MASTER'S DEGREE THESIS

MSc in Applied Mathematics

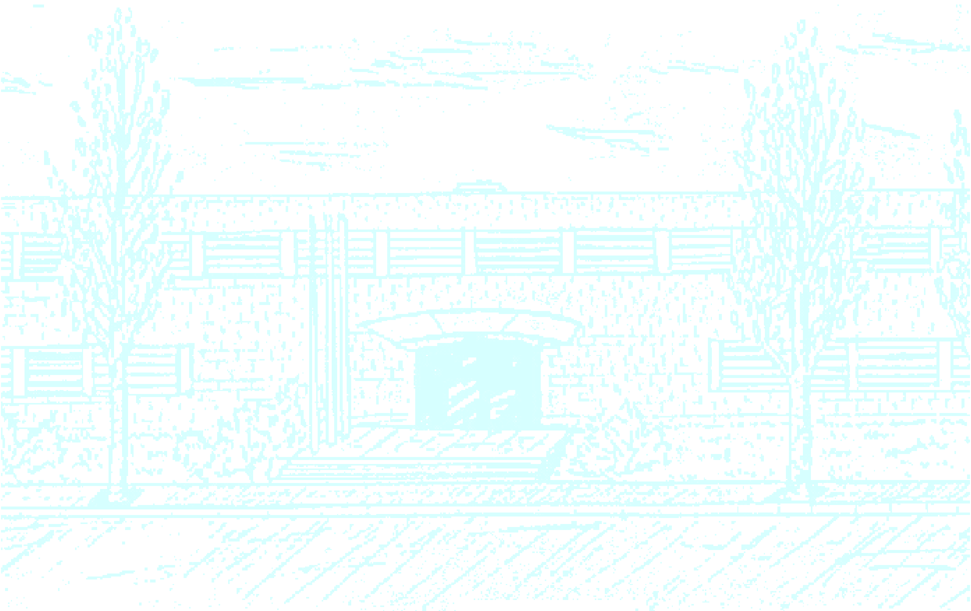
Title: Rational points on Atkin-Lehner quotients of Shimura curves

Author: Carlos de Vera Piquero

Advisor: Víctor Rotger Cerdà

Department: Matemàtica Aplicada II

Academic year: 2010/2011



UPC

Facultat de Matemàtiques i Estadística

UNIVERSITAT POLITÈCNICA DE CATALUNYA

Universitat Politècnica de Catalunya
Facultat de Matemàtiques i Estadística

Master's Degree Thesis

Rational points on Atkin-Lehner quotients of Shimura curves

Carlos de Vera Piquero

Advisor: Víctor Rotger Cerdà

Departament de Matemàtica Aplicada II

Abstract

Keywords: Abelian variety, Shimura variety, modular, Galois representation, Hasse principle.

MSC2010: 11G18, 14G35, 14G05.

Let X_B be the Shimura curve defined by an indefinite rational quaternion division algebra B. By the work of G. Shimura, the curve X_B admits a canonical model over $\mathbb{Q}$ as a coarse moduli solution to the moduli problem of classifying abelian surfaces with quaternionic multiplication by B. Shimura also proved that $X_B(\mathbb{R}) = \emptyset$, so that X_B cannot have rational points over any totally real number field. Going a step further, if K is an imaginary quadratic field, it follows from the work of B. W. Jordan [**Jor86**] that $X_B(K) = \emptyset$ for infinitely many choices of the algebra B. Moreover, Jordan's results provide families of counterexamples to the Hasse principle. More recently, A. N. Skorobogatov [**Sko05**] interpreted these results in terms of descent and, as a consequence, he found that the counterexamples to the Hasse principle derived from [**Jor86**] are accounted for by the Brauer-Manin obstruction. More precisely, he interprets Jordan's results on the non-existence of global points on X_B in terms of the descent performed on a certain X_B-torsor, which is defined from the 'Shimura covering' $X_{B,p}$ of X_B attached to a prime factor of $\mathrm{disc}(B)$ introduced in [**Jor81**].

On the other hand, the Shimura curve X_B is equipped with a natural supply of involutions, classically introduced by A. O. Atkin and J. Lehner. Although $X_B(\mathbb{Q}) = \emptyset$ by Shimura, the quotients $X_B^{(m)}$ of X_B by certain Atkin-Lehner involutions ω_m can have rational points. Indeed, if ω_m is a *twisting* involution then $X_B^{(m)}$ is a solution to the moduli problem of classifying abelian surfaces with real multiplication by $\mathbb{Q}(\sqrt{m})$ and admitting quaternionic multiplication by B. Using this modular interpretation, the main aim of this thesis is to study the Hasse principle over $\mathbb{Q}$ on these quotients. This is done by applying the ideas of Skorobogatov to a suitable $X_B^{(m)}$-torsor constructed by lifting the Atkin-Lehner involution ω_m to the Shimura covering $X_{B,p}$, and relating it to (suitable *extensions* of) the Galois representations attached to the abelian surfaces parametrized by $X_B^{(m)}$ used in [**Rot08**] by V. Rotger. Our main result gives some sufficient conditions for a pair (B, m) to satisfy $X_B^{(m)}(\mathbb{Q}) = \emptyset$, and under some extra conditions also to satisfy $X_B^{(m)}(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}} = \emptyset$. When $X_B^{(m)}(\mathbb{A}_\mathbb{Q}) \neq \emptyset$, these counterexamples to the Hasse principle are then accounted for by the Brauer-Manin obstruction.

Contents

Introduction

The problem of solving diophantine equations over the integers often reduces to the problem of finding rational points on an algebraic curve, that is, points on a curve with rational coordinates. Despite big efforts since the ancient Greeks, it is still not known whether there is a general algorithm that given the equation of a curve returns a list of its rational points, if the list is finite. Even if we know that the curve has infinitely many rational points, computing one of them with some desired property can be an extremely difficult task: for example, there is no general algorithm to compute a point of infinite order in an elliptic curve of positive rank, which is a problem closely related to the famous and still open Birch and Swinnerton-Dyer conjecture.

On the other hand, given an algebraic curve X we can try to prove that it has no rational points, that is, $X(\mathbb{Q}) = \emptyset$. Since a point in $X(\mathbb{Q})$ would define a point in $X(\mathbb{Q}_p)$ for every prime $p \leq \infty$ (being $\mathbb{Q}_\infty = \mathbb{R}$ as usual), it is clear that if $X(\mathbb{Q}_p)$ is empty for some prime p then $X(\mathbb{Q})$ must be empty as well. If this happens, it is said that *there is a local-global obstruction* to the existence of rational points on X. Indeed, a family of curves is said to satisfy the *Hasse principle* (or *local-global principle*) if every curve X in the family satisfies that $X(\mathbb{Q}) \neq \emptyset$ if and only if $X(\mathbb{Q}_p) \neq \emptyset$ for every prime $p \leq \infty$. When the Hasse principle is satisfied, there exists an algorithm which decides whether $X(\mathbb{Q})$ is empty or not in finitely many steps. For example, after the Hasse-Minkowski Theorem, every curve defined by a quadratic equation satisfies the Hasse principle. But, unfortunately, there are many counterexamples to the Hasse principle in the literature. One of the first curves violating the Hasse principle was found by Lind and Reichardt around 1940, independently, and it is the curve given by the affine equation

$$y^2 = x^4 - 17.$$

Selmer showed that the curve $3x^3 + 4y^3 + 5z^3 = 0$ is also a counterexample to the Hasse principle. Nowadays, this curve is known as the *Selmer cubic.*

In this work we focus on Shimura curves and some Atkin-Lehner quotients of them, and try to explain some counterexamples to the Hasse principle by the so-called Brauer-Manin obstruction. In the last decades, Shimura curves have appeared as a key object in several modularity questions, involved for example in Fermat's Last Theorem. And, currently, they are one of the main ingredients in some contributions to the Birch and Swinnerton-Dyer conjecture.

So let B be an indefinite quaternion division algebra over $\mathbb{Q}$ of reduced discriminant $D > 1$. Since all maximal orders in B are conjugate, let us fix one of them and denote it by $\mathcal{O}$. Then, under the isomorphism $B \otimes_{\mathbb{Q}} \mathbb{R} \simeq M_2(\mathbb{R})$, we can regard the subgroup

$$\mathcal{O}^1 = \{\gamma \in \mathcal{O}^\times : n(\gamma) = 1\} \subset \mathcal{O}^\times$$

of units of reduced norm 1 in $\mathcal{O}^\times$ as an arithmetic subgroup Γ_B of $\mathrm{SL}_2(\mathbb{R})$. If $\mathfrak{H}$ denotes the Poincaré upper half plane, then by the work of G. Shimura the compact Riemann surface $\Gamma_B \setminus \mathfrak{H}$ is the set of complex points of an algebraic curve X_B defined over $\mathbb{Q}$. Moreover, the so-called Shimura curve X_B is the coarse moduli scheme over $\mathbb{Q}$ which classifies isomorphism classes of abelian surfaces with quaternionic multiplication by $\mathcal{O}$ (or QM-abelian surfaces, for short), that is, of pairs (A,ι) where A is an abelian surface and $\iota : \mathcal{O} \hookrightarrow \mathrm{End}(A)$ is a ring monomorphism. Then, for a field k of characteristic zero the set of k-rational points $X_B(k)$ is identified with the set of isomorphism classes of QM-abelian surfaces defined over $\bar{k}$ whose field of moduli is contained in k, rather than defined over k.

B. W. Jordan proved in [**Jor86**] that a QM-abelian surface (A,ι) corresponding to a point $P \in X_B(k)$ admits a model rational over k if and only if k splits the quaternion algebra B. Then, assuming that a number field K splits B, he studied also one of the main problems in the arithmetic of these Shimura curves, namely that of deciding whether $X_B(K)$ is empty or not. In other words, whether there exists a QM-abelian surface defined over K or not. In this direction, he proved for example that if K is imaginary quadratic of class number not equal to 1, then there exist only finitely many quaternion algebras B such that $X_B(K) \neq \emptyset$. Moreover, from Jordan's results it follows that Shimura curves provide many counterexamples to the Hasse principle over imaginary quadratic fields.

