P. That is to say, for every $\sigma \in G_k$, $\phi_P(\sigma)$ is the uniquely determined automorphism in $\mathrm{Aut}(Y_{D,p}/X_D) \simeq \mathbb{F}_{p^2}^{\times 12}$ such that

$${}^{\sigma}P = \phi_P(\sigma)(P).$$

Assume for example that $K/\mathbb{Q}$ is an imaginary quadratic field, let v be a place of K over a prime ℓ and let (A_v, ι_v) be a pair corresponding to a K_v-point $P_v \in X_D(K_v)$. Assuming that K splits B_D, K_v also splits B_D, so that (A_v, ι_v) admits a model rational over K_v by Theorem 4.20. Then, by the modular interpretation of the Galois covering $X_{D,p} \to X_D$, the canonical isogeny character

$$\alpha_{(A_v,\iota_v)} : G_{K_v} \longrightarrow \mathrm{Aut}_{\mathcal{O}_D}(C_p) \simeq \mathbb{F}_{p^2}^{\times}$$

at p satisfies $\phi_{P_v} = \alpha_{(A_v,\iota_v)}^{12}$ (see [**Sko05**, Lemma 2.1]). Exploiting this relation and performing descent to the torsor $g_p : Y_{D,p} \to X_D$, Skorobogatov proved in [**Sko05**, Theorem 3.1] the following result, which strengthens [**Jor86**, Theorem 6.3]. Here, $\mathcal{P}_1'(q)$ is a finite set of primes depending on q, defined in a similar way to $\mathcal{P}_1(q)$ (see [**Sko05**] for details):

THEOREM 5.3 (Skorobogatov). *Let K be an imaginary quadratic field in which a prime q is ramified, and let B_D be a quaternion algebra in $\mathcal{B}_1(q)$ whose discriminant is divisible by a prime $p \notin \mathcal{P}_1'(q)$, $p \geq 5$, and which is split by K. Then $X_D(\mathbb{A}_K)^{\mathrm{Br}} = \emptyset$.*

Now assume that K does not necessarily splits B_D, and construct an extension L_w/K_v as in the previous section, over which the pair (A_v, ι_v) corresponding to P_v admits a rational model. We can assume that (A_v, ι_v) is defined over L_w. Then, again because of the modular interpretation of $X_{D,p} \to X_D$ we have that $\phi_{P_v|G_{L_w}} = \alpha_{(A_v,\iota_v)}^{12}$, where now

$$\alpha_{(A_v,\iota_v)} : G_{L_w} \longrightarrow \mathrm{Aut}_{\mathcal{O}_D}(C_p) \simeq \mathbb{F}_{p^2}^{\times}.$$

In order to avoid restricting to G_{L_w}, we can use the character

$$\alpha_{P_v} : G_{K_v} \longrightarrow \mathbb{F}_{p^2}^{\times}/\{\pm 1\}$$

attached to the point P_v obtained by the method explained in the previous chapter. As before, we shall write $\tilde{\alpha}_{P_v} : G_{K_v} \to \mathbb{F}_{p^2}^{\times}$ for a lift of α_{P_v} (which is not a homomorphism in general).

LEMMA 5.4. *For any $\sigma \in G_{K_v}$, $\tilde{\alpha}_{P_v}(\sigma)^{24} = \phi_{P_v}(\sigma)^2$. In terms of α_{P_v}, we have*

$$\alpha_{P_v}(\sigma)^{12} = \phi_{P_v}(\sigma) \mod \pm 1, \quad \textit{for all } \sigma \in G_{K_v}.$$

PROOF. Since $\tilde{\alpha}_{P_v}$ restricted to G_{L_w} coincides with $\alpha_{(A_v,\iota_v)}$, we can write $(\tilde{\alpha}_{P_v|G_{L_w}})^{12} = \phi_{P_v|G_{L_w}}$. Therefore, if $\sigma \in G_{K_v}$ then

$$\tilde{\alpha}_{P_v}(\sigma)^{24} = (\pm\tilde{\alpha}_{P_v}(\sigma^2))^{12} = (\tilde{\alpha}_{P_v|G_{L_w}}(\sigma^2))^{12} = \phi_{P_v|G_{L_w}}(\sigma^2) = \phi_{P_v}(\sigma)^2,$$

so the lemma follows. □

Together with Corollary 4.24, we obtain:

COROLLARY 5.5. *For $p \neq \ell$, $\phi_{P_v}^2$ is unramified.*

We are now in position to prove Theorem 5.1, which follows clearly from Theorem 5.6 and Corollary 5.10 below. The finite set of primes $\mathcal{P}_1(q)$ and the set of indefinite algebras $\mathcal{B}_1(q)$ associated to a prime q were defined at the beginning of the chapter.

THEOREM 5.6. *Let K be an imaginary quadratic field in which a prime q is ramified. If $B_D \in \mathcal{B}_1(q)$ is such that D is divisible by a prime $p \notin \mathcal{P}_1(q)$, $p \geq 5$, and p is not split in K then $X_D(K)$ consists only of CM-points.*

PROOF. Let $p \notin \mathcal{P}_1(q)$, $p \geq 5$, be a prime factor of D such that p is not split in K, and let $\mathfrak{p}$ be the unique prime of K above p. Let also $K'/\mathbb{Q}$ be a quadratic extension splitting the algebra B_D and such that q is not inert in K'. If $D = p_1 \cdots p_{2r}$, the existence of such a K' reduces to the existence of a discriminant d such that $(\frac{d}{p_i}) \neq 1$, $i = 1, \ldots, 2r$ and $(\frac{d}{q}) \neq -1$. By Čebotarev's Density Theorem, there are infinitely many such d.

Assume that $P \in X_D(K)$ is a K-rational point which does not have complex multiplication by $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$. By the modular interpretation of X_D, we can choose an abelian surface $(A, \iota)/\bar{K}$, with multiplication by $\mathcal{O}_D$ whose field of moduli is K. By means of the diagonal embedding $X_D(K) \hookrightarrow X_D(\mathbb{A}_K)$, the point P defines a sequence of local points $\{P_v\}_v \in X_D(\mathbb{A}_K)$. For each one of these points, say $P_v \in X_D(K_v)$, we can choose the same abelian surface (A, ι) representing it, now regarded as an abelian surface over $\bar{K}_v$. However, let v' be a place of K' above the same rational prime ℓ lying below v and, with the same notations as before, consider the composite field $L_w := K_v \cdot K'_{v'}$. Then, since $K'_{v'}$ splits B_D, we can choose a model (A_v, ι_v) of $(A, \iota)/\bar{K}_v$ rational over L_w. In particular, $P_v = [(A_v, \iota_v)]$. Note that (A_v, ι_v) has complex multiplication by neither $\mathbb{Q}(\sqrt{-1})$ nor $\mathbb{Q}(\sqrt{-3})$.

The global character

$$\phi : G_K \longrightarrow \mathbb{F}_{p^2}^{\times 12}$$

obtained by specialisation of the torsor g_p at P restricts to each one of the local characters ϕ_{P_v} attached to each point P_v on G_{K_v}. By Corollary 5.5 we have that ϕ^2 is unramified away from $\mathfrak{p}$. Moreover, the restriction of ϕ_{P_v} to G_{L_w} coincides with the Galois representation $\alpha^{12}_{(A_v,\iota_v)}$.

On the other hand, let $\mathfrak{q}$ be the unique prime of K above q, and let $\sigma_\mathfrak{q} \in G_{K_\mathfrak{q}}$ be a Frobenius element at $\mathfrak{q}$, i.e. an element inducing the Frobenius automorphism $\mathrm{Fr}_q \in \mathrm{Gal}\,(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ under reduction. We claim that

$$\tilde{\alpha}_{P_\mathfrak{q}}(\sigma_\mathfrak{q}^2)^{24} = q^{24} \quad \text{in} \quad \mathbb{F}_{p^2}^\times,$$

where $\alpha_{P_\mathfrak{q}} : G_{K_\mathfrak{q}} \to \mathbb{F}_{p^2}^\times/\{\pm 1\}$ is the Galois representation associated to $P_\mathfrak{q} = [(A_\mathfrak{q}, \iota_\mathfrak{q})] \in X_D(K_\mathfrak{q})$ over its field of moduli, arising from the action of $G_{K_\mathfrak{q}}$ on the canonical torsion subgroup of $A_\mathfrak{q}[p]$, and $\tilde{\alpha}_{P_\mathfrak{q}} : G_{K_\mathfrak{q}} \to \mathbb{F}_{p^2}^\times$ is a lift of it as usual.

By global class field theory, we have an exact sequence

$$\prod_v U_v \longrightarrow G_K^{ab} \longrightarrow \mathrm{Cl}(K) \longrightarrow 0,$$

where U_v is the group of units of the ring of integers of K_v and $U_v \to G_K^{ab}$ is defined by the local Artin map w_v. The idèle in $\prod_v U_v$ all of whose components equal $1/q$ except the component at $\mathfrak{q}$ which equals π^2/q, with π a uniformiser at $\mathfrak{q}$, maps to $\mathrm{Frob}_\mathfrak{q}^2$, the square of a Frobenius element $\mathrm{Frob}_\mathfrak{q} \in G_K^{ab}$ at $\mathfrak{q}$. Then,

$$\sigma_\mathfrak{q}^2 \circ \mathrm{Frob}_\mathfrak{q}^{-2} \in I_\mathfrak{q},$$

where $I_\mathfrak{q} \subseteq G_{K_\mathfrak{q}}$ denotes the inertia subgroup, and since ϕ^2 is unramified away from $\mathfrak{p}$ we deduce that $\phi^2(\sigma_\mathfrak{q}^2) = \phi^2(\mathrm{Frob}_\mathfrak{q}^2)$. But now observe that

$$\phi^2(\sigma_\mathfrak{q}^2) = \phi^2_{P_\mathfrak{q}}(\sigma_\mathfrak{q}^2) = \tilde{\alpha}_{P_\mathfrak{q}}(\sigma_\mathfrak{q}^2)^{24}$$

and

$$\phi^2(\mathrm{Frob}_\mathfrak{q}^2) = \phi^2_{P_\mathfrak{p}}(w_\mathfrak{p}(q^{-1})) = \tilde{\alpha}_{P_\mathfrak{p}}(w_\mathfrak{p}(q^{-1}))^{24},$$

so that our claim is reduced to proving that $\tilde{\alpha}_{P_\mathfrak{p}}(w_\mathfrak{p}(q^{-1}))^{24} = q^{24}$. There are two cases:

(a) p is inert in K. In this case, the group of units $U_\mathfrak{p}$ is an extension of $\mathbb{F}_{p^2}^\times$ by a pro-p-group. The homomorphism

$$\alpha_{P_\mathfrak{p}} \circ w_\mathfrak{p} : U_\mathfrak{p} \longrightarrow I_\mathfrak{p}^{ab} \longrightarrow \mathbb{F}_{p^2}^\times/\{\pm 1\}$$

must be trivial on the pro-p-part, so that it factors through a homomorphism

$$\mu : \mathbb{F}_{p^2}^\times \longrightarrow \mathbb{F}_{p^2}^\times/\{\pm 1\}.$$

If $a \in \mathbb{F}_{p^2}^\times$ is a generator of the cyclic group $\mathbb{F}_{p^2}^\times$, then the class $[a]$ of a in $\mathbb{F}_{p^2}^\times/\{\pm 1\}$ is a generator of $\mathbb{F}_{p^2}^\times/\{\pm 1\}$ as well, so that the homomorphism μ is determined by an integer c (uniquely determined modulo $(p^2-1)/2$) such that $\mu(a) = [a]^{-c}$.

Then, if we denote by $\tilde{u} \in \mathbb{F}_{p^2}^\times$ the reduction modulo $\mathfrak{p}$ of $u \in U_\mathfrak{p}$, we have

$$\alpha_{P_\mathfrak{p}}(w_\mathfrak{p}(u)) = \mu(\tilde{u}) = [\tilde{u}]^{-c}.$$

In particular, $\tilde{\alpha}_{P_\mathfrak{p}}(w_\mathfrak{p}(u)) = \pm\tilde{u}^{-c}$.