More recently, A. N. Skorobogatov [**Sko05**] has interpreted Jordan's work in terms of descent, by considering the 'Shimura covering' of X_B attached to a prime factor p of D, which was already introduced by Jordan in his PhD. Thesis [**Jor81**]. With a slightly different approach, Skorobogatov interprets Jordan's results on the non-existence of global points on X_B in terms of the descent performed on a certain X_B-torsor. This leads him to explain all the counterexamples to the Hasse principle derived from [**Jor86**] in terms of the Brauer-Manin obstruction.

For example, consider a prime number $q \neq 2$ and let $\mathcal{B}(q)$ be the set of rational indefinite quaternion algebras which are not split by $\mathbb{Q}(\sqrt{-q})$. Then, for a certain finite set of primes $P(q)$, the next result of Skorobogatov strengthens a theorem of Jordan (see Theorem 4.5 below):

Theorem 0.1 (Skorobogatov)**.** *Let K be an imaginary quadratic field in which a prime $q \neq 2$ is ramified, and assume that $B \in \mathcal{B}(q)$ has reduced discriminant divisible by a prime $p \notin P(q)$. If X_B is the Shimura curve attached to B, then $X(\mathbb{A}_K)^{\mathrm{Br}} = \emptyset$.*

The two articles [**Jor86**] and [**Sko05**] are the seeds of this thesis, together with the inspiring work of V. Rotger in [**Rot04b**] and [**Rot08**].

From the definition of the Shimura curve X_B, there is a naturally defined group of rational involutions acting on X_B, namely the Atkin-Lehner group of the order $\mathcal{O}$. The elements in this group, the so-called Atkin-Lehner involutions, are indexed by the positive divisors of D. From the work in [**Rot04b**], where forgetful maps from higher-dimensional Shimura varieties to Hilbert-Blumenthal varieties are studied, it follows that the quotient $X_B^{(m)} := X_B/\langle\omega_m\rangle$ of the Shimura curve X_B by a *twisting* Atkin-Lehner involution ω_m corresponding to a divisor m of D is a solution to the moduli problem of classifying abelian surfaces with real multiplication by the ring of integers $R_{\mathbb{Q}(\sqrt{m})}$ of $\mathbb{Q}(\sqrt{m})$, admitting quaternionic multiplication by $\mathcal{O}$. Therefore, when ω_m is twisting we can study questions about the existence of $\mathbb{Q}$-rational points on $X_B^{(m)}$ in terms of the existence of these abelian surfaces. This modular point of view makes interesting the study of the set $X_B^{(m)}(\mathbb{Q})$ when ω_m is twisting, as well as it gives us a powerful tool to do it.

In this direction, some necessary conditions are given in [**Rot08**] to prevent an abelian variety of dimension g admitting quaternionic multiplication from having real multiplication by an order in a number field of degree g defined over $\mathbb{Q}$. This is accomplished by studying the Galois representations arising from the Galois action on the torsion points of the abelian variety. In the particular case of dimension $g = 2$, these results can be read as results about the non-existence of $\mathbb{Q}$-rational points on $X_B^{(m)}$. Then, our main goal is to prove a result similar to Theorem 0.1 for Atkin-Lehner quotients of X_B by twisting involutions, in which the field K is replaced by the field $\mathbb{Q}$ of rational numbers.

We show that a cyclic étale covering of $X_B^{(m)}$ can be defined for each prime p of D, by lifting the Atkin-Lehner involution ω_m to the Shimura covering of X_B attached to p. In particular, we obtain an $X_B^{(m)}$-torsor that can be used to apply descent techniques. Using the ideas of Skorobogatov, the characters defined by specialization of this torsor can be related to certain Galois representations as those studied by Rotger to give a result similar to Theorem 0.1.

Indeed, one of the main achievements in this work is that, given an abelian surface parametrized by $X_B^{(m)}(\mathbb{Q}_\ell)$, for some prime ℓ, we can extend the corresponding Galois representations analogous to those appearing in [**Rot08**] to Galois representations on the whole absolute Galois group $\mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$, even in the case where the abelian surface does not admit a model rational over $\mathbb{Q}_\ell$. These *extended* Galois representations are constructed by studying carefully the relation between the field of moduli and the fields of definition of the abelian surfaces parametrized by $X_B^{(m)}(\mathbb{Q}_\ell)$.

This thesis is organized as follows. In the first chapter, we review some elementary topics for the rest of the exposition: abelian varieties, quaternion algebras and the Brauer group of a field. The second chapter contains the essential theory regarding quaternionic Shimura varieties to be used along the work. Although we are interested especially in Shimura curves, a general framework is presented, giving a particular attention to the Atkin-Lehner group and its subgroup of twisting involutions. Using the results of [**Rot04b**], especially the one quoted in Theorem 2.31, we show that the quotient $X_B^{(m)}$ of the Shimura curve X_B by a twisting involution parametrizes isomorphism classes of abelian surfaces with real multiplication by the ring of integers $R_{\mathbb{Q}(\sqrt{m})}$ of $\mathbb{Q}(\sqrt{m})$, admitting quaternionic multiplication by $\mathcal{O}$ (see Proposition 2.33).

Chapter 3 is a brief exposition of some notions and results for the study of obstructions to the existence of rational points on algebraic varieties. One of the central parts of this chapter is the introduction of the Brauer-Manin obstruction to the Hasse principle, which is compared with the descent obstruction. We would also like to emphasize the important role that the main theorem of descent theory of J.-L. Colliot-Thélène and J.-J. Sansuc, quoted in Theorem 3.32, plays in later sections.

Chapters 4 and 5 are mainly devoted to review the works [**Jor86**] and [**Sko05**], respectively. In Chapter 4, moreover, we explain in detail two main ingredients in Jordan's results: the canonical torsion subgroups of a QM-abelian surface and the canonical isogeny characters, as well as the Shimura covering of X_B attached to a prime factor p of D. As for Chapter 5, we show in its second section how to construct a cyclic étale covering of an Atkin-Lehner quotient of X_B from its Shimura covering at p. Closing the chapter, a precise statement of our main result is given in advance (see Theorem 5.10).

Finally, chapters 6 and 7 develop all the machinery that is needed for the proof of our main result, which is given in Theorem 7.31. In Chapter 6 we study the relation between the field of moduli and the field of definition of an abelian surface parametrized by $X_B^{(m)}$. Some known results are presented for the case where the abelian surface corresponds to a point in $X_B^{(m)}(\mathbb{Q})$, like Theorem 6.3 (which appears in [**BFGR06**]), which we generalize later for the case where $\mathbb{Q}$ is replaced by $\mathbb{Q}_\ell$ for a prime ℓ (see Theorem 6.9).

In Chapter 7, this study will allow us to prove a first approach to our main result in Theorem 7.19, under a condition regarding the field of definition of the abelian surfaces parametrized by $X_B^{(m)}(\mathbb{Q}_\ell)$, for some primes ℓ (in fact, for just a couple of primes). This will be done by combining the ideas from [**Sko05**] and [**Rot08**], relating the Galois representations attached to the abelian surfaces parametrized by $X_B^{(m)}(\mathbb{Q}_\ell)$ to the local characters attached to the points in $X_B^{(m)}(\mathbb{Q}_\ell)$ by specialization of a suitable torsor. At the end of Chapter 7, we will introduce the above mentioned *extended* Galois representations, which will be used to finally get a proof of our main result in Theorem 7.31 'à la Skorobogatov'.

Agraïments. En primer lloc, voldria agrair molt sincerament al meu tutor, el Víctor Rotger, la seva ajuda i dedicació al llarg d'aquests mesos. Per compartir les seves idees matemàtiques, i també per la seva paciència i complicitat, sense les quals aquesta tesi no seria possible.

D'altra banda, he d'agrair també als companys de viatge que m'han recolzat durant aquest temps, segurament més del que s'imaginen. Especialment a l'Anna, pels ànims en els moments difícils i pel seu suport incondicional.

Finalment, vull donar les gràcies a la meva família per estar sempre al meu costat i, sobretot, a la meva mare. A ella li vull també dedicar aquest treball.

Chapter 1
Background

The goal of this first chapter is to review some essential material for the rest of the text. We have chosen three main topics, although some other ones could have been included as well.

The first section is devoted to recall the very basic definitions and results about abelian varieties, with special attention to the classification of the ring of endomorphisms of simple abelian varieties. The second section is a brief summary of the general theory of quaternion algebras, containing the basic notions of orders and ideals in both the case of quaternion algebras over local fields and over number fields. Since the Shimura curves we will consider arise as moduli varieties parametrizing abelian varieties with quaternionic multiplication, the review of these topics in this chapter is fully justified.

Finally, we review also the Brauer group of a field. Since for defining the Brauer-Manin obstruction we need to consider the Brauer group of an algebraic variety (or more generally, of a scheme), it is helpful to be familiar first with the Brauer group of a field as a particular case.

In each section of this chapter some general references are given rather than giving an explicit one for each of the results that we state, providing a citation for a particular statement only when we consider it necessary.

1. Abelian varieties

We review here some of the basic facts about abelian varieties, with special emphasis on the study of the endomorphisms of simple abelian varieties.

For the complex theory, in which abelian varieties are the same as polarizable complex tori, a standard reference 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.

Definition 1.1. *An* abelian variety defined over a field k *is 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. Moreover, abelian varieties are nonsingular. Besides, the non-singularity allows us to identify Weil divisors and invertible sheaves.

Recall that a *Weil divisor on A* is a formal sum $D = \sum n_Y Y$ with $n_Y \in \mathbb{Z}$ and subvarieties Y of A of codimension 1. 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 rank 1 sheaf $\mathcal{L}$ on A. The set $\mathrm{Pic}(A)$ of isomorphism classes of invertible sheaves on A has a natural group structure, with the group law being the tensor product of sheaves and for which $\mathcal{O}_A$, the structural sheaf of A, is the identity element. Since A is nonsingular, there is an isomorphism

$$\mathrm{CH}^1(A) \simeq \mathrm{Pic}(A),$$

and we write $\mathcal{L} = \mathcal{O}_A(D)$ for the invertible sheaf associated to a Weil divisor D on A.

Let $\mathcal{L} \in \mathrm{Pic}(A)$ be an invertible sheaf, and write $\mathcal{L} = \mathcal{O}_A(D)$ for a 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

$$\begin{array}{rccc} \Psi_{\mathcal{L}}: & A & \longrightarrow & \mathbb{P}^{n-1} \\ & a & \longmapsto & \{s_1(a), \ldots, s_n(a)\}. \end{array}$$

Definition 1.2. *$\mathcal{L}$ is a* very ample invertible sheaf *if $\Psi_{\mathcal{L}}$ induces a closed immersion. And $\mathcal{L}$ is said to be an* ample invertible sheaf *or a* polarization *if $\mathcal{L}^{\otimes n}$ is very ample for some $n \geq 1$.*

A theorem of S. 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 polarization, 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 *polarized abelian variety.* Observe that from the very definitions:

Proposition 1.3. *An abelian variety is projective if and only if it admits a polarization.*

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

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

By a theorem of Lefschetz, $\mathcal{L}$ is a polarization if and only if H is positive definite, and in this 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 polarized 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 polarization $\mathcal{L}$, 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 polarization $\mathcal{L}$ is *primitive* if $d_1 = 1$, and it is *principal* if $d_1 = \cdots d_g = 1$.

Example 1.4. *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 $\tau \in \mathfrak{H} = \{z \in \mathbb{C} : \Im(z) > 0\}$. Moreover, every one-dimensional complex torus is polarizable, 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 1.5. *The Jacobian of a curve.* If C is an irreducible non-singular curve of genus g over a field k, then $\operatorname{Pic}^0_{\bar{k}}(C)$ is the set of $\bar{k}$-rational points of an abelian variety of dimension g, *the Jacobian of* C. It has a principal polarization:

$$\Theta = \{D \in \operatorname{Pic}^0(C) : h^0(\mathcal{O}_C(D)) = \ell(D) > 0\}$$

is an ample Weil divisor of $\operatorname{Pic}^0(C)$.

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* if the induced map $A(\bar{k}) \to B(\bar{k})$ is a group homomorphism. The set of all homomorphisms from A to B defined over k is denoted by $\operatorname{Hom}_k(A, B)$. It has a group structure in the natural way.

The case of $\operatorname{End}_k(A) = \operatorname{Hom}_k(A, A)$ is of particular interest. The group law in A gives a natural group structure in $\operatorname{End}_k(A)$, which is torsion-free and finitely generated as a $\mathbb{Z}$-module. Moreover, $\operatorname{End}_k(A)$ admits a natural ring structure, in which the product is the composition of endomorphisms. Then $\operatorname{End}_k(A)$ is called the *endomorphism ring* of A. It will be also important later to consider $\operatorname{End}^0_k(A) := \operatorname{End}_k(A) \otimes_{\mathbb{Z}} \mathbb{Q}$, which is a $\mathbb{Q}$-algebra called the *endomorphism algebra* of A.

Remark 1.6. 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. In this direction, we will write $\operatorname{Hom}_K(A, B)$ for $\operatorname{Hom}_K(A_K, B_K)$, where $A_K = A \times_k K$ is the base extension of A to K, and similarly for B_K. Analogously, $\operatorname{End}_K(A)$ stands for $\operatorname{End}_K(A_K)$.

Moreover, it is well-known that given A and B there exists a finite field extension K/k such that K is the smallest field of definition of all the homomorphisms from A to B (see [**Sil92**]).

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 it 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 $\deg(f) = [k(A) : k(B)]$ is by definition the *degree* of f. 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 $A \sim_k B$.

An important property of isogenies is the following: if $f : A \to B$ is an isogeny, then there exists an isogeny $g : B \to A$ and a positive integer n such that $f \circ g = n_B$ is the multiplication by n map on B. This fact implies that isogenies are invertible elements in $\operatorname{End}^0_k(A)$, hence isomorphisms in the category of abelian varieties over k up to isogeny.

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 $x \to nx$ 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 $A(\bar{k})$ of $\bar{k}$-rational points of A. It is well-known that, for a separable closure k^s of k, the kernel $A[n]$ of n_A has a group structure which is as follows:

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

An important property of the torsion groups $A[n]$ is that, since n_A is defined over k, there is a natural action of $\mathrm{Gal}\,(k^s/k)$ on $A[n](k^s)$: if $x \in A[n](k^s)$ then for any $\sigma \in \mathrm{Gal}\,(k^s/k)$ we have also ${}^{\sigma}x \in A[n](k^s)$.

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. Then, the inverse limit $T_\ell(A) = \varprojlim A[\ell^n](k^s)$ is the so-called *ℓ-adic Tate module.* An element $a = (a_n) \in T_\ell(A)$ is a sequence of points $a_n \in A(k^s)$ such that $\ell a_1 = 0$ and $\ell a_n = a_{n-1}$ for every integer $n > 1$.

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 $V_\ell(A)$.

Now consider again a homomorphism $f : A \to B$, which induces a group homomorphism $A[n](k^s) \to A[n](k^s)$ for each integer n, and therefore a $\mathbb{Z}_\ell$-homomorphism $T_\ell(f) : T_\ell(A) \to T_\ell(B)$. In this way, we obtain a map

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

sending $f \in \mathrm{Hom}_k(A, B)$ to $T_\ell(f)$. When $\ell \neq \mathrm{char}(k)$, it can be shown that this map is injective, and it extends to a map

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

In particular, when $A = B$ this 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, $\mathrm{End}_k(A)$ has at most rank $4g^2$ as a $\mathbb{Z}$-module.

If $\ell \neq \mathrm{char}(k)$ and $\phi \in \mathrm{End}_k(A)$, the characteristic polynomial $P_\phi(T)$ of $T_\ell(\phi)$ has integral coefficients and, moreover, it does not depend on the prime ℓ, hence it makes sense to call it *the characteristic polynomial* of ϕ. Then the *degree* and the *trace* of ϕ are defined as usual in terms of $P_\phi(T)$.

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 $\phi \in \mathrm{End}_k^0(A)$.

And finally, the action of $\mathrm{Gal}\,(k^s/k)$ on each group $A[\ell^n](k^s)$ gives a continuous action on $T_\ell(A)$. In other words, we obtain an *ℓ-adic representation* of $\mathrm{Gal}\,(k^s/k)$, that is, a continuous homomorphism

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

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 on 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 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 *polarization* 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 *polarized abelian variety.*

Associated to a polarization $\lambda = \varphi_{\mathcal{L}}$ 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 nonzero $\phi \in \mathrm{End}_k^0(A)$, 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, say that 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 $\bar{k}$.

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

Theorem 1.7. *Let A be an abelian variety over k. There exist k-simple and pairwise non-isogenous abelian varieties $A_1, \dots, A_r$, and positive integers $n_1, \dots, n_r$ 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 $\phi \in \mathrm{End}_k(A)$. The connected component of $\ker(\phi)$ 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 nonzero 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 1.8. *Let A be an abelian variety over k, whose decomposition into k-simple varieties up to isogeny is as in Theorem 1.7. 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 us to use Albert's classification as we now explain briefly.

As before, assume again that A is a k-simple abelian variety with endomorphism algebra $D = \mathrm{End}_k^0(A)$, and admitting a polarization over k. 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 certain polarization 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:

Theorem 1.9. *Let A be a k-simple abelian variety of dimension g. Let F be the center of $D = \operatorname{End}_k^0(A)$, and let $F_0 = \{x \in D : x' = x\}$ be the subfield fixed by the Rosati involution. Define $d = [D : F]^{1/2}$, $e = [F : \mathbb{Q}]$, $e_0 = [F_0 : \mathbb{Q}]$. Then the isomorphism type of D is one of the following four ones:*

- Type I: *$D = F = F_0$ is a totally real number field, and the Rosati involution is the identity. In this case, $e|g$.*
- Type II: *$F = F_0$ is a totally real number field and D is a totally indefinite quaternion division 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 $2e|g$.*
- Type III: *$F = F_0$ is a totally real number field and D is a totally definite quaternion division 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 $e^2|g$.*
- Type 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, $e_0d^2|g$ if $char(k) = 0$, and $e_0d|g$ if $char(k) > 0$.*

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 called of the *first* (resp. *second*) *kind* if the first (resp. second) case holds.

In general, for a non 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 $\operatorname{End}_k^0(A)$ contains a commutative semisimple algebra of dimension $2g$ over $\mathbb{Q}$, which is the maximal dimension of such a subalgebra. If $\operatorname{char}(k) = 0$ and A is k-simple, then A has CM over k if and only if $\operatorname{End}_k^0(A)$ is a CM number field of degree $2g$.

2. Quaternion algebras

Let k be a field. The theory of quaternion algebras over 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 good account in [**Pie82**]. Indeed, the isomorphism classes of quaternion algebras over k correspond to the 2-torsion subgroup of the Brauer group $\operatorname{Br}(k)$ of k. For the specific theory of quaternion algebras the basic reference is [**Vig80**].

2.1. Basic definitions and results.

We start by recalling some generalities about quaternion algebras over a field k.

Definition 1.10. *A* quaternion algebra *B over k is a central simple algebra of rank 4 over k.*

There are two well-known classical constructions describing quaternion algebras. For the first one, let L be a quadratic separable algebra over k,[1] let τ be the non trivial involution on L over k and let $m \in F^\times$ be any invertible element. Then the algebra

$$B = L + Lu, \tag{1}$$

where $u \in B$ is such that

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

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

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

The second construction, which is only valid if $\mathrm{char}(k) \neq 2$, goes as follows. Let $a, b \in k^\times$, and define

$$B = \left(\frac{a,b}{k}\right) = k + ki + kj + kij \tag{2}$$

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 B is again a quaternion algebra over k, and it is also true that any quaternion algebra over k admits a presentation like this. Indeed, observe that $(\frac{a,b}{k}) = \{k(i), b\}$. Assume from now on that $\mathrm{char}(k) \neq 2$, so that we can deal with both descriptions (1) and (2) of quaternion algebras.

Remark 1.11. 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 dissertation about when two quaternion algebras $(\frac{a,b}{k})$ and $(\frac{a',b'}{k})$ are isomorphic.