Besides, from [**Ser72**, Prop. 3, 8] we have

$$\chi_p(w_\mathfrak{p}(u)) = N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\tilde{u})^{-1} \quad \text{for every } u \in U_\mathfrak{p}.$$

Thus, applying (4.3),

$$N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\tilde{\alpha}_{P_\mathfrak{p}}(w_\mathfrak{p}(u))^2) = \chi_p(w_\mathfrak{p}(u))^2 = N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\tilde{u})^{-2} = \tilde{u}^{-2(p+1)} \in \mathbb{F}_p^\times,$$

and we also have

$$N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\tilde{\alpha}_{P_\mathfrak{p}}(w_\mathfrak{p}(u))^2) = N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\tilde{u}^{-2c}) = \tilde{u}^{-2c(p+1)} \in \mathbb{F}_p^\times.$$

From this we get that $2c \equiv 2 \bmod p-1$. Therefore, $\tilde{\alpha}_{P_\mathfrak{p}}(w_\mathfrak{p}(q^{-1}))^{24} = q^{24}$ as claimed.

(b) p is ramified in K. In this case, $U_\mathfrak{p}$ is an extension of $\mathbb{F}_p^\times$ by a pro-p-group. Hence, the homomorphism

$$\alpha_{P_\mathfrak{p}} \circ w_\mathfrak{p} : U_\mathfrak{p} \longrightarrow I_\mathfrak{p}^{ab} \longrightarrow \mathbb{F}_{p^2}^\times/\{\pm 1\}$$

factors now through a homomorphism

$$\mu : \mathbb{F}_p^\times \longrightarrow \mathbb{F}_{p^2}^\times/\{\pm 1\}.$$

Then, $\alpha_{P_\mathfrak{p}}(w_\mathfrak{p}(U_\mathfrak{p}))$ must be contained in the unique cyclic subgroup of order $p-1$ of $\mathbb{F}_{p^2}^\times/\{\pm 1\}$. In particular, for every $u \in U_\mathfrak{p}$, $\alpha_{P_\mathfrak{p}}(w_\mathfrak{p}(u))^2$ lies in $\mathbb{F}_p^\times/\{\pm 1\} \subseteq \mathbb{F}_{p^2}^\times/\{\pm 1\}$, which is the unique subgroup of order $(p-1)/2$ of $\mathbb{F}_{p^2}^\times/\{\pm 1\}$.

So, if we denote again by $\tilde{u} \in \mathbb{F}_p^\times$ the reduction of u modulo $\mathfrak{p}$, there exists an integer c, uniquely determined modulo $(p-1)/2$ such that

$$\alpha_{P_\mathfrak{p}}(w_\mathfrak{p}(u))^2 = [\tilde{u}]^{-c},$$

where $[\tilde{u}]$ denotes the class of $\tilde{u}$ in $\mathbb{F}_p^\times/\{\pm 1\}$. In particular, $\tilde{\alpha}_{P_\mathfrak{p}}(w_\mathfrak{p}(u))^2 = \pm\tilde{u}^{-c}$.

Now, [**Ser72**, Prop. 3, 8] implies that

$$\chi_p(w_\mathfrak{p}(u)) = N_{\mathbb{F}_p/\mathbb{F}_p}(\tilde{u})^{-2} = \tilde{u}^{-2},$$

so that applying (4.3) we get

$$N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\tilde{\alpha}_{P_\mathfrak{p}}(w_\mathfrak{p}(u))^2) = \chi_p(w_\mathfrak{p}(u))^2 = \tilde{u}^{-4}.$$

Furthermore,

$$N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\tilde{\alpha}_{P_\mathfrak{p}}(w_\mathfrak{p}(u))^2) = (\pm\tilde{u}^{-c})^2 = \tilde{u}^{-2c},$$

since $\tilde{\alpha}_{P_\mathfrak{p}}(w_\mathfrak{p}(u))^2 \in \mathbb{F}_p^\times$. Hence, $2c \equiv 4 \bmod p-1$. We deduce that

$$\tilde{\alpha}_{P_\mathfrak{p}}(w_\mathfrak{p}(q^{-1}))^{24} = q^{24} \in \mathbb{F}_p^\times,$$

and the claim also follows in this case.

Now, since q is not inert in K', if $\mathfrak{q}'$ is a prime of K' above q, the residue field of $K'_{\mathfrak{q}'}$ is $\mathbb{F}_q$. As a consequence, also the residue field of $L_\mathfrak{Q} = K_\mathfrak{q} \cdot K'_{\mathfrak{q}'}$ is $\mathbb{F}_q$.

Then, since $A_\mathfrak{q}/L_\mathfrak{Q}$ has potential good reduction, following the construction of Serre and Tate [**ST68**, p. 498] we get an abelian surface $\tilde{A}_\mathfrak{q}$ defined over $\mathbb{F}_q$ such that the quaternion algebra $B_D \subseteq \mathrm{End}^0_{L_\mathfrak{q}}(A_\mathfrak{q})$ embeds in $\mathrm{End}^0_{\mathbb{F}_q}(\tilde{A}_\mathfrak{q})$. Moreover, $\sigma_\mathfrak{q} \in G_{L_\mathfrak{Q}}$, and its action on the Tate modules $T_p(A_\mathfrak{q})$ and $T_p(\tilde{A}_\mathfrak{q})$ is the same.

As in [**Jor86**, §5], the trace of $\bar{\varrho}_{(A_\mathfrak{q},\iota_\mathfrak{q})}(\sigma_\mathfrak{q}^n)$ is the reduction modulo p of an integer $a_{\mathfrak{q},n}$, $|a_{\mathfrak{q},n}| \leq 2q^{n/2}$, such that

$$a_{\mathfrak{q},n} \bmod p = \mathrm{Tr}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\alpha_{(A_\mathfrak{q},\iota_\mathfrak{q})}(\sigma_\mathfrak{q}^n)) = \alpha_{(A_\mathfrak{q},\iota_\mathfrak{q})}(\sigma_\mathfrak{q}^n) + q^n\alpha_{(A_\mathfrak{q},\iota_\mathfrak{q})}(\sigma_\mathfrak{q}^n)^{-1}.$$

In particular, if $a_{\mathfrak{q}} := a_{\mathfrak{q},2}$ then

$$a_{\mathfrak{q}} \bmod p = \alpha_{(A_{\mathfrak{q}},\iota_{\mathfrak{q}})}(\sigma_{\mathfrak{q}}^2) + q^2\alpha_{(A_{\mathfrak{q}},\iota_{\mathfrak{q}})}(\sigma_{\mathfrak{q}}^2)^{-1}.$$

Since $\alpha_{(A_{\mathfrak{q}},\iota_{\mathfrak{q}})} = \tilde{\alpha}_{P_{\mathfrak{q}}|G_{L_\Omega}}$ and $\sigma_{\mathfrak{q}} \in G_{L_\Omega}$, using the claim proved above we can write

$$a_{\mathfrak{q}} \bmod p = \tilde{\alpha}_{P_{\mathfrak{q}}}(\sigma_{\mathfrak{q}}^2) + q^2\tilde{\alpha}_{P_{\mathfrak{q}}}(\sigma_{\mathfrak{q}}^2)^{-1} = q(\zeta + \zeta^{-1}),$$

where $\zeta = \frac{\tilde{\alpha}_{P_{\mathfrak{p}}}(\sigma_{\mathfrak{q}}^2)}{q}$ is a 24-th root of unity. Computing the possible values of $q(\zeta + \zeta^{-1})$ we get that either $a_{\mathfrak{q}} \mod p = 0$ or p divides

$$a_{\mathfrak{q}} \pm q, a_{\mathfrak{q}}^2 - 2q^2, a_{\mathfrak{q}}^2 - 3q^2, a_{\mathfrak{q}} \pm 2q, \text{ or } a_{\mathfrak{q}}^4 - 4a_{\mathfrak{q}}^2q^2 + q^4.$$

Since $|a_{\mathfrak{q}}| \leq 2q$, the hypothesis $p \notin \mathcal{P}_1(q)$ implies that actually

$$a_{\mathfrak{q}} = 0, \pm q, \pm\sqrt{2}q, \pm\sqrt{3}q, \pm 2q, \text{ or } \pm q\sqrt{2 \pm \sqrt{3}}.$$

But, since $a_{\mathfrak{q}}$ is an integer, the only possibilities are $a_{\mathfrak{q}} = 0, \pm q$, or $\pm 2q$. Now, if we let ξ be a 48-th root of unity such that $\xi^2 = \zeta$, the trace of the characteristic polynomial of $\bar{\varrho}_{(A_{\mathfrak{q}},\iota_{\mathfrak{q}})}(\sigma_{\mathfrak{q}})$ is the reduction modulo p of an integer $b_{\mathfrak{q}} := a_{\mathfrak{q},1}$ of absolute value at most $2\sqrt{q}$ with $b_{\mathfrak{q}} \bmod p = \sqrt{q}(\xi + \xi^{-1})$. Applying the Honda-Tate theory (see [**Jor86**, Theorem 2.1]) for both cases, we get the following list of possibilities:

$a_{\mathfrak{q}} = 0$, $q = 2$: then $\mathbb{Q}(\sqrt{-1})$ splits B_D;
$a_{\mathfrak{q}} = q = 3$: then $\mathbb{Q}(\sqrt{-3})$ splits B_D;
$a_{\mathfrak{q}} = -2q$: then $\mathbb{Q}(\sqrt{-q})$ splits B_D.

In any case, we obtain a contradiction with the assumption that $B_D \in \mathcal{B}_1(q)$, hence the statement follows. □

Directly from the above proof, we see that for a pair (B_D, K) satisfying the hypotheses of Theorem 5.6, $X_D(K)$ contains only points with CM by either $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$. Thus, in order to give sufficient conditions for the emptiness of $X_D(K)$, it remains to study the sets

$$X_D(K) \cap \mathrm{CM}(\mathbb{Q}(\sqrt{-1})) \quad \text{and} \quad X_D(K) \cap \mathrm{CM}(\mathbb{Q}(\sqrt{-3})).$$

Here, for an imaginary quadratic field L, $\mathrm{CM}(L)$ denotes the union of the sets $\mathrm{CM}(R) \subseteq X_D(\bar{\mathbb{Q}})$, where R ranges through the quadratic orders in L (cf. Section 3.5 of Chapter 1).

The existence of CM-points on Shimura curves and their fields of definition are well characterised and described. For the sake of completeness, we study in detail the sets $X_D(K) \cap \mathrm{CM}(\mathbb{Q}(\sqrt{-1}))$ and $X_D(K) \cap \mathrm{CM}(\mathbb{Q}(\sqrt{-3}))$ in the next two lemmas, using the results and notations from Section 3.5 of Chapter 1.

LEMMA 5.7. *Assume that (D, K) satisfies the hypotheses of Theorem 5.1. If $P \in X_D(K)$ has CM by $\mathbb{Q}(\sqrt{-1})$, then $K = \mathbb{Q}(\sqrt{-1})$ and $P \in \mathrm{CM}(R_i)$ for some $i \in \{1, 2\}$, where $R_i \subseteq R_{\mathbb{Q}(\sqrt{-1})}$ denotes the unique order of conductor i in the ring of integers of $\mathbb{Q}(\sqrt{-1})$.*

PROOF. Let $P \in X_D(K)$. Since X_D has no rational points and K is imaginary quadratic, it follows that $\mathbb{Q}(P) = K$. Assume further that P has CM by $\mathbb{Q}(\sqrt{-1})$. Then we have $P \in \mathrm{CM}(R_f)$ for some $f \geq 1$, where R_f is the unique order of conductor f in $\mathbb{Q}(\sqrt{-1})$. By Theorem 1.50, we then know that $K \cdot \mathbb{Q}(\sqrt{-1}) = H_f$, where $H_f := H_{R_f}$ is the ring class field of R_f.

Suppose first that $K \neq \mathbb{Q}(\sqrt{-1})$. Therefore, $H_f = K \cdot \mathbb{Q}(\sqrt{-1})$ is a biquadratic extension, and then $h_f = [H_f : \mathbb{Q}(\sqrt{-1})] = 2$. Computing the class number h_f, the only values of f for which $h_f = 2$ are $f = 3, 4, 5$. Moreover, because of the assumption $\mathrm{CM}(R_f) \neq \emptyset$, we know by Proposition 1.48 that $D/D(R_f)$ divides $\mathrm{disc}(R_f)$. But, since $[H_f : K] = 2$, by Theorem 1.51 $D(R_f) = 1$, so that D divides $\mathrm{disc}(R_f) = -4f^2$. Therefore, the case $f = 4$ is ruled out since $\mathrm{disc}(R_4) = -2^6$. And for $f = 3, 5$, the only possible reduced discriminants are $D = 2 \cdot 3$ and $D = 2 \cdot 5$, respectively. But these discriminants do not fulfill the hypotheses of Theorem 5.1 for any choice of prime q: in the first case, the only prime factors of D are smaller than 5, and in the second case it is enough to observe that $5 \in \mathcal{P}_1(q)$ for every prime q.