From the very definition, it follows that if B is a quaternion algebra over k then it has a canonical anti-involution called *conjugation*, which is usually denoted by $\beta \mapsto \bar{\beta}$. If we use the description (1), then it is defined by extending τ to B by $\bar{u} = -u$. And if we take the description (2) and $\beta = x + yi + zj + tij$ then $\bar{\beta} = x - yi - zj - tij$. When we say that $\beta \mapsto \bar{\beta}$ is anti-involuting, we mean that if $\alpha, \beta \in B$ and $x, y \in k$ then

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

Clearly, any element $\beta \in B$ is a root of the quadratic polynomial

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

where

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

are defined as the *reduced trace* and *reduced norm* of β, respectively. In particular, for every $\beta \in B^\times \setminus k^\times$ we have that $k(\beta)/k$ is a quadratic extension. Moreover, when restricted to $k(\beta)$, the conjugation on B coincides with the non trivial k-automorphism of $k(\beta)$, which implies that $\mathrm{tr}(\beta), \mathrm{n}(\beta) \in k$ for every $\beta \in B$ and then the above polynomial lies in $k[X]$. In fact, a quaternion algebra over k is in some sense a bunch of quadratic extensions glued together in a non-commutative way.

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

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

defines an isomorphism $(\frac{1,b}{k}) \simeq \mathrm{M}_2(k)$ for any $b \in k^\times$. If a quaternion algebra B over k is isomorphic to $\mathrm{M}_2(k)$ then B is said to be a *split* algebra, as opposed to the division case.

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

$$\varepsilon(B) = \begin{cases} -1 & \text{if } B \text{ is division,} \\ 1 & \text{if not.} \end{cases}$$

Moreover, this dichotomy can be translated into the theory of quadratic forms, which is therefore strongly related to that of quaternion algebras. It is not difficult to check (see [**Pie82**, §1.6]) that the quaternion algebra $B = (\frac{a,b}{k})$ is a division algebra if and only if the quadratic form $ax^2 + by^2 - z^2 = 0$ has only the trivial solution $x = y = z = 0$ in k^3. It is customary to define the *Hilbert symbol* of the pair (a, b) over k by

$$(a,b)_k = \begin{cases} 1 & \text{if } ax^2+by^2-z^2=0 \text{ has non trivial solutions in } k^3, \\ -1 & \text{if not.} \end{cases}$$

Then, by the above quoted result $(a, b)_k = \varepsilon((\frac{a,b}{k}))$.

Remark 1.13. As for the relation between quaternion algebras and quadratic forms, there is a good treatment in [**AB04**]. From the study of CM points in Shimura curves, a classification of binary quadratic forms with algebraic coefficients by arithmetic Fuchsian groups is presented, recovering Gauss' theory on the classification of binary quadratic forms with integral coefficients by the action of the modular group.

Matrix algebras play also an important role in the notion of *splitting field*: a field extension K/k is said to be a splitting field for a quaternion algebra B over k if the quaternion algebra $B \otimes_k K$ over K obtained by extension of scalars is split (i.e. isomorphic to $\mathrm{M}_2(K)$). By [**Vig80**, Théorème I.2.8], a quadratic extension K/k splits the algebra B if and only if K is isomorphic to a maximal subfield of B. If a field K splits the algebra B, then by means of the natural inclusion $B \hookrightarrow B \otimes_k K \simeq \mathrm{M}_2(K)$ the reduced trace and the reduced norm of an element $\beta \in B$ can be computed inside $\mathrm{M}_2(K)$ as the usual trace and determinant, respectively.

Given a field k, the problem of classifying the isomorphism classes of quaternion algebras over k naturally arises. In view of the remark after Example 1.12, it suffices to classify division quaternion algebras over k. Let us give two important examples.

Example 1.14. In 1843, W. R. Hamilton discovered that the real algebra $\mathbb{H}$ of rank 4 generated by elements i, j satisfying $i^2 = j^2 = -1$, $ij = -ji$, is a non-commutative division algebra. In our notation, it corresponds to the quaternion algebra $(\frac{-1,-1}{\mathbb{R}})$. By the Theorem of Frobenius ([**Vig80**, Corollaire I.2.5], [**Pie82**, Corollary 13.1.c]), the Hamilton quaternion algebra $\mathbb{H}$ is the unique finite-dimensional non-commutative division algebra over $\mathbb{R}$, up to isomorphism. Therefore, any quaternion algebra over $\mathbb{R}$ is isomorphic either to $\mathrm{M}_2(\mathbb{R})$ or to $\mathbb{H}$.

Example 1.15. If k is an algebraically closed field, from Wedderburn's Theorem on the classification of simple algebras one deduces 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 $\mathrm{M}_2(\mathbb{C})$.

2.2. Orders and ideals. The non-commutativity of quaternion algebras make the theory of orders a little bit more subtle than its analogue in number fields. We present here the main definitions and results relating orders and ideals in quaternion algebras for later use. Through the following lines, let R be a Dedekind domain with fraction field k, and let B be a quaternion algebra over k.

As in the number field case, an element $\beta \in B$ is said to be *integral* if $\mathrm{tr}(\beta), \mathrm{n}(\beta) \in R$. But in the case of quaternion algebras it is not true that the set of integral elements of B is a ring. An easy example is given by the following two matrices in the algebra $\mathrm{M}_2(\mathbb{Q})$:

$$A = \begin{pmatrix} \frac{1}{2} & -3 \\ \frac{1}{4} & \frac{1}{2} \end{pmatrix}, \quad B = \begin{pmatrix} 0 & \frac{1}{5} \\ 5 & 0 \end{pmatrix}.$$

Both A and B are integral but neither $A + B$ nor AB is.

Hence, a good way to generalize the notion of order to the context of quaternion algebras is the following:

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. An order $\mathcal{O}$ is an* Eichler order *if it is the intersection of two maximal orders.*

Recall that an R-lattice in B is a torsion-free R-module $\Lambda \subseteq B$. Then, an *R-ideal* (or simply an *ideal*) is an R-lattice I in B such that $I \otimes_R k \simeq B$. An ideal is said to be *integral* if all its elements are integral. According to the above definition, an order is an ideal which is also a ring. For example, if $\{v_1, v_2, v_3, v_4\}$ is a k-basis of B, then $R[v_1, v_2, v_3, v_4]$ is both an ideal and an order in B.

For an ideal I of B, its associated *left* and *right orders* are defined 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 *two-sided* if $\mathcal{O}_\ell(I) = \mathcal{O}_r(I)$, and it is easy to check that

$$I \text{ is integral} \iff II \subseteq I \iff I \subseteq \mathcal{O}_\ell(I), \mathcal{O}_r(I).$$

An ideal I 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

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

Two ideals I, J are *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. Therefore, since orders are ideals, for an order $\mathcal{O}$ we can define $\mathrm{Pic}_\ell(\mathcal{O})$ to be the set of left-ideal classes of $\mathcal{O}$. That is, $\mathrm{Pic}_\ell(\mathcal{O})$ is the set of ideals with right order $\mathcal{O}$ modulo equivalence on the left. Analogously, we could define 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 $\mathcal{O}$, $|\operatorname{Pic}_\ell(\mathcal{O})|$ is called the *class number of $\mathcal{O}$*. It is not difficult to show that all maximal orders have the same class number, so that it makes sense to define the *class number* of B as $h(B) = |\operatorname{Pic}_\ell(\mathcal{O})|$ for any maximal order $\mathcal{O}$.

Given an order $\mathcal{O}$, we can also conjugate it by an element $\beta \in B^\times$ to get again an order. Two orders are said to be of the same *type* if they are conjugate by some $\beta \in B^\times$. Then, the *type number* $t(B)$ of B is the number of conjugacy classes of maximal orders of B. The type number is always less than or equal to the class number, $t(B) \leq h(B)$.

Now, for an ideal I let $n(I)$ denote the fractional R-ideal generated by the reduced norms of elements of I. For an order $\mathcal{O}$, the *different* $d(\mathcal{O})$ is the fractional ideal defined by $d(\mathcal{O}) = (\mathcal{O}^*)^{-1}$, where $\mathcal{O}^* = \{\beta \in B : \operatorname{tr}(\beta\mathcal{O}) \subseteq R\}$. Then the *discriminant* $D(\mathcal{O})$ of the order $\mathcal{O}$ is defined as the norm of the 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 $R\det(\operatorname{tr}(v_iv_j))$.

2.3. Quaternion algebras over local fields. Now we focus on quaternion algebras over local fields. Recall that a field k is said to be a *local field* if it is a finite extension of one of the following fields:

- $\mathbb{R}$, the field of real numbers,
- $\mathbb{Q}_p$, the field of p-adic numbers, for some prime p, or
- $\mathbb{F}_p[[T]]$, the field of formal series in one variable over the finite field $\mathbb{F}_p$ of p elements, for some prime p.

The local fields $\mathbb{R}$ and $\mathbb{C}$ are called *archimedean*, while the rest of them are called *non-archimedean.*

The classification of quaternion algebras over local fields is particularly simple. From Example 1.15, the only quaternion algebra over $\mathbb{C}$ (up to isomorphism) is the matrix algebra $\mathrm{M}_2(\mathbb{C})$. And from Example 1.14, there is only one quaternion division algebra over $\mathbb{R}$ up to isomorphism, namely the Hamilton quaternion algebra $\mathbb{H}$. Being these cases covered, assume from now on that k is a non-archimedean local field.

As is proved in [**Vig80**, §I.1], the Theorem of Frobenius extends to the non-archimedean case, that is, there is only a single quaternion division algebra over k up to isomorphism.

In order to make precise this statement, we need some notation. We denote by R_k the ring of integers of k, and we let π be a prime element in R_k, i.e. such that R_k/π is the residue field of k. We also let L_{nr} be the unique non-ramified quadratic extension of k inside a separable closure k^s of k. Then, 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 announced before admits the following explicit form (cf. [**Vig80**, Théorème II.1.3]):

Theorem 1.17. *The quaternion algebra $H = \{L_{nr}, \pi\}$ is the unique quaternion division algebra over k up to isomorphism. Moreover, a finite extension K/k splits H if and only if its degree $[K : k]$ is even.*

This simple classification of quaternion algebras over local fields results in an easy study of the orders and ideals as well.

Suppose first that B is the split algebra over k, that is, $B \simeq \mathrm{M}_2(k)$. Then, we can think of B as the endomorphism algebra of a two-dimensional k-vector space V and write $B \simeq \mathrm{End}(V)$. 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 Λ_i complete R_k-lattices of V. This implies:

Proposition 1.18. *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 $\mathrm{M}_2(R_k)\pi = \pi\mathrm{M}_2(R_k)$.*

And secondly, assume now that $B = H$ is the unique (up to isomorphism) quaternion division algebra over k from Theorem 1.17. If v is a discrete valuation of k, then it can be extended to a discrete valuation w of B by setting $w(\beta) = v(\mathrm{n}(\beta))$ for $\beta \in B$. In this way, the valuation ring of w is $\mathcal{O} = \{\beta \in B : \mathrm{n}(\beta) \in R_k\}$, which is an order and, since it contains all the integral elements of B, it is a maximal order.

Proposition 1.19. *Let B be a quaternion division algebra over k. Then B contains a unique maximal order, which is $\mathcal{O} = \{\beta \in B : \mathrm{n}(\beta) \in R_k\}$. In particular, it is also the unique Eichler order. Moreover, the ideal πR_k ramifies: $\pi\mathcal{O} = \mathfrak{p}^2$, where $\mathfrak{p}$ is the unique maximal ideal of $\mathcal{O}$.*

2.4. Quaternion algebras over a number field. Now we move on to the case of number fields (more generally, we could consider the case of global fields). Let F be a number field, and denote by R_F its ring of integers. For each place v of F, choose embeddings $F \hookrightarrow F_v$, where F_v stands for the completion of F at v. Recall that the finite places are in bijection with the prime ideals in R_F, the real places correspond to the distinct real embeddings of F and the complex places correspond to the distinct pairs of conjugate complex embeddings of F.

If B is a quaternion algebra over F, then we can define $B_v := B \otimes_F F_v$, which is naturally a quaternion algebra over the local field F_v. Considering these algebras B_v for all the places v and using the results quoted above, we can study global properties of the quaternion algebra B.

From Example 1.15, if v is a complex place of F then $B_v \simeq M_2(\mathbb{C})$. Otherwise, if v is a real or non-archimedean place, then Theorem 1.17 implies that either $B_v \simeq M_2(F_v)$ or $B_v \simeq \mathbb{H}_v$, where $\mathbb{H}_v$ denotes the unique quaternion division algebra over F_v. This fact motivates the following definition:

Definition 1.20. *Let v be a place of F. It is said that v* splits *in B if $B_v \simeq M_2(F_v)$, and it is said that v* ramifies *in B if B_v is division.*

The ramification at the real places will play an important role for us. It is said that B is *totally indefinite* over F if no real place ramifies in B, and that B is *totally definite* over F if every real place ramifies in B. For the case $F = \mathbb{Q}$, we just say B is indefinite, respectively definite, since there is only one real place to check.

Let $\mathrm{Ram}(B)$ denote the set of places of F which ramify in B. The following classification theorem, due to H. Hasse, tells us that this set determines completely B up to isomorphism (cf. [**Vig80**, Théorème III.3.1]):

Theorem 1.21 (Hasse)**.** *The number* $|\mathrm{Ram}(B)|$ *of ramified places in a quaternion algebra* B *over* F *is even. Moreover, for every finite set* S *of places of* F *of even cardinality, there exists a unique quaternion algebra* B *over* F*, up to isomorphism, such that* $\mathrm{Ram}(B) = S$.

In other words, the isomorphism class of a quaternion algebra over a number field is uniquely determined by the (finite) set of ramified places. For a quaternion algebra B over F, the *reduced discriminant* $\mathfrak{D} = \mathrm{disc}(B)$ is the product of the finite places in $\mathrm{Ram}(B)$. Hence, we can regard $\mathfrak{D} = \mathfrak{p}_1 \cdots \mathfrak{p}_s$ as an ideal of R_F, where $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ are pairwise distinct prime ideals of R_F.

Theorem 1.21 is extremely useful. Not only because it gives a clear and precise classification of the quaternion algebras over F, but also because of the quite important corollaries that can be deduced from it. We now explain briefly some of them (see [**Vig80**, pp. 75-76] for details).

The first corollary we want to mention is the so-called *Hasse Principle for quadratic forms*, which can be proved using Theorem 1.21:

Corollary 1.22. *If* f *is a quadratic form over a number field* F*, then* f *is isotropic over* F *if and only if* f *is isotropic over* F_v*, for every place* v *of* F.

The next consequence relates the Hilbert symbols $(\cdot,\cdot)_v := (\cdot,\cdot)_{F_v}$ of the completions of F, and is known as the *reciprocity law of the Hilbert symbol.* In fact, the quadratic reciprocity law can be deduced from it:

Corollary 1.23. *Let* F *be a number field, and for a pair of elements* $a, b \in F^\times$ *denote by* $(a,b)_v = (a,b)_{F_v}$ *their Hilbert symbol relative to* F_v*. Then one has the* product formula

$$\prod_v (a,b)_v = 1,$$

where the product is over all the places v *of* F.

Note that the product in the above formula is in fact a finite product, since by Theorem 1.21 only a finite number of Hilbert symbols are $\neq 1$. In the case where $F = \mathbb{Q}$, an application of the last corollary is the computation of the local Hilbert symbols. For $a, b \in \mathbb{Q}$ and a prime $p \neq 2$, the Hilbert symbol $(a,b)_p$ is easy computed following the recipe in [**Vig80**, p. 37], and then by the product formula

$$(a,b)_2 = \prod_{v \neq 2} (a,b)_v.$$

From Theorem 1.21 there are also two properties which are important by themselves. The first one is the parity of the number of ramified places in a quaternion algebra, and the second one is a characterization of the matrix algebra: a quaternion algebra B over F is isomorphic to $\mathrm{M}_2(F)$ if and only if $B_v \simeq \mathrm{M}_2(F_v)$ for every place v of F. These properties lead to the next two corollaries, regarding the norms in quadratic extensions of F and the splitting fields for the algebra B.

Corollary 1.24. *Let* F *be a number field,* L/F *a quadratic extension and* $\theta \in F^\times$*. Then* θ *is the norm of an element in* L *if and only if* θ *is a norm of an element in* $L_v := L \otimes F_v$ *for every place* v *of* F*, except for possibly one.*

Corollary 1.25. *Let* B *be a quaternion algebra over a number field* F*. A finite field extension* L/F *is a splitting field for* B *if and only if* L_w *is a splitting field for* B_v*, for every place* $w|v$ *of* L.

Before moving into orders and ideals, let us quote an important result characterizing the quadratic subfields of B:

Theorem 1.26. *A quadratic extension L/F is a subfield of the quaternion algebra B if and only if $L_v = L \otimes F_v$ is a field for every $v \in \mathrm{Ram}(B)$.*

Behind the proof of all these results, there is the idea of working "adellically". For the study of orders and ideals it is also the key tool, so that we describe it briefly.

Start by choosing a finite set S of places of F, including the infinite ones, and let

$$R = R_{(S)} = \bigcap_{v \notin S} (R_v \cap F),$$

where $R_v := R_{F,v}$. Then R is a Dedekind domain, and should be regarded as the ring of elements which are integral outside S.

Then consider the general situation in which we are given a locally compact group G_v for each place v of F, and for every place $v \notin S$ we are also given a compact open subgroup C_v of G_v.

Definition 1.27. *With the above notations, the* restricted product $G_{\mathbb{A}}$ *of the groups G_v with respect to the subgroups C_v is*

$$G_{\mathbb{A}} = \{x = (x_v) \in \prod_v G_v : x_v \in C_v \textit{ for almost all } v \notin S\}.$$

The group $G_{\mathbb{A}}$ can be endowed with a topology for which it becomes a locally compact topological group, which moreover do not depend on S. This situation arises when G is an algebraic group defined over F. Then, G_v is the set $G(F_v)$ of F_v-rational points, and C_v is defined to be the set $G(R_v)$ for v outside a finite set S of places of F. Then, the group $G_{\mathbb{A}}$ is called the *group of adèles* of G.

Example 1.28. The *ring of adèles* $\mathbb{A}_F$ of F arises in this way when choosing $G_v = F_v$, $S = \infty$ the set of infinite places and $C_v = R_v$. The group of the invertible elements in $\mathbb{A}_F$ is the *group of idèles* $\mathbb{A}_F^\times$ of F, and arises by choosing $G_v = F_v^\times$, $S = \infty$ and $C_v = R_v^\times$.

Example 1.29. A quaternion algebra B over F also gives rise to some groups of adèles in a similar way. The *ring of adèles* $B_{\mathbb{A}}$ of B is defined by choosing $G_v = B_v$, $S \supseteq \infty$ and $C_v = \mathcal{O}_v$, where $\mathcal{O}$ is an order of B over the ring $R = R_{(S)}$ and $\mathcal{O}_v = \mathcal{O} \otimes_R R_v$. Then $B_{\mathbb{A}}$ is isomorphic to the tensor product $\mathbb{A}_F \otimes_F B$. As it is expected, the group $B_{\mathbb{A}}^\times$ of invertible elements of $B_{\mathbb{A}}$ is obtained by setting $G_v = B_v^\times$, $S \supseteq \infty$ and $C_v = \mathcal{O}_v^\times$.

Now fix the set S of places of the number field F, containing the infinite ones. If $S = \infty$, then note that $R = R_\infty$ is the ring of integers R_F of F.

In order to use the local properties of ideals and orders, if Y is an R-lattice of B, then put $Y_v = Y \otimes_R R_v$. When $v \in S$, then $R_v = F_v$ and $Y_v = B_v$. The key point is that the R-lattice Y is uniquely determined by the local lattices $(Y_v)_{v \notin S}$ (see [**Vig80**, Proposition III.5.1]). Therefore, we have a notion of *local property* concerning ideals (lattices). Namely, a property $\star$ is local if an ideal I satisfies $\star$ if and only if I_v satisfies $\star$ for every $v \notin S$. Examples of local properties of ideals are: being an ideal, being an integral ideal, being an order, being a maximal order, among others.

However, the property of being a principal ideal is not a local property, and this is one of the main reasons for working in the adelic language. An R-lattice Y will be replaced by its localizations $(Y_v)_{v \notin S}$ and we will write

$$Y_{\mathbb{A}} = \prod_v Y_v, \quad \text{with } Y_v = B_v \text{ if } v \in S.$$

We now consider maximal orders in B. Since the ideals whose left and right orders are maximal are locally principal ([**Vig80**, p. 86]), we assume that all the ideals considered are locally principal. Fixed a maximal order $\mathcal{O}$ of B, we can associate to it the following adelic objects:

(i) $\mathcal{O}_{\mathbb{A}}$, the ring of adèles of $\mathcal{O}$,
(ii) $\mathcal{O}_{\mathbb{A}}^{\times}$, the group of units of $\mathcal{O}_{\mathbb{A}}$,
(iii) $N(\mathcal{O}_{\mathbb{A}})$, the normalizer of $\mathcal{O}_{\mathbb{A}}$ inside $B_{\mathbb{A}}^{\times}$.