Therefore, $K = \mathbb{Q}(\sqrt{-1})$. But then, $H_f = \mathbb{Q}(\sqrt{-1})$ as well. Computing the class number $h_f = [H_f : \mathbb{Q}(\sqrt{-1})]$, the only values of f for which $h_f = 1$ are $f = 1, 2$, hence the statement follows. □

LEMMA 5.8. *Assume that (D, K) satisfies the hypotheses of Theorem 5.1. If $P \in X_D(K)$ has CM by $\mathbb{Q}(\sqrt{-3})$, then $K = \mathbb{Q}(\sqrt{-3})$ and $P \in \mathrm{CM}(R_i)$ for some $i \in \{1, 2, 3\}$, where $R_i \subseteq R_{\mathbb{Q}(\sqrt{-3})}$ denotes the unique order of conductor i in the ring of integers of $\mathbb{Q}(\sqrt{-3})$.*

PROOF. Let $P \in X_D(K)$. Again, we have $\mathbb{Q}(P) = K$ because X_D has no rational points and K is imaginary quadratic. If we further assume that P has CM by $\mathbb{Q}(\sqrt{-3})$, then $P \in \mathrm{CM}(R_f)$ for some $f \geq 1$, where R_f stands for the unique order of conductor f in $\mathbb{Q}(\sqrt{-3})$. By Theorem 1.50, we have $K \cdot \mathbb{Q}(\sqrt{-3}) = H_f$, where $H_f = H_{R_f}$ is the ring class field of R_f.

Now start assuming that $K \neq \mathbb{Q}(\sqrt{-3})$. Therefore, $H_f = K \cdot \mathbb{Q}(\sqrt{-3})$ is a biquadratic extension and $h_f = [H_f : \mathbb{Q}(\sqrt{-3})] = 2$. The only values of f for which this holds are $f = 4, 5$ or 7. Moreover, because of the assumption $\mathrm{CM}(R_f) \neq \emptyset$, Proposition 1.48 implies that $D/D(R_f)$ divides $\mathrm{disc}(R_f)$. But it follows from Theorem 1.51 that $D(R_f) = 1$ because $[H_f : K] = 2$, hence D divides $\mathrm{disc}(R_f) = -3f^2$. Then, for $f = 4, 5, 7$, the only possible reduced discriminants are $D = 2 \cdot 3$, $D = 3 \cdot 5$ and $D = 3 \cdot 7$, respectively. Similarly as in the previous lemma, this contradicts the fact that (D, K) satisfies the hypotheses of Theorem 5.1, using that $5, 7 \in \mathcal{P}_1(q)$ for every prime q.

Therefore, $K = \mathbb{Q}(\sqrt{-3})$, which implies that $H_f = \mathbb{Q}(\sqrt{-3})$ as well. And the only values of f for which $h_f = [H_f : \mathbb{Q}(\sqrt{-3})] = 1$ are $f = 1, 2$ or 3, hence the statement follows. □

In view of Lemmas 5.7 and 5.8, it follows that if the set of CM-points $X_D(K) \cap \mathrm{CM}(\mathbb{Q}(\sqrt{-1}))$, respectively $X_D(K) \cap \mathrm{CM}(\mathbb{Q}(\sqrt{-3}))$, is non-empty, then $K = \mathbb{Q}(\sqrt{-1})$, respectively $K = \mathbb{Q}(\sqrt{-3})$. However, given a Shimura curve X_D it is easy to characterise the sets $X_D(\mathbb{Q}(\sqrt{-1})) \cap \mathrm{CM}(\mathbb{Q}(\sqrt{-1}))$ and $X_D(\mathbb{Q}(\sqrt{-3})) \cap \mathrm{CM}(\mathbb{Q}(\sqrt{-3}))$. Indeed, the next lemma is an immediate consequence of Proposition 1.48:

LEMMA 5.9. *Let X_D be the Shimura curve associated to an indefinite rational quaternion algebra of reduced discriminant D. Then:*

(i) *If R_f is an order in $\mathbb{Q}(\sqrt{-1})$ of conductor f, then $\mathrm{CM}(R_f) = \emptyset$ if and only if there exists a prime $\ell \mid D$ such that $\ell \nmid f$ and $\ell \equiv 1 \mod 4$.*
(ii) *If R_f is an order in $\mathbb{Q}(\sqrt{-3})$ of conductor f, then $\mathrm{CM}(R_f) = \emptyset$ if and only if there exists a prime $\ell \mid D$ such that $\ell \nmid f$ and $\ell \equiv 1 \mod 3$.*

Using these lemmas, the next corollary completes the proof of Theorem 5.1. It turns out that in all cases where we can prove that $X_D(K) = \emptyset$, this is accounted for by the Brauer-Manin obstruction.

COROLLARY 5.10. *Assume that the pair (B_D, K) satisfies the hypotheses of Theorem 5.1.*

(i) *If $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, then $X_D(K) = X_D(\mathbb{A}_K)^{\mathrm{Br}} = \emptyset$.*
(ii) *If $K = \mathbb{Q}(\sqrt{-1})$ and there exists a prime $\ell \equiv 1 \mod 4$ dividing D, then $X_D(K) = X_D(\mathbb{A}_K)^{\mathrm{Br}} = \emptyset$.*
(iii) *If $K = \mathbb{Q}(\sqrt{-3})$ and there exists a prime $\ell \equiv 1 \mod 3$ dividing D, then $X_D(K) = X_D(\mathbb{A}_K)^{\mathrm{Br}} = \emptyset$.*

PROOF. Theorem 5.6 together with Lemmas 5.7, 5.8 and 5.9 imply that $X_D(K)$ is empty in all the cases.

Now, assume that $X_D(\mathbb{A}_K) \neq \emptyset$, as otherwise there is nothing to prove. Suppose that there exists a sequence of local points $P_v \in X_D(K_v)$, one for each non-archimedean place v of K, and let

$$\phi_{P_v} : G_{K_v} \longrightarrow \mathbb{F}_{p^2}^{\times 12}$$

denote the local character given by specialisation of the torsor g_p at P_v. Assume that all these local characters are the restriction of a global character

$$\phi : G_K \longrightarrow \mathbb{F}_{p^2}^{\times 12}.$$

For each point P_v, we can choose a pair $(A_v, \iota_v)/\bar{K}_v$ with field of moduli K_v representing it, and then the proof of Theorem 5.1 applies verbatim to get a contradiction, showing that such a sequence of local points cannot exist. Therefore, the descent subset $X_D(\mathbb{A}_K)^{g_p}$ associated to the torsor g_p is empty, and applying the main theorem of descent theory of Colliot-Thélène and Sansuc (cf. Theorem 1.64, or [**Sko01**, Theorem 6.1.2]) the statement follows. □

Since the hypotheses of Corollary 5.10 are explicit and computable, we can produce pairs (B_D, K) such that K is deficient for X_D (i.e., such that $X_D(K) = \emptyset$), and for which the absence of K-rational points on X_D is explained by the Brauer-Manin obstruction. Using the work of Jordan and Livné in [**JL85**], we can even give explicit sufficient conditions for X_D to be in fact a counterexample to the Hasse principle over K. Let us recall first some notations from [**JL85**].

For an order R in an imaginary quadratic field L, let us set

$$S(R) := \frac{h(R)}{[R^\times : \mathbb{Z}^\times]} \prod_{\substack{q \mid D \\ q \text{ prime}}} \left(1 - \left\{\frac{R}{q}\right\}\right),$$

where $h(R)$ is the class number of R, and recall that for a rational prime q

$$\left\{\frac{R}{q}\right\} := \begin{cases} 1 & \text{if } q \mid \mathrm{cond}(R), \\ (\frac{L}{q}) & \text{otherwise,} \end{cases}$$

denotes the Eichler symbol. Note that $S(R) \neq 0$ if and only if the conductor of R is prime to D and L splits B_D. Then, define

$$\Sigma_\ell(D) = \frac{1}{2} \sum_{\substack{s \in \mathbb{Z} \\ s^2 < 4\ell}} \sum_R S(R), \tag{5.1}$$

where R runs through the set of orders in imaginary quadratic fields such that R contains the roots of $x^2 + sx + \ell$.

Corollary 5.11. *Let $g = g(X_D)$ be the genus of X_D. Under the hypotheses of Corollary 5.10, assume also that the following conditions hold:*

(i) *$\Sigma_\ell(D) \neq 0$ for every prime $\ell < 4g^2$, $\ell \nmid D$, ℓ not inert in K.*
(ii) *For every prime $\ell \mid D$ ramifying in K, either $\mathbb{Q}(\sqrt{-\ell})$ splits B_D or $\ell = 2$ and $\mathbb{Q}(\sqrt{-1})$ splits B_D.*
(iii) *For every prime $\ell \mid D$ splitting in K, either $D = 2\ell$ with $\ell \equiv 1 \mod 4$, or $\ell = 2$ and $D = 2q_1 \cdots q_{2r-1}$ with primes $q_i \equiv 3 \mod 4$ not splitting in K.*

Then X_D is a counterexample to the Hasse principle over K accounted for by the Brauer-Manin obstruction.

Proof. The statement follows directly from Corollary 5.10 and the work in [**JL85**], together with the fact that $X_D(\mathbb{Q}_\ell) \neq \emptyset$ for every prime $\ell > 4g^2$, by Weil's bound. □

Since all the conditions of this corollary are explicit and computable, we are able to obtain Shimura curves X_D violating the Hasse principle over imaginary quadratic fields K for which (B_D, K) is an exceptional pair: that is, $K = \mathbb{Q}(\sqrt{d})$ fails to split B_D. As far as we know, these counterexamples were not known before. Furthermore, all these counterexamples are accounted for by the Brauer-Manin obstruction. Table 1 at the beginning of this chapter collects some of them.

2. Proof of Theorem 5.2

We turn now our attention to the quotient $X_D^{(m)}$ of X_D by the action of the Atkin-Lehner involution associated with a positive divisor m of D, in order to prove Theorem 5.2. The proof goes along the same lines as the proof of Theorem 5.1, thus we first need to choose a suitable étale covering of the curve $X_D^{(m)}$.

As in Section 4 of Chapter 4, we place ourselves under Assumption 4.25, so that $D = pm$ is odd and p is a prime such that $(\frac{m}{p}) = -1$. We also assume that $p \equiv 3 \mod 4$. In particular, it follows from Ogg's formula for the number of fixed points of an Atkin-Lehner involution that ω_m is fixed point free, hence the natural quotient map

$$\pi_m : X_D \longrightarrow X_D^{(m)}$$

is unramified. Applying descent to this double cover of $X_D^{(m)}$, some sufficient conditions for the emptiness of $X_D^{(m)}(\mathbb{Q})$ were found in [**RSY05**]. Here, we shall rather use another cyclic étale covering of $X_D^{(m)}$. Namely, by virtue of Theorem 2.2, if $Y_{D,p}^{(m)} := Y_{D,p}/\langle\hat{\omega}_m\rangle$ denotes the quotient of the curve $Y_{D,p}$ by the action induced by the Atkin-Lehner involution $\hat{\omega}_m$ lifting ω_m to $X_{D,p}$, then the natural map

$$g_p^{(m)} : Y_{D,p}^{(m)} \longrightarrow X_D^{(m)}$$

is a cyclic étale covering of degree $(p^2-1)/12$. In other words:

Lemma 5.12. *The covering $g_p^{(m)} : Y_{D,p}^{(m)} \to X_D^{(m)}$ is an $X_D^{(m)}$-torsor under the constant group scheme $\mathbb{F}_{p^2}^{\times 12} \simeq \mathbb{Z}/\frac{p^2-1}{12}\mathbb{Z}$.*

Remark 5.13. We have invoked the machinery of Chapter 2 in order to ensure that $Y_{D,p}^{(m)} \to X_D^{(m)}$ is a cyclic étale covering. However, under the assumptions of this section one can proceed in a simpler way, avoiding many technicalities that were needed in Chapter 2.