Then, by means of the map $(x_v) \in B_{\mathbb{A}}^{\times} \mapsto I$, where I is the ideal such that $I_v = \mathcal{O}_v x_v$ if $\notin S$, the set of left $\mathcal{O}$-ideals is in bijection with $\mathcal{O}_{\mathbb{A}}^{\times} \setminus B_{\mathbb{A}}^{\times}$. Hence, the set of two-sided $\mathcal{O}$-ideals is in bijection with $\mathcal{O}_{\mathbb{A}}^{\times} \setminus N(\mathcal{O}_{\mathbb{A}})$. As for the maximal orders, they are in bijection with $N(\mathcal{O}_{\mathbb{A}})/B_{\mathbb{A}}^{\times}$: just send an element $(x_v) \in B_{\mathbb{A}}^{\times}$ to the order $\mathcal{O}'$ such that $\mathcal{O}'_v = x_v^{-1}\mathcal{O}_v x_v$ for $v \notin S$.

In this manner, the following global-adelic dictionary is obtained:

$$\begin{aligned} \text{left } \mathcal{O}\text{-ideals} \quad &\leftrightarrow \quad \mathcal{O}_{\mathbb{A}}^{\times} \setminus B_{\mathbb{A}}^{\times}, \\ \text{two-sided } \mathcal{O}\text{-ideals} \quad &\leftrightarrow \quad \mathcal{O}_{\mathbb{A}}^{\times} \setminus N(\mathcal{O}_{\mathbb{A}}), \\ \text{maximal orders} \quad &\leftrightarrow \quad N(\mathcal{O}_{\mathbb{A}})/B_{\mathbb{A}}^{\times}, \\ \mathrm{Pic}_{\ell}(\mathcal{O}) \quad &\leftrightarrow \quad \mathcal{O}_{\mathbb{A}}^{\times} \setminus B_{\mathbb{A}}^{\times}/B^{\times}, \\ \text{types of maximal orders} \quad &\leftrightarrow \quad B^{\times} \setminus B_{\mathbb{A}}^{\times}/N(\mathcal{O}_{\mathbb{A}}). \end{aligned}$$

In analogy to the commutative theory, it seems natural to expect these sets to be finite, and related to the class number of F, namely the order of $R_{F,\mathbb{A}}^{\times} \setminus \mathbb{A}_F/F^{\times}$. Indeed, the study of the above coset interpretation in the adelic language of maximal orders leads us to the finiteness of the class number:

Theorem 1.30. *Let $\mathcal{O}$ be a maximal order in B. Then* $\mathrm{Pic}_{\ell}(\mathcal{O})$ *is finite, hence the class number and the type number of B are finite.*

Nevertheless, in some cases we can go a step further. Let F_B be the set of elements in F which are positive at the real places ramifying in B. By the Norm Theorem (see [**Vig80**, Théorème III.4.1]), $F_B = \mathrm{n}(B)$. Denote also by P_B the subgroup of the group $Frac(F)$ of fractional ideals of F consisting on the principal ideals generated by an element of F_B, and let h_B be the order of the quotient $Frac(F)/P_B$. Note that $h(F) \leq h_B \leq h^+(F)$, where $h(F)$ and $h^+(F)$ stand for the class number and the narrow class number of F, respectively.

Then, the reduced norm induces a map between double coset spaces

$$\mathcal{O}_{\mathbb{A}}^{\times} \setminus B_{\mathbb{A}}^{\times}/B \longrightarrow R_{\mathbb{A}}^{\times} \setminus \mathbb{A}_F^{\times}/F_B.$$

This map is shown to be a bijection, using the Strong Approximation Theorem (see [**Vig80**, III.4.3]) for injectivity, and leads to the following result, which is a consequence of a Theorem due to M. Eichler:

Theorem 1.31. *Let $\mathcal{O}$ be a maximal order of a not totally definite quaternion algebra B over F. The reduced norm induces a bijection* $\mathrm{Pic}_{\ell}(\mathcal{O}) \to Frac(F)/P_B$. *In particular, the class number of B is h_B.*

When B is a totally indefinite quaternion algebra, the condition defining P_B is empty, so that $P_B = P$, the group of principal ideals of F, and $h_B = h(F)$ coincides with the class number of F. If moreover B is a rational quaternion algebra, since $h(\mathbb{Q}) = 1$:

Corollary 1.32. *The class number of an indefinite rational quaternion algebra is 1. Moreover, all maximal orders in an indefinite rational quaternion algebra are conjugate.*

3. The Brauer group of a field

We introduce the Brauer group $\mathrm{Br}(k)$ of a field k in terms of central simple algebras, recalling the basic definitions and relating the group $\mathrm{Br}(k)$ to the second Galois cohomology group $\mathrm{H}^2(\mathrm{Gal}\,(\bar{k}/k), \bar{k}^{\times})$. We also state the main theorems describing the Brauer group of certain families of fields. For a detailed treatment of the Brauer group of a field, see [**Pie82**] and [**GS06**], for example.

Recall that a k-algebra A is said to be *central* if its center is $Z(A) = k$, and it is called *simple* if it contains no proper two-sided ideals other than 0. Denote by CS_k the set of finite-dimensional central simple algebras over k. In this set, the matrix algebras play an important role, as the next proposition shows.

Proposition 1.33. *For a k-algebra A, the following are equivalent:*

- (i) *A is a finite-dimensional central simple algebra over k.*
- (ii) *The $\bar{k}$-algebra $A \otimes_k \bar{k}$ is isomorphic to $\mathrm{M}_n(\bar{k})$ for some $n \geq 1$.*
- (iii) *The k^s-algebra $A \otimes_k k^s$ is isomorphic to $\mathrm{M}_n(k^s)$ for some $n \geq 1$.*
- (iv) *(Wedderburn's Theorem) There is a k-algebra isomorphism $A \simeq \mathrm{M}_r(D)$ for some integer $r \geq 1$ and some finite-dimensional central division algebra D over k. Here, the integer r and the isomorphism class of D are uniquely determined.*

Moreover, if $A \in \mathrm{CS}_k$ then $A^{op} \in \mathrm{CS}_k$, where A^{op} denotes the opposite algebra of A, and for any field extension L/k, $A \otimes_k L \in \mathrm{CS}_L$. And if $B \in \mathrm{CS}_k$ is another central simple algebra over k, then we have $A \otimes_k B \in \mathrm{CS}_k$. These properties make us think about a group structure in CS_k, for which we have to define first an equivalence relation. For $A, B \in \mathrm{CS}_k$, we say that A and B are similar, and we write $A \sim B$, if one of the following equivalent conditions hold:

- (S1) there are integers $m, n \geq 1$ and a division algebra $D \in \mathrm{CS}_k$ such that $A \simeq \mathrm{M}_m(D)$ and $B \simeq \mathrm{M}_n(D)$;
- (S2) there are integers $m, n \geq 1$ such that $\mathrm{M}_m(A) \simeq \mathrm{M}_n(B)$ as k-algebras.

The relation $\sim$ defines an equivalence relation in the set CS_k, and then we can denote the quotient by

$$\mathrm{Br}(k) := \mathrm{CS}_k / \sim .$$

The operations $A, B \mapsto A \otimes_k B$ and $A \mapsto A^{op}$ on CS_k induce the multiplication and inverse maps for a group structure on $\mathrm{Br}(k)$. Moreover, the similarity class of k as a k-algebra (which is also the class of the matrix algebras $\mathrm{M}_n(k)$) is the identity element for these operations. It turns out that $\mathrm{Br}(k)$ is an abelian group, called the *Brauer group* of k. One can also define $\mathrm{Br}(k)$ as the set of isomorphism classes of finite-dimensional central division algebras over k, and a slightly different operation gives also a group structure on $\mathrm{Br}(k)$.

As for the extension of scalars, if A is a central simple algebra over k and L/k is a field extension then the map $A \mapsto A \otimes_k L \in \mathrm{CS}_L$ induces a group homomorphism

$$\mathrm{Br}(k) \to \mathrm{Br}(L),$$

so that Br is a covariant functor from the category of fields to the category of abelian groups. The kernel of the above map is denoted by $\mathrm{Br}(L/k)$, and it is called the *Brauer group of k relative to L*. By definition, if $A \in \mathrm{Br}(L/k)$ then $A \otimes_k L$ is similar to a matrix algebra over L.

Definition 1.34. *A field L containing k is said to be a* splitting field *of a central simple algebra A over k (or L* splits *A, for short) if $A \in \mathrm{Br}(L/k)$.*

It is well-known that every maximal subfield of a central simple algebra A over k splits A. For example, every quadratic extension K/k which is a subfield of a quaternion algebra B over k splits B. It is also a well-known fact that every central simple algebra A over k has a maximal subfield which is separable over k, and this implies the following important consequence:

Proposition 1.35. *The Brauer group of k admits a decomposition*

$$\mathrm{Br}(k) = \bigcup \mathrm{Br}(L/k),$$

where L runs over the finite Galois extensions of k in $\bar{k}$.

Now, this decomposition makes the cohomological interpretation for $\mathrm{Br}(k)$ easier. Assume that k is a perfect field and let L/k be a finite Galois extension. Consider $L^\times$ as a discrete $\mathrm{Gal}\,(L/k)$-module via the Galois action, and choose a two-cocycle $c \in Z^2(\mathrm{Gal}\,(L/k), L^\times)$. If A_c denotes the free L-module with basis $\{e_\sigma\}_{\sigma\in\mathrm{Gal}\,(L/k)}$, a product in A_c can be defined by setting

- $e_\sigma x = {}^\sigma x e_\sigma$ for $x \in L$ and $\sigma \in \mathrm{Gal}\,(L/k)$,
- $e_\sigma e_\tau = c(\sigma,\tau)e_{\sigma\tau}$, for $\sigma,\tau \in \mathrm{Gal}\,(L/k)$.