Indeed, by virtue of Lemma 1.45, one can choose a twist χ_m of norm m as a representative of ω_m in $\mathrm{Norm}_{B_{D,+}^\times}(\mathcal{O}_D)$. Then $\chi_m^2 = m$ and $\mathrm{w}_m = \chi_m\alpha$ for some $\alpha \in \mathcal{O}_D^\times$ of reduced norm -1. The Atkin-Lehner involution $\omega_m : X_D \to X_D$ does not depend on this choice, and notice that now the monomorphism ι_{ω_m} is described by

$$\iota_{\omega_m}(\beta) = \iota(\chi_m^{-1}\beta\chi_m), \quad \beta \in \mathcal{O}_D.$$

Having fixed this choice, one can define the automorphism

$$\hat{\omega}_m : X_{D,p} \longrightarrow X_{D,p}$$

using only the moduli interpretation of $X_{D,p}$ by the rule

$$P = [(A, \iota, x_p)] \longmapsto \hat{\omega}_m(P) = [(A, \iota_{\omega_m}, x_p)]. \tag{5.2}$$

Since χ_m normalizes $\mathcal{O}_D$, observe that x_p is still a generator of the canonical torsion subgroup $C_p \subseteq A[p]$ when regarded as an $\mathcal{O}_D$-module via ι_{ω_m}, hence $\hat{\omega}_m$ is well defined. Moreover, the condition $\chi_m^2 = m$ implies that $\hat{\omega}_m$ certainly is an involution lifting ω_m to $X_{D,p}$. In fact, it follows from standard moduli considerations that $\hat{\omega}_m$ is a rational involution of the curve $X_{D,p}/\mathbb{Q}$.

From the very description (5.2) of $\hat{\omega}_m$, it clearly commutes with every diamond automorphism $\delta \in \Delta$, so that $\hat{\omega}_m$ acts as an involution lifting ω_m on each intermediate covering of $X_{D,p} \to X_D$, giving rise in turn to a cyclic covering of $X_D^{(m)}$ after taking the quotient by the action of $\hat{\omega}_m$. In particular, the étale covering $Y_{D,p} \to X_D$ produces the above cyclic étale covering

$$Y_{D,p}^{(m)} \longrightarrow X_D^{(m)}.$$

Now we can proceed similarly as in the previous section. If k is a field of characteristic zero and $Q \in X_D^{(m)}(k)$, by specialisation of the torsor $g_p^{(m)}$ at the point Q we get a continuous character

$$\varphi_Q : G_k \longrightarrow \mathrm{Aut}(Y_{D,p}^{(m)}/X_D^{(m)}) \simeq \mathbb{F}_{p^2}^{\times 12}$$

by which the Galois group acts on the fibre of $g_p^{(m)} : Y_{D,p}^{(m)} \to X_D^{(m)}$ at Q. For example, the specialisation of $g_p^{(m)}$ at a point $Q_\ell \in X_D^{(m)}(\mathbb{Q}_\ell)$ gives rise to a (local) Galois character

$$\varphi_{Q_\ell} : G_{\mathbb{Q}_\ell} \to \mathbb{F}_{p^2}^{\times 12}.$$

Using the moduli interpretation for the quotient $X_D^{(m)}$ (cf. Proposition 1.46), if (A_ℓ, i_ℓ) is a pair parametrised by the point $Q_\ell \in X_D^{(m)}(\mathbb{Q}_\ell)$, then the local character φ_{Q_ℓ} is closely related to the Galois representation

$$\alpha_{Q_\ell,\mathfrak{p}} : G_{\mathbb{Q}_\ell} \longrightarrow \mathbb{F}_{p^2}^{\times}/\{\pm 1\}$$

attached to the point Q_ℓ in the previous section. The proof of the next lemma is analogous to that of Lemma 5.4:

LEMMA 5.14. *For any $\sigma \in G_{\mathbb{Q}_\ell}$,*

$$\tilde{\alpha}_{Q_\ell,\mathfrak{p}}(\sigma)^{24} = \varphi_{Q_\ell}(\sigma)^2.$$

In terms of $\alpha_{Q_\ell,\mathfrak{p}}$, we have

$$\alpha_{Q_\ell,\mathfrak{p}}(\sigma)^{12} = \varphi_{Q_\ell}(\sigma) \mod \pm 1, \quad \textit{for all } \sigma \in G_{\mathbb{Q}_\ell}.$$

Together with Corollary 4.30 (a) it follows immediately:

COROLLARY 5.15. *For $\ell \neq p$, the local character $\varphi_{Q_\ell}^2$ is unramified.*

At this point, we have only considered abelian surfaces parametrised by local points on $X_D^{(m)}$. However, we need to discuss some global considerations before proving Theorem 5.2. In the following lemmas, we still assume that D is odd. Let also $Q \in X_D^{(m)}(\mathbb{Q})$, and let K be the imaginary quadratic field generated by the preimages of Q by π_m. That is,

$$\pi_m^{-1}(Q) = \{P, \omega_m(P)\} \subseteq X_D(K).$$

Understanding the field K is of great importance, and this fact appears reflected in the definition of the set $\mathcal{B}_2(q)$ introduced before the statement of Theorem 5.2.

LEMMA 5.16. *The involution ω_m is fixed point free if and only if the imaginary quadratic field $\mathbb{Q}(\sqrt{-m})$ does not embed in B_D.*

PROOF. It follows immediately from the criterion of Hasse and the formula for the number of fixed points of an Atkin-Lehner involution due to Ogg ([**Ogg83**]). □

Now, we use descent to prove the following:

LEMMA 5.17. *If $\mathbb{Q}(\sqrt{-m})$ does not embed in B_D, then K is unramified away from D.*

PROOF. By the above lemma, $\pi_m : X_D \to X_D^{(m)}$ is unramified, so it is an $X_D^{(m)}$-torsor under the constant group scheme $\mathbb{Z}/2\mathbb{Z}$. By the work of Morita on integral models of X_D (see [**Mor81**]), π_m extends to a smooth morphism of smooth and projective schemes over $\mathrm{Spec}(\mathbb{Z}[1/D])$, and yields a torsor under $\mathbb{Z}/2\mathbb{Z}$, now regarded as a constant $\mathrm{Spec}(\mathbb{Z}[1/D])$-group scheme.

By descent theory, the $\mathbb{Q}$-rational points of $X_D^{(m)}$ can be recovered from the $\mathbb{Q}$-rational points on the twisted torsors of $\pi_m : X_D \to X_D^{(m)}$. More precisely,

$$X_D^{(m)}(\mathbb{Q}) = \bigsqcup_{\tau \in \mathrm{H}^1(\mathbb{Q},\{\pm 1\})} {}^{\tau}X_D{}^{(m)}(\mathbb{Q}),$$

where ${}^{\tau}X_D{}^{(m)}(\mathbb{Q})$ is an abbreviation for ${}^{\tau}\pi_m({}^{\tau}X_D(\mathbb{Q}))$. Here the cohomology classes $\tau \in \mathrm{H}^1(\mathbb{Q}, \{\pm 1\})$ must be regarded as Galois quadratic characters

$$\tau : \mathrm{Gal}\,(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \{\pm 1\},$$

hence they are in correspondence with quadratic extensions. Since X_D has no real points, we can restrict ourselves to the imaginary quadratic ones. Moreover, by [**SY04**, Lemma 1.1] or [**Sko05**, p. 106], if $L/\mathbb{Q}$ is a quadratic extension ramified at a prime not dividing D, then ${}^{\tau_L}X_D(\mathbb{Q}) = \emptyset$,

where τ_L is the Galois quadratic character corresponding to L. In other words, only the quadratic characters unramified away from D contribute in the above decomposition of $X_D^{(m)}(\mathbb{Q})$.

In particular, since $P \in X_D(K)$ and $\pi_m(P) = Q \in X_D^{(m)}(\mathbb{Q})$, the class $\zeta(Q) \in \mathrm{H}^1(\mathbb{Q}, \{\pm 1\})$ of the $\mathbb{Q}$-torsor given by the fibre $X_{D,Q} \to Q$ is the quadratic character τ_K corresponding to the quadratic extension $K/\mathbb{Q}$. Hence, the point Q arises from a $\mathbb{Q}$-rational point on the twisted curve ${}^{\tau_K}X_D$. By the above discussion, K must be unramified away from D. □

Indeed, Lemma 5.17 proves the case $F = \mathbb{Q}$ of [**Rot08**, Proposition 1.3], which states how K depends on the pair $(\mathcal{O}, R_m)$. Finally, we are in position to prove Theorem 5.2. Similarly as we did for Theorem 5.1, first of all we show that under the hypotheses of Theorem 5.2 the only rational points on the curve $X_D^{(m)}$ should have CM by either $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$:

THEOREM 5.18. *Let B_D be an indefinite quaternion algebra of odd discriminant $D = pm$, with $p \geq 7$ a prime such that $p \equiv 3 \mod 4$. If there is a prime q such that $B_D \in \mathcal{B}_2(q)$ and $p \notin \mathcal{P}_2(q)$, then*

$$X_D^{(m)}(\mathbb{Q}) = X_D^{(m)}(\mathbb{Q}) \cap \pi_m(\mathrm{CM}(\mathbb{Q}(\sqrt{-1})) \cup \mathrm{CM}(\mathbb{Q}(\sqrt{-3}))).$$

PROOF. First of all, notice that if $(\frac{m}{p}) = 1$, then $X_D^{(m)}(\mathbb{A}_\mathbb{Q}) = \emptyset$ by [**RSY05**, Theorem 3.1] and there is nothing to prove. Thus, we can assume $(\frac{m}{p}) = -1$, placing ourselves under Assumption 4.25 as before.

Suppose there exists a point $Q \in X_D^{(m)}(\mathbb{Q})$ which is not a CM point by $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$. By the moduli interpretation of $X_D^{(m)}$, we can choose an abelian surface (A, i) with real multiplication by the ring of integers R_m of $E = \mathbb{Q}(\sqrt{m})$ whose field of moduli is $\mathbb{Q}$, and such that $\mathcal{O}_D \hookrightarrow \mathrm{End}_{\bar{\mathbb{Q}}}(A)$, corresponding to the point Q. The preimages of Q under π_m are rational over a quadratic extension $K/\mathbb{Q}$, that is,

$$\pi_m^{-1}(Q) = \{P, \omega_m(P)\} \subseteq X_D(K).$$

After Shimura, K must be imaginary. By means of the diagonal embedding $X_D^{(m)}(\mathbb{Q}) \hookrightarrow X_D^{(m)}(\mathbb{A}_\mathbb{Q})$, the point Q defines a sequence of local points $\{Q_\ell\}_\ell \in X_D^{(m)}(\mathbb{A}_\mathbb{Q})$. For each one of these points, say $Q_\ell \in X_D^{(m)}(\mathbb{Q}_\ell)$, we can choose the same abelian surface (A, i) representing it. For the sake of clarity, however, we denote it by (A_ℓ, i_ℓ). Note that (A_ℓ, i_ℓ) has complex multiplication by neither $\mathbb{Q}(\sqrt{-1})$ nor $\mathbb{Q}(\sqrt{-3})$.

The global character

$$\varphi : G_\mathbb{Q} \longrightarrow \mathbb{F}_{p^2}^{\times 12}$$

obtained by specialisation of the torsor $g_p^{(m)}$ at Q restricts to each one of the local characters φ_{Q_ℓ} attached to each point Q_ℓ on $G_{\mathbb{Q}_\ell}$. Therefore, by Corollary 5.15 we have that φ^2 is unramified away from p.

Consider the abelian surface (A_q, i_q) representing the point $Q_q \in X_D^{(m)}(\mathbb{Q}_q)$, and the Galois representation

$$\alpha_{Q_q,\mathfrak{p}} : G_{\mathbb{Q}_q} \longrightarrow \mathbb{F}_{p^2}^\times / \{\pm 1\}$$

attached to Q_q over its field of moduli, arising from the action of $G_{\mathbb{Q}_q}$ on the canonical torsion subgroup of $A_q[p]$. Choose also a lift

$$\tilde{\alpha}_{Q_q,\mathfrak{p}} : G_{\mathbb{Q}_q} \longrightarrow \mathbb{F}_{p^2}^\times$$

of this representation as usual. By Lemma 5.14, the local character

$$\varphi_{Q_q} : G_{\mathbb{Q}_q} \longrightarrow \mathbb{F}_{p^2}^{\times 12}$$

attached to Q_q by specialisation of $g_p^{(m)}$ satisfies

$$\varphi_{Q_q}^2 = \tilde{\alpha}_{Q_q,\mathfrak{p}}^{24} \quad \text{and} \quad \varphi_q \mod \pm 1 = \alpha_{Q_q,\mathfrak{p}}^{12}.$$

Choose now a Frobenius element $\sigma_q \in G_{\mathbb{Q}_q}$, i.e. an element inducing $\mathrm{Fr}_q \in \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ under reduction. We first claim that the equality

$$\tilde{\alpha}_{Q_q,\mathfrak{p}}(\sigma_q)^{24} = q^{12}$$

holds in $\mathbb{F}_p^\times$.

For each prime ℓ, consider the local Artin reciprocity map

$$w_\ell : \mathbb{Z}_\ell^\times \xrightarrow{\simeq} I_\ell^{ab},$$

and let

$$w : \prod_\ell \mathbb{Z}_\ell^\times \xrightarrow{\prod w_\ell} G_{\mathbb{Q}}^{ab}$$

be the global Artin map. Observe that the image under w of the idèle

$$\beta = (q^{-1}, \dots, q^{-1}, 1, q^{-1}, \dots) \in \prod_\ell \mathbb{Z}_\ell^\times,$$

where the 1 is in the q-th position, is a Frobenius element $\mathrm{Frob}_q \in G_{\mathbb{Q}}^{ab}$ at q. Therefore,

$$\sigma_q \circ \mathrm{Frob}_q^{-1} \in I_q,$$

where here $I_q \subseteq \mathrm{Gal}\,(\bar{\mathbb{Q}}_q/\mathbb{Q}_q)$ denotes the inertia subgroup. Since φ restricted to $\mathrm{Gal}\,(\bar{\mathbb{Q}}_q/\mathbb{Q}_q)$ coincides with φ_{Q_q}, whose square is unramified, we have $\varphi(\sigma_q)^2 = \varphi(\mathrm{Frob}_q)^2$.

In order to show our claim, first note that we have

$$\varphi(\sigma_q)^2 = \varphi_{Q_q}(\sigma_q)^2 = \tilde{\alpha}_{Q_q,\mathfrak{p}}(\sigma_q)^{24},$$

because $\varphi_{|G_{\mathbb{Q}_q}} = \varphi_{Q_q}$. Besides, since φ^2 is unramified away from p,

$$\varphi(\mathrm{Frob}_q)^2 = \varphi(w(\beta))^2 = \varphi_{Q_p}(w_p(q^{-1}))^2 = \varphi_{Q_p}(\tau_{q^{-1}})^2 = \tilde{\alpha}_{Q_p,\mathfrak{p}}(\tau_{q^{-1}})^{24},$$

where we choose any representative $\tau_{q^{-1}} \in I_p$ of $w_p(q^{-1}) \in I_p^{ab}$. Then, we must show that

$$\tilde{\alpha}_{Q_p,\mathfrak{p}}(\tau_{q^{-1}})^{24} = q^{12}.$$

More generally, let us denote by $\tau_x \in I_p$ any representative of $w_p(x) \in I_p^{ab}$, for $x \in \mathbb{Z}_p^\times$, and denote also by $\tilde{x} \in \mathbb{F}_p^\times$ the reduction modulo p of x. By [**Ser72**, Prop. 3, 8], if we denote by

$$\bar{\chi}_p : G_{\mathbb{Q}_p} \longrightarrow \mathbb{F}_p^\times$$

the reduction modulo p of the p-th cyclotomic character, then we have

$$\bar{\chi}_p(\tau_x) = \tilde{x}^{-1} \quad \text{for all} x \in \mathbb{Z}_p^\times.$$

Then (cf. Corollary 4.30, Lemma 4.31):

$$\begin{aligned} \tilde{x}^{-2} &= \bar{\chi}_p(\tau_x^2) = \pm \det(\bar{\varrho}_{Q_p,\mathfrak{p}}(\tau_x^2)) = \pm\psi(\tau_x^2) N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\tilde{\alpha}_{Q_p,\mathfrak{p}}(\tau_x^2)) = \\ &= \pm\tilde{\alpha}_{Q_p,\mathfrak{p}}(\tau_x^2)^2 = \pm\tilde{\alpha}_{Q_p,\mathfrak{p}}(\tau_x)^4, \end{aligned}$$

where we have used that $\tilde{\alpha}_{Q_p,\mathfrak{p}}(\tau^2) \in \mathbb{F}_p^\times$ for every $\tau \in I_p$ (see Remark 4.33). In particular, for $x = q^{-1}$ we get

$$\tilde{\alpha}_{Q_p,\mathfrak{p}}(\tau_{q^{-1}})^{24} = q^{12} \in \mathbb{F}_p^\times, \tag{5.3}$$

as we claimed.

Now, since $(\frac{m}{p}) = -1$ and $p \equiv 3 \mod 4$, we have $(\frac{-m}{p}) = 1$, so that $\mathbb{Q}(\sqrt{-m})$ does not embed in B_D. By Lemma 5.17, K is unramified away from D. Also, since $B_D \in \mathcal{B}_2(q)$ the prime q is not inert in K. If we let $\mathfrak{q}$ be a prime of K above q, then we can regard the point P as a point in $X_D(K_\mathfrak{q})$, where $K_\mathfrak{q}$ is the completion of K at $\mathfrak{q}$, so that, using the notation from Lemma 4.27, we can choose K_q to be the quadratic extension $K_\mathfrak{q}$ of $\mathbb{Q}_q$. Moreover, note that the residue field of this extension is isomorphic to $\mathbb{F}_q$.

On the other hand, since A_q/K_q has potential good reduction, following the construction of Serre and Tate at the end of p. 498 in [**ST68**], we can choose a finite totally ramified extension L_q/K_q such that the closed fibre of the Néron model of $A_q \times_{K_q} L_q$ over the ring of integers of L_q is an abelian surface $\tilde{A}_q$ over $\mathbb{F}_q$. Moreover, the action of the Frobenius element σ_q on the Tate modules $T_p(A_q)$ and $T_p(\tilde{A}_q)$ is the same.

Besides, the quaternion algebra $B_D \subseteq \mathrm{End}^0_{K_q}(A_q)$ is embedded in $\mathrm{End}^0_{\mathbb{F}_q}(\tilde{A}_q)$, since the residue field of $K_q/\mathbb{Q}_q$ is $\mathbb{F}_q$. Moreover, $\sigma_q \in \mathrm{Gal}\,(\bar{\mathbb{Q}}_q/K_q) \subseteq \mathrm{Gal}\,(\bar{\mathbb{Q}}_q/\mathbb{Q}_q)$, thus by Corollary 4.32 the characteristic polynomial of $\varrho_{(A_q,i_q),\mathfrak{p}}(\sigma_q)$ reduced modulo $\mathfrak{p}$ is congruent to

$$T^2 - (\tilde{\alpha}_{Q_q,\mathfrak{p}}(\sigma_q) + q\tilde{\alpha}_{Q_q,\mathfrak{p}}(\sigma_q)^{-1})T + q \in \mathbb{F}_{p^2}[T].$$

This implies, by [**Jor86**, Theorem 2.1], that

$$\tilde{\alpha}_{Q_q,\mathfrak{p}}(\sigma_q) + q\tilde{\alpha}_{Q_q,\mathfrak{p}}(\sigma_q^{-1})$$

is the reduction modulo p of an integer a_q of absolute value at most $2\sqrt{q}$. Then, using (5.3) we can write

$$a_q \equiv \sqrt{q}(\zeta + \zeta^{-1}) \mod \bar{\mathfrak{p}},$$

where $\zeta = \frac{\tilde{\alpha}_{Q_q,\mathfrak{p}}(\sigma_q)}{\sqrt{q}}$ is a 24-th root of 1, and $\bar{\mathfrak{p}}$ a prime of $\bar{\mathbb{Q}}$ over $\mathfrak{p}$. Computing the possible values of $\sqrt{q}(\zeta + \zeta^{-1})$ with ζ a 24-th root of 1 leads to

$$a_q \equiv 0, \pm\sqrt{q}, \pm\sqrt{2q}, \pm\sqrt{3q}, \pm 2\sqrt{q} \text{ or } \pm\sqrt{q}\cdot\sqrt{2\pm\sqrt{3}} \mod \bar{\mathfrak{p}}.$$

In other words, $p|a_q^2 - sq$ for some $s = 0, 1, 2, 3, 4$ or $p|a_q^4 - 4a_q^2 q + q^2$. But since $|a_q| \leq 2\sqrt{q}$, from the definition of $\mathcal{P}_2(q)$ the above congruence must be an equality. Moreover, since a_q is an integer the only possibilities are

(i) $a_q = 0$,
(ii) $q = 2$ and $a_2 = \pm 2$, or
(iii) $q = 3$ and $a_q = \pm 3$.

According to the classification of abelian surfaces admitting quaternionic multiplication over finite fields following from the Honda-Tate theory (see [**Jor86**, Theorem 2.1]), we deduce that for these cases one has $\mathrm{End}^0_{\mathbb{F}_q}(\tilde{A}_q) \simeq \mathrm{M}_2(\mathbb{Q}(\sqrt{-q}))$, $\mathrm{M}_2(\mathbb{Q}(\sqrt{-1}))$ or $\mathrm{M}_2(\mathbb{Q}(\sqrt{-3}))$, respectively. It follows that B_D is split by $\mathbb{Q}(\sqrt{-q})$, $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$, respectively, which contradicts the assumption that $B_D \in \mathcal{B}_2(q)$. Then, all the points in $X_D^{(m)}(\mathbb{Q})$ must have CM by either $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$, so the theorem follows. □

Now we can use again the results from Section 3.5 of Chapter 1 to check that, under the hypotheses of Theorem 5.2, both $X_D^{(m)}(\mathbb{Q}) \cap \pi_m(\mathrm{CM}(\mathbb{Q}(\sqrt{-1})))$ and $X_D^{(m)}(\mathbb{Q}) \cap \pi_m(\mathrm{CM}(\mathbb{Q}(\sqrt{-3})))$ are empty. In other words, the points in $X_D^{(m)}(\bar{\mathbb{Q}})$ with CM by either $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$ cannot be rational. We give the details in the following lemmas.

LEMMA 5.19. *If a pair (D, m) satisfies the hypotheses of Theorem 5.2, then $X_D^{(m)}(\mathbb{Q})$ does not contain points with CM by $\mathbb{Q}(\sqrt{-1})$.*

PROOF. Assume on the contrary that $Q \in X_D^{(m)}(\mathbb{Q})$ has CM by some imaginary quadratic order R_f in $\mathbb{Q}(\sqrt{-1})$ of conductor $f \geq 1$. Let $K/\mathbb{Q}$ be the imaginary quadratic field such that $\pi_m^{-1}(Q) = \{P, \omega_m(P)\} \subseteq X_D(K)$. Since X_D has no rational points, observe that $K = \mathbb{Q}(P)$, the field generated by the coordinates of P. By Theorem 1.50, $K \cdot \mathbb{Q}(\sqrt{-1}) = H_f$, where H_f is the ring class field of R_f.

Assume first that $K \neq \mathbb{Q}(\sqrt{-1})$. Then, $H_f/\mathbb{Q}(\sqrt{-1})$ has degree 2, so that $h_f = h(R_f) = 2$. The only values of f for which this is possible are $3, 4$ and 5. Moreover, since $\mathrm{CM}(R_f) \neq \emptyset$, Proposition 1.48 implies that $D/D(R_f)$ divides $\mathrm{disc}(R_f) = -4f^2$. But since $[H_f : K] = 2$, by Theorem 1.51 we find $D(R_f) = 1$, so that D divides $-4f^2$. Therefore, the only possible values for D are $2 \cdot 3$ and $2 \cdot 5$ (corresponding to $f = 3$ and 5, respectively), but these discriminants cannot arise in Theorem 5.2 because they are even.