This operation makes A_c into a ring, which is in fact a central simple algebra over k containing L as a maximal subfield. In the classical notation, the algebra A_c obtained in this way is called the *crossed product* of L and $\mathrm{Gal}\,(L/k)$ relative to c, and denoted by $(L, \mathrm{Gal}\,(L/k), c)$. Then, the class of A_c in $\mathrm{Br}(k)$ lies in $\mathrm{Br}(L/k)$. Moreover, if c' is a two-cocycle defining the same cohomology class as c, then $A_{c'}$ and A_c are similar central simple k-algebras. Therefore, there is a well-defined map

$$\mathrm{H}^2(\mathrm{Gal}\,(L/k), L^\times) \longrightarrow \mathrm{Br}(L/k), \quad [c] \longmapsto [A_c].$$

It can be shown that this map is in fact an isomorphism and, by taking direct limits over L it follows that:

Theorem 1.36. *There is a group isomorphism*

$$\mathrm{Br}(k) \simeq \mathrm{H}^2(\mathrm{Gal}\,(\bar{k}/k), \bar{k}^\times).$$

In particular,

Corollary 1.37. *The Brauer group* $\mathrm{Br}(k)$ *is a torsion group.*

Remark 1.38. There is also available a cohomological interpretation of the Brauer group $\mathrm{Br}(k)$ involving the first cohomology sets $\mathrm{H}^1(\mathrm{Gal}\,(k^s/k), \mathrm{PGL}_n(k^s))$, since a central simple k-algebra of dimension n^2 is a *twisted form* of the matrix algebra $\mathrm{M}_n(k)$. More precisely, for each integer $r \geq 1$ there exists an injection (see [**Poo**, Proposition 1.4.5])

$$\frac{\{\text{central simple } k\text{-algebras of dimension } r^2\}}{k\text{-isomorphism}} \hookrightarrow \mathrm{H}^1(\mathrm{Gal}\,(k^s/k), \mathrm{PGL}_r(k^s)).$$

Finally, we state some known results describing the Brauer group of certain fields. In general, computing the Brauer group of a field is not an easy task. However, for some families of fields the Brauer group is known to be trivial:

Theorem 1.39 (Wedderburn)**.** *If k is a finite field, then* $\mathrm{Br}(k) = 0$.

Theorem 1.40 (Tsen)**.** *If k is a field of transcendence degree one, then* $\mathrm{Br}(k) = 0$.

The case of local fields is also well understood. As we have quoted before, the Brauer group of a field k can also be interpreted as classifying central division algebras over k. Hence, from examples 1.14 and 1.15 we know that the Brauer group of $\mathbb{R}$ has only two elements, and the Brauer group of $\mathbb{C}$ is trivial. As for a non-archimedean local field k, the Brauer group of k relative to the unique unramified extension of k of degree n (in a fixed separable closure) is isomorphic to the cyclic group $\mathbb{Z}/n\mathbb{Z}$. All this picture can be summarized in the following theorem:

Theorem 1.41. *Let k be a local field. Then,*

(a) *There is an injective group homomorphism* $\mathrm{inv} : \mathrm{Br}(k) \to \mathbb{Q}/\mathbb{Z}$ *whose image is*

$$\begin{cases} \frac{1}{2}\mathbb{Z}/\mathbb{Z} & \text{if } k = \mathbb{R}, \\ 0 & \text{if } k = \mathbb{C}, \\ \mathbb{Q}/\mathbb{Z} & \text{otherwise.} \end{cases}$$

(b) *For any finite extension L of k, the diagram*

$$\begin{tikzcd}
\mathrm{Br}(k) \arrow[r, "\mathrm{inv}"] \arrow[d] & \mathbb{Q}/\mathbb{Z} \arrow[d, "{[L:k]}"] \\
\mathrm{Br}(L) \arrow[r, "\mathrm{inv}"] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

commutes.

Finally, if k is a global field, the above theorem can be used to describe the Brauer group of the completions k_v at the places v of k, and all this information can be put together to give a description of $\mathrm{Br}(k)$ as the next theorem shows:

Theorem 1.42. *Let k be a global field. For each place v of k, denote by k_v the completion of k at v, and let $\mathrm{inv}_v : \mathrm{Br}(k_v) \to \mathbb{Q}/\mathbb{Z}$ be the injection associated to the local field k_v from the above theorem. Then,*

(a) *The sequence*

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

is exact, where the second arrow is induced by the inclusions $k \hookrightarrow k_v$.

(b) *For any finite extension L of k, the diagram*

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Br}(k) \arrow[r] \arrow[d] & \bigoplus_v \mathrm{Br}(k_v) \arrow[r, "\sum \mathrm{inv}_v"] \arrow[d] & \mathbb{Q}/\mathbb{Z} \arrow[r] \arrow[d, "{[L:k]}"'] & 0 \\
0 \arrow[r] & \mathrm{Br}(L) \arrow[r] & \bigoplus_v \bigoplus_{w|v} \mathrm{Br}(L_w) \arrow[r, "\sum \mathrm{inv}_w"] & \mathbb{Q}/\mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

commutes.

Chapter 2
Quaternionic Shimura varieties and Atkin-Lehner quotients

Shimura varieties can be thought as higher-dimensional analogues of modular curves, arising as quotients of a Hermitian symmetric space by a congruence subgroup of a reductive algebraic group defined over $\mathbb{Q}$. Some special instances of these varieties were originally introduced by G. Shimura in his foundational papers in the 1960s ([**Shi63**], [**Shi67**]), while he was pursuing generalizations of the reciprocity law of complex multiplication theory.

It is fair to mention that the term "Shimura variety" was later introduced by P. Deligne ([**Del71**]), who created an axiomatic framework for the ideas of Shimura. In Deligne's formulation, Shimura varieties parametrize certain types of Hodge structures. As well as modular curves are moduli spaces for elliptic curves with level structure, Shimura varieties generalize them to higher dimension.

In this chapter, we consider a particular case of Shimura varieties. Namely, those that are defined by a totally indefinite quaternion algebra over a totally real number field. We call them *quaternionic Shimura varieties*, and they are introduced in the first section. These Shimura varieties parametrize abelian varieties with quaternionic multiplication. In the next section, the Atkin-Lehner group of a quaternionic maximal order is studied. This is a group of rational involutions on the Shimura variety, and a moduli interpretation is also available for their action, which is analyzed in the later sections following the work in [**Rot04b**] and with special attention to the case of *twisting* involutions, in which we are particularly interested.

Throughout this chapter, F will be a totally real number field of degree $n = [F : \mathbb{Q}]$, and R_F will stand for its ring of integers. Let also B be a totally indefinite quaternion algebra over F, so that $B \otimes_F F_v \simeq \mathrm{M}_2(F_v)$ for every archimedean place v of F. The reduced discriminant of B is denoted by $\mathfrak{D} = \mathrm{disc}(B) = \mathfrak{p}_1 \cdots \mathfrak{p}_{2r}$, where the $\mathfrak{p}_i$ are pairwise distinct prime ideals of R_F. Since $F = \mathbb{Q}$ corresponds to the case of Shimura curves and we will restrict to them after this chapter, we particularize to this case most of the definitions and results, and some examples are given.

1. The Shimura variety X_B

Fix a triplet $(\mathcal{O}, \mathcal{I}, \varrho)$, where $\mathcal{O}$ is a maximal order in B, $\mathcal{I}$ is a left $\mathcal{O}$-ideal (or rather its class in $\mathrm{Pic}_\ell(\mathcal{O})$) and ϱ is a positive (anti-)involution on B. Such a triplet is called a *quaternionic datum.*

Remark 2.1. By the Noether-Skolem Theorem (see [**Pie82**, §12.6]), ϱ is conjugate to the canonical involution on B, which we denote by $\beta \mapsto \bar{\beta}$. Hence, there exists $\mu \in B^\times$ such that $\beta^\varrho = \mu^{-1}\bar{\beta}\mu$ for all $\beta \in B$. Moreover, the positiveness of ϱ implies (see [**Rot03**]) that $\mathrm{tr}(\mu) = 0$ and $\mathrm{n}(\mu) \in F_+^\times$, so that μ satisfies an equation of the form $\mu^2 + \delta = 0$ for some

$\delta \in F_+^\times$. Since this element μ is determined up to multiplication by units of F, we can denote ϱ also by ϱ_μ.

Definition 2.2. *A* polarized abelian variety with quaternionic multiplication by $(\mathcal{O}, \mathcal{I}, \varrho)$ *(or with QM by $\mathcal{O}$, for short) is a triplet $(A, \iota, \mathcal{L})$ where*

- *A is an abelian variety of dimension $g = 2n$,*
- *$\iota : \mathcal{O} \hookrightarrow \mathrm{End}(A)$ is a ring monomorphism such that $\mathrm{H}_1(A, \mathbb{Z}) \simeq \mathcal{I}$ as left $\mathcal{O}$-modules,*
- *$\mathcal{L}$ is a primitive polarization on A such that the Rosati involution $'$ defined by $\mathcal{L}$ on $\mathrm{End}^0(A) = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ restricts to ϱ in $\iota(\mathcal{O})$, i.e. $'\,_{|\iota(\mathcal{O})} = \varrho \circ \iota$.*

With this definition, an isomorphism between two polarized abelian varieties $(A_1, \iota_1, \mathcal{L}_1)$ and $(A_2, \iota_2, \mathcal{L}_2)$ with QM by $\mathcal{O}$ is just an isomorphism $\alpha : A_1 \to A_2$ of the underlying abelian varieties such that $\alpha\iota_1(\beta) = \iota_2(\beta)\alpha$ for every $\beta \in \mathcal{O}$ and $\alpha^*(\mathcal{L}_2) = \mathcal{L}_1$. In particular, the following diagram must commute for every $\beta \in \mathcal{O}$:

$$\begin{tikzcd}
A_1 \arrow[r, "\alpha"] \arrow[d, "\iota_1(\beta)"'] & A_2 \arrow[d, "\iota_2(\beta)"] \\
A_1 \arrow[r, "\alpha"] & A_2
\end{tikzcd}$$

Then, attached to the quaternionic datum $(\mathcal{O}, \mathcal{I}, \varrho)$ there is the moduli problem over $\mathbb{Q}$ of classifying isomorphism classes of polarized abelian varieties with QM by $\mathcal{O}$. By the work of Shimura, it is known that the moduli functor corresponding to this moduli problem is coarsely represented by an irreducible and reduced quasi-projective scheme $X_B/\mathbb{Q} = X_{(\mathcal{O},\mathcal{I},\varrho)}/\mathbb{Q}$ over $\mathbb{Q}$ of dimension n. Moreover, if B is division then it is a complete variety (see [**Shi63**], [**Shi67**]).