Then, we can place ourselves in the case $K = \mathbb{Q}(\sqrt{-1})$. In this case, $H_f = \mathbb{Q}(\sqrt{-1})$, so that $h_f = h(R_f) = 1$, and therefore f is either 1 or 2. Moreover, by Proposition 1.48 $D/D(R_f)$ must divide $\mathrm{disc}(R_f) = -4$ or $-4 \cdot 2^2$, respectively. Since D is odd, this implies that $D(R_f) = D$. Also, since $H_f = \mathbb{Q}(\sqrt{-1})$, observe that $\sigma_{\mathfrak{a}} = 1$ for every ideal $\mathfrak{a} \in I(R_f)$. Then, from Proposition 1.53

we deduce that $\mathbb{Q}(Q) = \mathbb{Q}$ if and only if $D(R_f)$ divides m, hence, if and only if $m = D$. But this case cannot arise in Theorem 5.2.

Summing up, under the hypotheses of Theorem 5.2 we conclude that $X_D^{(m)}(\mathbb{Q})$ does not contain points with CM by $\mathbb{Q}(\sqrt{-1})$. □

LEMMA 5.20. *If a pair (D, m) satisfies the hypotheses of Theorem 5.2, then $X_D^{(m)}(\mathbb{Q})$ does not contain points with CM by $\mathbb{Q}(\sqrt{-3})$.*

PROOF. Imagine that $Q \in X_D^{(m)}(\mathbb{Q})$ is a $\mathbb{Q}$-rational point with CM by some imaginary quadratic order R_f in $\mathbb{Q}(\sqrt{-3})$ of conductor $f \geq 1$, and let $K/\mathbb{Q}$ be the imaginary quadratic field such that $\pi_m^{-1}(Q) = \{P, \omega_m(P)\} \subseteq X_D(K)$. Notice that $K = \mathbb{Q}(P)$, because $X_D(\mathbb{Q}) = \emptyset$. By Theorem 1.50, we have $K \cdot \mathbb{Q}(\sqrt{-3}) = H_f$, where H_f is the ring class field of R_f.

If $K \neq \mathbb{Q}(\sqrt{-3})$, then $H_f/\mathbb{Q}(\sqrt{-3})$ is a degree 2 extension, hence $h_f = h(R_f) = 2$. This implies that f is either $4, 5$ or 7. Moreover, since $\mathrm{CM}(R_f) \neq \emptyset$, Proposition 1.48 implies that $D/D(R_f)$ divides $\mathrm{disc}(R_f) = -3f^2$. But since $[H_f : K] = 2$, we know that $D(R_f) = 1$ by Theorem 1.51, so that D divides $-3f^2$. Therefore, the only possible values for D are $2 \cdot 3$, $3 \cdot 5$ and $3 \cdot 7$. But notice that $D = 6$ and $D = 15$ cannot arise in Theorem 5.2: 6 is even and 15 is not divisible by a prime $p > 5$, $p \equiv 3 \mod 4$. As for the case $D = 3 \cdot 7$, the only possibility is $p = 7$ and $m = 3$, but one checks that $7 \in \mathcal{P}_2(q)$ for every prime $q \neq 3$ and $B_{21} \notin \mathcal{B}_2(3)$. Hence, $D = 21$ cannot arise in Theorem 5.2 either.

Suppose now that $K = \mathbb{Q}(\sqrt{-3})$. In this case, $H_f = \mathbb{Q}(\sqrt{-3})$, so that $h_f = h(R_f) = 1$, and one deduces that f is either $1, 2$ or 3. Moreover, $D/D(R_f)$ must divide $\mathrm{disc}(R_f) = -3f^2$ by Proposition 1.48. Since D is odd, we immediately see that it must be $D/D(R_f) = 1$ or 3. On the other hand, since $H_f = \mathbb{Q}(\sqrt{-3})$ observe that $\sigma_{\mathfrak{a}} = 1$ for every ideal $\mathfrak{a} \in I(R_f)$. Then, from Proposition 1.53 we deduce that $\mathbb{Q}(Q) = \mathbb{Q}$ if and only if $D(R_f)$ divides m. Since $D/D(R_f)$ is either 1 or 3, this implies that either $m = D$ or $m = D(R_f)$ and $3m = 3D(R_f) = D$. But none of these cases can arise in Theorem 5.2.

Summing up, under the hypotheses of Theorem 5.2, $X_D^{(m)}(\mathbb{Q})$ does not contain points with CM by $\mathbb{Q}(\sqrt{-3})$. □

As we quoted before, it is now plain that Theorem 5.18 together with the above two lemmas completely proves Theorem 5.2.

Finally, it is natural to ask whether the examples of Atkin-Lehner quotients of Shimura curves without rational points arising from Theorem 5.2 include counterexamples to the Hasse principle or not. In [**RSY05**, Theorem 3.1], a criterion for the existence of adèlic points on $X_D^{(m)}$ was given, which together with Theorem 5.2 can be indeed used to produce counterexamples to the Hasse principle over $\mathbb{Q}$. In the particular case where D is the product of two primes, we obtain the following corollary, where for an integer $n > 0$ the quantity $\Sigma_n(D)$ is defined as in (5.1):

COROLLARY 5.21. *Assume that $D = pm$ satisfies the hypotheses of Theorem 5.2 with m a prime such that $(\frac{m}{p}) = -1$, and let g be the genus of $X_D^{(m)}$. If for every prime $\ell \nmid pm$ with $\ell < 4g^2$, it holds either $\Sigma_\ell(D) \neq 0$ or $\Sigma_{\ell m}(D) \neq 0$, then $X_D^{(m)}$ is a counterexample to the Hasse principle over $\mathbb{Q}$.*

PROOF. First of all, we have $X_{pm}^{(m)}(\mathbb{Q}) = \emptyset$ by Theorem 5.2. Secondly, by assumption we have $(\frac{m}{p}) = -1$ and $p \equiv 3 \mod 4$, so that using the Quadratic Reciprocity Law one obtains

$$\left(\frac{-m}{p}\right) = 1, \quad \left(\frac{-p}{m}\right) = -1.$$

By virtue of [**RSY05**, Theorem 3.1], these conditions together with the last hypothesis in the statement concerning the primes $\ell \nmid pm$, $\ell < 4g^2$, imply that $X_{pm}^{(m)}(\mathbb{A}_{\mathbb{Q}}) \neq \emptyset$. □

This corollary allows us to produce easily new counterexamples to the Hasse principle over $\mathbb{Q}$ realised by Atkin-Lehner quotients of Shimura curves. Some of them are collected in Table 2 after the statement of Theorem 5.2, at the beginning of the chapter.

REMARK 5.22. Assume that $D = pm$ satisfies the hypotheses of Theorem 5.2, so that $X_D^{(m)}(\mathbb{Q}) = \emptyset$. We were unable to prove that this is accounted for by the Brauer-Manin obstruction and we leave it as an open question here. The ultimate reason why we did manage to prove the analogous statement for Shimura curves over imaginary quadratic fields K and can not do so here relies on Theorem 4.26, which shows that the obstruction B_Q for a point $Q \in X_D^{(m)}(\mathbb{Q})$ to be represented by an abelian surface admitting a model over $\mathbb{Q}$ *depends* on the point Q. This is in contrast with Theorem 4.20, which asserts that, for a point $P \in X_D(K)$, we have $B_P = B_D \otimes_{\mathbb{Q}} K$, independently of the choice of P and even of the field K.

This raises the following questions, which we find interesting in themselves: let X be the moduli space of a family of abelian varieties, possibly equipped with additional structure (polarisation, endomorphisms, marked torsion points, etc.), and assume X admits a canonical model over $\mathbb{Q}$. Let k be a field of characteristic 0 and assume Hypothesis 4.8 holds for all points $P \in X(k)$.

QUESTION 5.23. Is the quaternion algebra $B_P \in \mathcal{Q}_k$ independent of the choice of P? If not, is the set $\{B_P, P \in X(k)\} \subset \mathcal{Q}_k$ comparatively more manageable than the set $X(k)$ itself? If yes, is there in fact a quaternion algebra $B \in \mathcal{Q}_{\mathbb{Q}}$ such that $B_P = B \otimes_{\mathbb{Q}} k$ for all $P \in X(k)$, independently of the field k?

3. A different approach for $X_D^{(m)}$

In the previous section we have studied the non-existence of rational points on certain Atkin-Lehner quotients of Shimura curves, using an approach which is inspired by the work of Skorobogatov [**Sko05**], Jordan [**Jor86**] and Rotger [**Rot08**]. That is, by combining descent applied to a suitable étale covering of $X_D^{(m)}$ from Chapter 2 together with the study of certain Galois representations over fields of moduli studied in Chapter 4. However, Lemma 5.17 together with [**Rot08**, Theorem 1.4] already allows us to prove the non-existence of rational points on some Atkin-Lehner quotients of Shimura curves from a different approach (see Theorem 5.25 below).

Let $Q \in X_D^{(m)}(\mathbb{Q})$, and let $K/\mathbb{Q}$ be the imaginary quadratic extension such that $\pi_m^{-1}(Q) = \{P, \omega_m(P)\} \subseteq X_D(K)$. The next observation follows from [**Jor86**, p. 93]:

LEMMA 5.24. *If $2 \nmid D$, then $B_P = B_D \otimes K \simeq \mathrm{M}_2(K)$.*

In other words, by Theorem 4.20, we can choose a pair (A, ι) defined over K such that $P = [(A, \iota)]$. Hence, this observation goes in the same direction as Lemma 4.27 in the local context.

On the other hand, for a given rational prime q, let us define $\mathcal{P}_0(q) \subseteq \mathcal{P}_2(q)$ to be the set of rational primes dividing some non-zero integer in the set

$$\bigcup_{|a| \leq 2\sqrt{a}} \bigcup_{s=0}^{4} \{a^2 - sq\}.$$

For instance, we have $\mathcal{P}_0(3) = \{2, 3, 5, 11\}$ and $\mathcal{P}_0(5) = \{2, 3, 5, 7, 11, 19\}$.

THEOREM 5.25. *Let p, m be two different primes, $p \equiv m \equiv 3 \bmod 4$, $(\frac{m}{p}) = -1$. If there exists an odd prime q such that $p \notin \mathcal{P}_0(q)$, $(\frac{q}{p}) = 1$ and $(\frac{q}{m}) = -1$, then $X_{pm}^{(m)}(\mathbb{Q})$ consists only of CM-points.*

PROOF. Suppose that there exists a non-CM point $Q \in X_{pm}^{(m)}(\mathbb{Q})$, and let K be the imaginary quadratic field such that $\pi_m^{-1}(Q) = \{P, \omega_m(P)\} \subseteq X_{pm}(K)$. By Lemma 5.17, K is unramified at the primes not dividing pm. Hence the only possibilities for K are $\mathbb{Q}(\sqrt{-p})$, $\mathbb{Q}(\sqrt{-m})$, $\mathbb{Q}(\sqrt{-pm})$.

The last option is excluded because $\mathbb{Q}(\sqrt{-pm})$ is ramified at 2. But the case $\mathbb{Q}(\sqrt{-m})$ can also be excluded. Indeed, since $(\frac{-m}{p}) = (\frac{-1}{p})(\frac{m}{p}) = 1$ we get that $-m$ is a square in $\mathbb{Q}_p$. If ${}^{-m}X_{pm}$ denotes the quadratic twist of X_{pm} by $\mathbb{Q}(\sqrt{-m})$ and ω_m, this implies that ${}^{-m}X_{pm} \times \mathbb{Q}_p \simeq X_{pm} \times \mathbb{Q}_p$, but $X_{pm}(\mathbb{Q}_p) = \emptyset$ by [**JL85**]. Hence $K = \mathbb{Q}(\sqrt{-p})$.

But now observe that $B_{pm} \simeq (\frac{-p,m}{\mathbb{Q}})$. Therefore, by the above lemma and [**BFGR06**, Theorem 4.5] the point Q corresponds, in the terminology of [**Rot08**], to a *modular triplet* $(\mathcal{O}_{pm}, R_m, \mathbb{Q}(\sqrt{-p}))$.

By applying [**Rot08**, Theorem 1.4], we deduce $(\frac{-q}{m}) = -1$, but our assumptions imply

$$\left(\frac{-q}{m}\right) = \left(\frac{-1}{m}\right)\left(\frac{q}{m}\right) = 1,$$

and thus we get a contradiction. Therefore, $X_{pm}^{(m)}(\mathbb{Q})$ contains only CM-points. □

COROLLARY 5.26. *Under the hypotheses of Theorem 5.25, if $p \neq 3$, 7, 11, 19, 43, 67, 163, then $X_{pm}^{(m)}(\mathbb{Q}) = \emptyset$.*

PROOF. By Theorem 5.25, we know that $X_{pm}^{(m)}(\mathbb{Q})$ consists only of CM-points, so it suffices to show that under the extra assumption on the prime p there are no CM-points in $X_{pm}^{(m)}(\mathbb{Q})$.

For $i = 1, 2$, let $\mathcal{R}_i$ denote the set of orders R in imaginary quadratic fields such that $h(R) = i$, where $h(R)$ denotes the class number of R. And for any $R \in \mathcal{R}_1$, set $p_R = 2$ if $\mathrm{disc}(R) = -2^k$ and p_R to be the single odd prime dividing $\mathrm{disc}(R)$, otherwise. From [**BFGR06**, Proposition 5.1], based on the work in [**GR06**, §5], the non-existence of CM-points in $X_{pm}^{(m)}(\mathbb{Q})$ is equivalent to the emptiness of the sets

$$S_1 = \{R \in \mathcal{R}_1 : p_R = p\}, \quad S_2 = \{R \in \mathcal{R}_2 : \frac{-pm}{\mathrm{disc}(R)} \in \mathbb{Q}^{\times 2}\}.$$

Let us show that under the hypotheses in the statement both S_1 and S_2 are empty.

Let first $R \in \mathcal{R}_1$, which has to be an order in an imaginary quadratic field L of class number 1. Since $\mathrm{disc}(R) = d_L \cdot f^2$, where d_L is the discriminant of L and f is the conductor of R, the only possibilities for p_R are 2, 3, 7, 11, 19, 43, 67, 163. By our hypotheses on p, the equality $p_R = p$ cannot occur, hence $S_1 = \emptyset$.

Now let $R \in \mathcal{R}_2$, which is therefore an order in an imaginary quadratic field L of class number 1 or 2. Let $f \geq 1$ be the conductor of R, so that $\mathrm{disc}(R) = d_L \cdot f^2$, where again d_L denotes the discriminant of L. Then, observe that

$$\frac{-pm}{\mathrm{disc}(R)} = \frac{-pm}{d_L \cdot f^2} \in \mathbb{Q}^{\times 2} \iff d_L = -4pm,$$

since d_L is a discriminant of a quadratic field and $p \equiv m \equiv 3 \mod 4$. Looking at the list of imaginary quadratic fields of class number 1 and 2, none of their discriminants is of the form $-4pm$ with $p \equiv m \equiv 3 \mod 4$, hence $S_2 = \emptyset$.

Summing up, both S_1 and S_2 are empty, so that $X_{pm}^{(m)}(\mathbb{Q}) = \emptyset$. □

This result is significant progress with respect to [**RSY05**, Theorem 5.1] and [**RSY05**, Corollary 5.2]. Fixed a prime q, Theorem 5.25 says that $X_{pm}^{(m)}(\mathbb{Q}) = \emptyset$ whenever m and p are different primes such that $p \notin \mathcal{P}_0(q)$, $p \neq 3$, 7, 11, 19, 43, 67, 163, $m \equiv p \equiv 3 \mod 4$, $(\frac{m}{p}) = -1$, $(\frac{q}{p}) = 1$ and $(\frac{q}{m}) = -1$. By Čebotarev's Density Theorem, there exist infinitely many such m and p.

In Table 3 below, for each prime $p \equiv 3 \mod 4$, $3 \leq p < 200$, $p \neq 3$, 7, 11, 19, 43, 67, 163, we list the primes $m \equiv 3 \mod 4$, with $m < 200$, such that p and m satisfy the hypotheses from Theorem 5.25, so that $X_{pm}^{(m)}(\mathbb{Q}) = \emptyset$.

REMARK 5.27. Note that Theorem 5.25 does not require the Atkin-Lehner involution ω_m to be twisting. Indeed, if p and m are as in Theorem 5.25, using the Quadratic Reciprocity Law one checks that $(\frac{-pm,m}{\mathbb{Q}})$ is ramified at p, but not at m. Hence, $B_{pm} \not\simeq (\frac{-pm,m}{\mathbb{Q}})$, and therefore ω_m is not twisting. As a consequence, Theorem 5.25 gives examples of Atkin-Lehner quotients of Shimura curves by non-twisting involutions having no rational points. In particular, the examples arising from Theorem 5.25 are not covered by Theorem 5.2, and vice versa.

REMARK 5.28. As in Corollary 5.21, if we assume moreover that $\Sigma_\ell(pm) \neq 0$ or $\Sigma_{\ell m}(pm) \neq 0$ for every prime $\ell \neq p, m$ with $\ell < 4g^2$, where g is the genus of $X_{pm}^{(m)}$, then [**RSY05**, Theorem 3.1] directly implies that the examples obtained from Theorem 5.25 are indeed counterexamples to the Hasse principle over $\mathbb{Q}$. For instance, we recover the example $X_{23\cdot 107}^{(107)}$ pointed out in [**RSY05**], and many others.

p	m's such that $X_{pm}^{(m)}(\mathbb{Q}) = \emptyset$, $m < 200$
23	7, 11, 19, 43, 67, 79, 83, 103, 107, 199
31	3, 11, 23, 43, 79, 83, 127, 139, 151, 167, 179, 199
47	11, 19, 23, 31, 43, 67, 107, 127, 139, 151, 163, 179, 199
59	11, 23, 31, 43, 47, 67, 83, 103, 131, 151, 179, 191
71	7, 11, 23, 31, 47, 59, 67, 127, 139, 163
79	3, 7, 43, 47, 59, 71, 103, 107, 127, 139,191, 199
83	19, 43, 47, 67, 71, 79, 103, 107, 139, 163, 179
103	3, 11, 31, 43, 47, 67, 71, 127, 151, 191, 199
107	7, 31, 43, 59, 67, 71, 103, 127, 131, 139, 167, 179, 191
127	3, 7, 23,43, 59, 67, 83, 139, 151, 167
131	19, 23, 31, 47, 67, 71, 79, 83, 103, 127, 139, 163, 199
139	3, 19, 23, 43, 59, 103, 151, 179, 199
151	3, 7, 23, 67, 71, 79, 83, 107, 131, 163, 179, 199
167	23, 43, 59, 67, 71, 79, 83, 103, 131, 139, 151, 163
179	7, 11,23, 71, 79, 103, 127, 131, 163, 167
191	7, 11, 19, 31, 47, 71, 83, 127, 131, 139, 151, 167, 179
199	3, 11, 19, 59, 67, 71, 83, 107, 127, 163, 167, 179, 191

TABLE 3. Examples from Theorem 5.25.

Bibliography

[BC91] J.-F. Boutot and H. Carayol. Uniformisation p-adique des courbes de Shimura: les théorèmes de Čerednik et de Drinfeld. *Astérisque*, 196-197:45–158, 1991.

[BCDT01] C. Breuil, B. Conrad, F. Diamond, and R. Taylor. On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14:843–939, 2001.

[BFGR06] N. Bruin, V. Flynn, J. Gonzàlez, and V. Rotger. On finiteness conjectures for endomorphism algebras of abelian surfaces. *Math. Proc. Camb. Phil. Soc.*, 141(3):383–408, 2006.

[BG13] M. Bhargava and B. H. Gross. The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point, 2013. Preprint, `arXiv:1208.1007v2`.

[Bha14] M. Bhargava. A positive proportion of plane cubics fail the Hasse principle, 2014. Preprint, `arXiv:1402.1131v1`.

[BL92] C. Birkenhake and H. Lange. *Complex Abelian Varieties*, volume 302 of *Gundl. math. Wiss.* Springer, 1992.

[BP11] Y. Bilu and P. Parent. Serre's Uniformity Problem in the Split Cartan Case. *Ann. Math. (2)*, 173:569–584, 2011.

[Bru13] N. Bruin. Success and challenges in determining the rational points on curves. In *ANTS X: Proceedings of the Tenth Algorithmic Number Theory Symposium*, The Open Book Series 1-1, pages 187–212, 2013.

[BS13a] M. Bhargava and A. Shankar. The average number of elements in the 4-Selmer groups of elliptic curves is 7, 2013. Preprint, `arXiv:1312.7333v1`.

[BS13b] M. Bhargava and A. Shankar. The average size of the 5-Selmer group of elliptic curves is 6, and the average rank is less than 1, 2013. Preprint, `arXiv:1312.7859v1`.

[BS13c] M. Bhargava and A. Shankar. Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves, 2013. Preprint, `arXiv:1006.1002v3`. To appear in *Ann. of Math.*

[BS13d] M. Bhargava and A. Shankar. Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0, 2013. Preprint, `arXiv:1007.0052v2`. To appear in *Annals of Math.*

[BSD63] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. I. *J. Reine Angew. Math.*, 212:7–25, 1963.

[BSD65] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. II. *J. Reine Angew. Math.*, 218:79–108, 1965.

[Cas91] J. W. S. Cassels. *Lectures on Elliptic Curves*, volume 24 of *LMS Student Texts*. Cambridge University Press, 1991.

[Cla03] P. Clark. *Rational points on Atkin-Lehner quotients of Shimura curves*. PhD Thesis, Harvard University, 2003.

[Cla09] P. Clark. On the Hasse principle for Shimura curves. *Israel J. Math.*, 171(1):349–365, 2009.

[CQ05] G. Cardona and J. Quer. Field of moduli and field of definition for curves of genus 2. In *Computational aspects of algebraic curves*, volume 13 of *Lecture Notes Ser. Comput.*, pages 71–83. World Scientific, 2005.

[CT86] J.-L. Colliot-Thélène. Surfaces cubiques diagonales. In *Séminaire de Théorie des Nombres de Paris 1984-1985*, volume 63 of *Progress in Math.*, pages 51–66. Birkhäuser, 1986.

[CTKS87] J.-L. Colliot-Thélène, D. Kanevsky, and J.-J. Sansuc. Arithmétique des Surfaces Cubiques Diagonales. In *Diophantine approximation and transcendence theory (Bonn 1985)*, volume 1290 of *Lecture Notes in Math.*, pages 1–108. Springer, Berlin, 1987.

[Dar03] H. Darmon. *Rational points on modular elliptic curves*, volume 101 of *CBMS Regional Conference Series in Mathematics*. American Mathematical Society, Providence, RI, 2003.

[Del71] P. Deligne. Travaux de Shimura. In *Séminaire Bourbaki, 23ème année (1970/71), Exp. No. 389*, volume 244 of *Lecture Notes in Math.*, pages 123–165. Springer, 1971.

[Dem09] C. Demarche. Obstruction de descente et obstruction de Brauer-Manin étale. *Algebra and Number Theory*, 3(2):237–254, 2009.

[DI95] F. Diamond and J. Im. Modular forms and modular curves. In V. K. Murty, editor, *Seminar on Fermat's Last Theorem (Fields Institute for Research in Mathematical Sciences, Toronto, ON, 1993-1994)*, volume 17 of *CMS Conference Proceedings*, pages 39–133. AMS, Providence, RI, 1995.

[Dri76] V. G. Drinfeld. Coverings of p-adic symmetric regions. *Functional Analysis and its Applications*, 10(2):29–40, 1976.

[ES01] J. S. Ellenberg and C. Skinner. On the modularity of $\mathbb{Q}$-curves. *Duke Math. J.*, 109:97–122, 2001.

[Fal83] G. Faltings. Endlichkeissätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983. English translation: pp. 9-27 in Arithmetic geometry, eds. G. Cornell and J. Silverman, Springer-Verlag, New York-Berlin, 1986.

[FM14] C. Franc and M. Masdeu. Computing fundamental domains for the Bruhat-Tits tree for $\mathrm{GL}_2(\mathbb{Q}_p)$, p-adic automorphic forms, and the canonical embedding of Shimura curves. *LMS J. Comp. Math.*, 17(1):1–23, 2014.

[Gil13] F. Gillibert. Points rationnels sur les quotients d'Atkin-Lehner de courbes de Shimura de discriminant pq. *Ann. Inst. Fourier*, 63(4):1613–1649, 2013.

[GR04] J. González and V. Rotger. Equations of Shimura curves of genus two. *Int. Math. Res. Not.*, 14:661–674, 2004.

[GR06] J. González and V. Rotger. Non-elliptic Shimura curves of genus one. *J. Math. Soc. Japan*, 58(4):927–948, 2006.

[GS06] P. Gille and T. Szamuely. *Central Simple Algebras and Galois Cohomology*. Cambridge University Press, 2006.

[Gui10] X. Guitart. *Arithmetic properties of abelian varieties under Galois conjugation*. PhD Thesis, Universitat Politècnica de Catalunya, 2010.

[GZ86] B. H. Gross and D. B. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84(2):225–320, 1986.

[Har02] D. Harari. Groupes algébriques et points rationnels. *Math. Ann.*, 322(4):811–826, 2002.

[Isk71] V. A. Iskovskih. A counterexample to the Hasse principle for systems of two quadratic forms in five variables. *Mat. Zametki*, 10:253–257, 1971. In Russian.

[JL85] B. Jordan and R. Livné. Local diophantine properties of Shimura curves. *Math. Ann.*, 270:235–248, 1985.

[Jor81] B. W. Jordan. *On the Diophantine Arithmetic of Shimura curves*. PhD Thesis, Harvard University, 1981.

[Jor86] B. W. Jordan. Points on Shimura curves rational over number fields. *J. Reine Angew. Math.*, 371:92–114, 1986.

[Kat76] N. M. Katz. p-adic Interpolation of Real Analytic Eisenstein Series. *Ann. of Math.*, 104(3):459–571, 1976.

[Ken81] M. A. Kenku. On the modular curves $X_0(125)$, $X_1(25)$ and $X_1(49)$. *J. London Math. Soc.*, 23(2):415–427, 1981.

[KM88] M. A. Kenku and F. Momose. Automorphism groups of the modular curves $X_0(N)$. *Compos. Math.*, 60:51–80, 1988.

[Kol90] V. Kolyvagin. Euler Systems. In *The Grothendieck Festschrift (vol. II)*, volume 87 of *Progress in Math.*, pages 435–483. Birkhäuser, 1990.

[KR08] A. Kontogeorgis and V. Rotger. On the non-existence of exceptional automorphisms on Shimura curves. *Bull. London Math. Soc.*, 40:363–374, 2008.

[Kur79] A. Kurihara. On some examples of equations defining Shimura curves and the Mumford uniformization. *J. Fac. Sci. Univ. Tokyo, Sec. IA*, 25:277–301, 1979.

[Lin40] C.-E. Lind. Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Eins, 1940. Diss. Univ. Uppsala.

[LRV] M. Longo, V. Rotger, and C. de Vera-Piquero. Étale coverings of Drinfeld's p-adic upper half plane and the effective computation of Heegner points. In progress.

[Mat70] Yu. Matiyasevich. The Diophantineness of enumerable sets (in Russian). *Dokl. Akad. Nauk SSSR*, 191:279–282, 1970.

[Maz77] B. Mazur. Modular curves and the Eisenstein ideal. *Publ. Math. IHES*, 47:33–186, 1977.

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

[Mic81] J. F. Michon. Courbes de Shimura hyperelliptiques. *Bull. Soc. Math. Fr.*, 109(2):217–225, 1981.

[Mil72] J. S. Milne. Abelian varieties defined over their fields of moduli. I. *Bull. London Math. Soc.*, 4:370–372, 1972.

[Mil74] J. S. Milne. Correction: "Abelian varieties defined over their fields of moduli. I" (Bull. London Math. Soc. 4:370-372, 1972). *Bull. London Math. Soc.*, 6:145–146, 1974.

[Mil79] J. S. Milne. Points on Shimura varieties mod p. *Proc. Symp. Pure Math.*, 33:165–184, 1979.

[Mil80] J. S. Milne. *Étale cohomology*, volume 33 of *PMS*. Princeton University Press, 1980.

[Mil86] J. S. Milne. Abelian varieties. In G. Cornell and J. H. Silverman, editors, *Arithmetic geometry*, pages 103–150. Springer-Verlag, 1986.

[Mil04] J. S. Milne. Introduction to Shimura varieties, 2004. Available at www.jmilne.org/math/.

[Mil08] J. S. Milne. Abelian varieties (v2.00), 2008. Available at www.jmilne.org/math/.

[Miy89] T. Miyake. *Modular forms*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 1989. Translated from the Japanese by Yoshitaka Maeda.

[Mol12] S. Molina. Equations of hyperelliptic Shimura curves. *Proceedings of the LMS*, 105(5):891–920, 2012.

[Mom84] F. Momose. Rational points on the modular curves $X_{\mathrm{split}}(p)$. *Compositio Math.*, 52(1):115–137, 1984.

[Mom87] F. Momose. Rational points on the modular curves $X_0^+(N)$. *J. Math. Soc. Japan*, 39(2):269–286, 1987.

[Mor22] L. J. Mordell. On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proc. Cambridge Phil. Soc.*, 21:179–192, 1922.

[Mor81] Y. Morita. Reduction modulo $\mathfrak{P}$ of Shimura curves. *Hokkaido Math. J.*, 10:209–238, 1981.

[Mum70] D. Mumford. *Abelian Varieties*. Oxford University Press, 1970.

[Mum72] D. Mumford. An analytic construction of degenerating curves over complete local rings. *Compositio Math.*, 24:129–174, 1972.

[Ogg77] A. P. Ogg. Über die automorphismengruppe von $X_0(N)$. *Math. Ann.*, 228:279–292, 1977.

[Ogg83] A. P. Ogg. Real points on Shimura curves. In *Arithmetic and geometry*, volume 35 of *Progress in Math.*, pages 277–307. Birkhäuser, 1983.

[Ogg85] A. P. Ogg. Mauvaise réduction des courbes de Shimura. In *Séminaire de théorie des nombres, Paris 1983-84*, volume 59 of *Progress in Math.*, pages 199–217. Birkhäuser, 1985.

[Oht74] M. Ohta. On ℓ-adic representations of galois groups obtained from certain two dimensional abelian varieties. *J. Fac. Sci. Univ. Tokyo IA*, 21:299–308, 1974.

[Pie82] R. S. Pierce. *Associative Algebras*, volume 88 of *Graduate Texts in Mathematics*. Springer-Verlag, 1982.

[Poo06] B. Poonen. Heuristics for the Brauer-Manin obstruction for curves. *Experimental Math.*, 15(4):415–420, 2006.

[Poo13] B. Poonen. Rational points on varieties, 2013. Course notes, available at http://www-math.mit.edu/~poonen/papers/Qpoints.pdf.

[PS14] B. Poonen and M. Stoll. Most odd degree hyperelliptic curves have only one rational point, 2014. Preprint, `arXiv:1302.0061v3`.

[PV04] B. Poonen and F. Voloch. Random Diophantine equations. In *Arithmetic of higher-dimensional algebraic varieties (Palo Alto, CA, 2002)*, pages 175–184, 2004.

[PY07] P. Parent and A. Yafaev. Proving the triviality of rational points on Atkin-Lehner quotients of Shimura curves. *Math. Ann.*, 339:915–935, 2007.

[Pyl02] E. Pyle. Abelian varieties over $\mathbb{Q}$ with large endomorphism algebras and their simple components over $\bar{\mathbb{Q}}$. In J. Cremona, J.-C. Lario, J. Quer, and K. Ribet, editors, *Modular curves and abelian varieties*, volume 224 of *Progress in Math.*, pages 189–239. Birkhäuser, 2002.

[Rei42] H. Reichardt. Einige im Kleinen überall lösbare, im Großen unlösbare diophantische Gleichungen. *J. Reine Angew Math.*, 184:12–18, 1942.

[Rib92] K. A. Ribet. Abelian varieties over $\mathbb{Q}$ and modular forms. In *1992 Proceedings of KAIST Mathematics Workshop*, pages 53–79. Korea Advanced Institute of Science and Technology, Taejon, 1992. Reprinted in J. Cremona, J.-C. Lario, J. Quer, and K. Ribet, editors, *Modular curves and abelian varieties*, volume 224 of *Progress in Math.*, pp. 241-261.

[Rot02] V. Rotger. On the Group of Automorphisms of Shimura Curves and Applications. *Compos. Math.*, 132:229–241, 2002.

[Rot03] V. Rotger. Quaternions, polarizations and class numbers. *J. Reine Angew Math.*, 561, 2003.

[Rot04a] V. Rotger. The field of moduli of quaternionic multiplication on abelian varieties. *International J. Math. M. Sc.*, 52:2795–2808, 2004.

[Rot04b] V. Rotger. Modular Shimura varieties and forgetful maps. *Trans. Amer. Math. Soc.*, 356:1535–1550, 2004.

[Rot08] V. Rotger. Which quaternion algebras act on a modular abelian variety? *Math. Res. Letters*, 15:251–263, 2008.

[RSY05] V. Rotger, A. Skorobogatov, and A. Yafaev. Failure of the Hasse principle for Atkin-Lehner quotients of Shimura curves over $\mathbb{Q}$. *Moscow Math. J.*, 5(2):463–476, 2005.

[RV14] V. Rotger and C. de Vera-Piquero. Galois representations over fields of moduli and rational points on Shimura curves. *Canad. J. Math.*, 66:1167–1200, 2014.

[Sel51] E. Selmer. The diophantine equation $ax^3 + by^3 + cz^3 = 0$. *Acta Math.*, 85:203–362, 1951.

[Ser72] J.-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15:259–331, 1972.

[Ser73] J.-P. Serre. *A course in Arithmetic*. Springer-Verlag, 1973.

[Ser79] J.-P. Serre. *Local Fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, 1979.

[Shi63] G. Shimura. On Analytic Families of Polarized Abelian Varieties and Automorphic Functions. *Ann. of Math.*, 78:149–192, 1963.

[Shi67] G. Shimura. Construction of Class Fields and Zeta Functions of Algebraic Curves. *Ann. of Math.*, 85:58–159, 1967.

[Shi72] G. Shimura. On the field of rationality for an abelian variety. *Nagoya Math. J.*, 45:161–178, 1972.

[Shi75] G. Shimura. On the Real Points of an Arithmetic Quotient of a Bounded Symmetric Domain. *Math. Ann.*, 215:259–331, 1975.

[Sil86] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, 1986.

[Sil92] A. Silverberg. Fields of definition for homomorphisms of abelian varieties. *J. Pure Appl. Algebra*, 77:253–262, 1992.

[Sko99] A. Skorobogatov. Beyond the Manin obstruction. *Invent. Math.*, 135(2):399–424, 1999.

[Sko01] A. Skorobogatov. *Torsors and Rational Points*, volume 144 of *Cambridge tracts in mathematics*. Cambridge University Press, 2001.

[Sko05] A. Skorobogatov. Shimura coverings of Shimura curves and the Manin obstruction. *Math. Res. Lett.*, 12(5-6):779–788, 2005.

[Sko09] A. Skorobogatov. Descent obstruction is equivalent to étale Brauer-Manin obstruction. *Math. Ann.*, 344:501–510, 2009.

[ST68] J.-P. Serre and J. Tate. Good reduction of abelian varieties. *Ann. of Math.*, 88:492–517, 1968.

[Sto07] M. Stoll. Finite descent obstructions and rational points on curves. *Algebra and Number Theory*, 1(4):349–391, 2007.

[SY04] A. Skorobogatov and A. Yafaev. Descent on certain Shimura curves. *Israel J. Math.*, 140:319–332, 2004.

[Tei90] J. Teitelbaum. Geometry of an étale covering of the p-adic upper half plane. *Ann. Inst. Fourier*, 40(1):69–78, 1990.

[Tei98] J. Teitelbaum. On Drinfeld's universal formal group over the p-adic upper half plane. *Math. Ann.*, 284:647–674, 1998.

[TW95] R. Taylor and A. Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math.*, 141:553–572, 1995.

[Vera] C. de Vera-Piquero. Atkin-Lehner quotients of Shimura curves violating the Hasse principle. In progress.

[Verb] C. de Vera-Piquero. Local points on Shimura coverings of Shimura curves at bad reduction primes. Submitted.

[Ver13] C. de Vera-Piquero. The Shimura covering of a Shimura curve: automorphisms and étale subcoverings. *J. Number Theory*, 133(10):3500–3516, 2013.

[Vig80] M.-F. Vignéras. *Arithmétique des algèbres de quaternions*, volume 800 of *Lect. Notes Math.* Springer, 1980.

[VW14] J. Voight and J. Willis. Computing power series expansions of modular forms. In G. Boeckle and G. Wiese, editors, *Computations with modular forms*, volume 6 of *Contrib. Math. Comput. Sci.*, pages 331–361. Springer, Berlin, 2014.

[Wei56] A. Weil. The field of definition of a variety. *Amer. J. Math.*, 78:509–524, 1956.

[Wil95] A. Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math.*, 142(3):443–551, 1995.