Definition 2.3. *$X_{(\mathcal{O},\mathcal{I},\varrho)}$ is the* Shimura variety *defined by the quaternionic datum $(\mathcal{O}, \mathcal{I}, \varrho)$. If $(\mathcal{O}, \mathcal{I}, \varrho)$ is understood, we write X_B for its model over $\mathbb{Q}$ given by Shimura and we say that it is the Shimura variety defined by B.*

Remark 2.4. When $B \simeq \mathrm{M}_2(F)$ is the split algebra, the varieties X_B are the classical *Hilbert-Blumenthal modular varieties*. These are non-complete, but some suitable compactifications can be constructed at the cost of producing new singularities (the *cusps*). The one-dimensional case corresponds to the case of *modular curves*, which have been extremely important in the last years.

On the other hand, if B is division, as we have quoted the varieties X_B are already projective. Although this might seem to be an advantage, this fact makes the study of the arithmetic of X_B highly difficult, since in the Hilbert-Blumenthal case much of it is encoded in the added cusps.

As complex manifolds, the varieties X_B can be described as quotients of bounded symmetric domains by congruence subgroups acting on them and, by the work of W. L. Baily and A. Borel ([**BB66**]), they become quasi-projective complex algebraic varieties. More precisely, the complex manifold $X_B(\mathbb{C})$ can be constructed as the quotient of n copies of the Poincaré's upper half plane $\mathfrak{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ by the action of a discontinuous group. Indeed, since B is totally indefinite we can choose an embedding $B \hookrightarrow B \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathrm{M}_2(\mathbb{R}) \oplus \cdots \oplus \mathrm{M}_2(\mathbb{R})$, and the group $\mathcal{O}^1 = \{\gamma \in \mathcal{O}^\times : \mathrm{n}(\gamma) = 1\}$ can be identified with its image Γ_B under this embedding, which is a discrete subgroup of $\mathrm{SL}_2(\mathbb{R})^n$. An element $\gamma = (\gamma_1, \ldots, \gamma_n) \in \Gamma_B$ acts on the cartesian product $\mathfrak{H}^n$ by Moebius transformations:

$$\gamma \cdot (\tau_1, \ldots, \tau_n)^t = \left(\frac{a_1\tau_1 + b_1}{c_1\tau_1 + d_1}, \ldots, \frac{a_n\tau_n + b_n}{c_n\tau_n + d_n}\right)^t, \quad \text{where } \gamma_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}).$$

Then

$$X_B(\mathbb{C}) \simeq \Gamma_B \setminus \mathfrak{H}^n. \tag{3}$$

From this analytic approach, the quotient $\Gamma_B \setminus \mathfrak{H}^n$ can also be shown to be compact when B is division (see [**Kat92**, Theorem 5.4.1], [**BHC62**]).

Being a solution to the above moduli problem, the complex points of X_B (or equivalently, the Γ_B-orbits of $\mathfrak{H}^n$) can be interpreted clearly in the following way:

$$X_B(\mathbb{C}) = \{(A, \iota, \mathcal{L})/\mathbb{C} \text{ abelian variety with QM by } \mathcal{O}\}_{/\simeq}.$$

This moduli interpretation admits a uniformization map described in the next proposition.

Proposition 2.5. *There is a uniformization map*

$$\begin{array}{rcl} \mathfrak{H}^n & \longrightarrow & X_B(\mathbb{C}) \\ \tau = (\tau_1, \dots, \tau_n) & \longmapsto & [(A_\tau, \iota_\tau, \mathcal{L}_\tau)] \end{array}$$

realizing the isomorphism (3).

Sketch of proof. First we show how to attach to a point $\tau \in \mathfrak{H}^n$ an abelian variety with QM by $(\mathcal{O}, \mathcal{I}, \varrho)$. By means of the isomorphism $B \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathrm{M}_2(\mathbb{R})^n$, B acts naturally on $\mathbb{C}^{2n}$, so that defining $v_\tau = (\tau_1, 1, \dots, \tau_n, 1)^t \in \mathbb{C}^{2n}$, $\Lambda = \mathcal{I} \cdot v_\tau$ is a full lattice in $\mathbb{C}^{2n}$. Hence, $A_\tau = \mathbb{C}^{2n}/\Lambda$ is a complex torus of dimension $g = 2n$, and being $\mathcal{I}$ a left $\mathcal{O}$-ideal, the $\mathcal{O}$-action on $\mathbb{C}^{2n}$ preserves Λ and therefore induces a ring homomorphism $\iota_\tau : \mathcal{O} \hookrightarrow \mathrm{End}(A_\tau)$. Moreover, from the isomorphism $\Lambda \simeq \mathrm{H}_1(A_\tau, \mathbb{Z})$ we get $\mathcal{I} \simeq \mathrm{H}_1(A_\tau, \mathbb{Z})$ as left $\mathcal{O}$-modules. Hence, it suffices to define a primitive polarization $\mathcal{L}_\tau$ on A whose induced Rosati involution is compatible with $\varrho = \varrho_\mu$. By Remark 2.1, we can choose $\mu \in \mathcal{O}$ such that $\mu + \mathrm{n}(\mu) = 0$ with $\mathrm{n}(\mu) \in R_{F+}$ square-free. As it is well-known, to give a polarization $\mathcal{L}_\tau$ on $A_\tau = \mathbb{C}^{2n}/\Lambda$ amounts to give a Riemann form $E_\tau : \mathbb{C}^{2n} \times \mathbb{C}^{2n} \to \mathbb{R}$, namely an alternate $\mathbb{R}$-bilinear form which is integral when restricted to Λ, satisfying the relation

$$E_\tau(\sqrt{-1}u, \sqrt{-1}v) = E_\tau(u, v) \quad \text{for all } u, v \in \mathbb{C}^{2n}$$

and whose associated hermitian form $H(u, v) = E_\tau(\sqrt{-1}u, v) + \sqrt{-1}E_\tau(u, v)$ is positive definite. These conditions are checked to be true for the form

$$\begin{array}{rcl} E_\tau : \mathbb{C}^{2n} \times \mathbb{C}^{2n} & \longrightarrow & \mathbb{R}, \\ (u, v) & \longmapsto & E_\tau(u, v) = \mathrm{tr}_{B \otimes_{\mathbb{Q}} \mathbb{R}/\mathbb{R}}(\mu\gamma\bar{\beta}), \end{array}$$

where $\gamma, \beta \in B \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathrm{M}_2(\mathbb{R})^n$ are elements such that $u = \gamma \cdot v_\tau$ and $v = \beta \cdot v_\tau$. For example, the fact that E_τ is alternate follows from the fact that $\mathrm{tr}(\mu) = 0$.

As for the compatibility, recall that with this description of $\mathcal{L}_\tau$, its Rosati involution $'$ on $\mathrm{End}^0(A_\tau)$ is characterized by satisfying $E_\tau(u, \psi v) = E_\tau(\psi' u, v)$, for any $\psi \in \mathrm{End}^0(A_\tau)$ and $u, v \in \mathbb{C}^{2n}$. So we must check that

$$E_\tau(u, \psi v) = E_\tau(\psi^\varrho u, v) \quad \text{for any } \psi \in \mathcal{O}, u, v \in \mathbb{C}^{2n}.$$

But if we put $u = \gamma \cdot v_\tau$ and $v = \beta \cdot v_\tau$ for some $\gamma, \beta \in B \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathrm{M}_2(\mathbb{R})^n$, just applying the definitions we get

$$\begin{array}{rcl} E_\tau(u, \psi v) & = & E_\tau(\gamma \cdot v_\tau, \psi\beta \cdot v_\tau) = \mathrm{tr}(\mu\gamma\overline{\psi\beta}) = \mathrm{tr}(\mu\gamma\bar{\beta}\bar{\psi}) = \mathrm{tr}(\bar{\psi}\mu\gamma\bar{\beta}) = \\ & = & \mathrm{tr}(\mu\mu^{-1}\bar{\psi}\mu\gamma\bar{\beta}) = E_\tau(\mu^{-1}\bar{\psi}\mu\gamma \cdot v_\tau, \beta \cdot v_\tau) = E_\tau(\psi^\varrho u, v). \end{array}$$

Conversely, we must show that any QM-abelian variety $(A, \iota, \mathcal{L})$ is isomorphic to one of the form $(A_\tau, \iota_\tau, \mathcal{L}_\tau)$ for some $\tau \in \mathfrak{H}^n$ and that any two isomorphic QM-abelian varieties are represented by Γ_B-equivalent points in $\mathfrak{H}^n$.

For the first statement, let $(A, \iota, \mathcal{L})/\mathbb{C}$ be a QM-abelian variety. As a complex manifold, we can write $A(\mathbb{C}) \simeq \mathbb{C}^{2n}/\Lambda$, where Λ is a full lattice in $\mathbb{C}^{2n}$ that can be identified with the first homology group $\mathrm{H}_1(A, \mathbb{Z})$. Hence, by asking A to admit an embedding $\iota : \mathcal{O} \to \mathrm{End}(A)$ such that $\mathrm{H}_1(A, \mathbb{Z}) \simeq \mathcal{I}$ as $\mathcal{O}$-modules, we are imposing that Λ is isomorphic to $\mathcal{I}$ as $\mathcal{O}$-modules. Furthermore, $\Lambda \otimes \mathbb{Q}$ is then a left B-module of the same rank over $\mathbb{Q}$ as B, so since every left B-module is free there exists a vector $v \in \mathbb{C}^{2n}$ such that $\Lambda \otimes \mathbb{Q} = B \cdot v$, and hence $\Lambda = \mathcal{I} \cdot v$. Moreover, using the analytic and rational representations ([**BL92**, §1.2]) it is possible to show that in a suitable basis the element v can be chosen of the form $(\tau_1, 1, \ldots, \tau_n, 1)^t$ with $\tau_i \in \mathfrak{H}$. Then, if we write $\tau = (\tau_1, \ldots, \tau_n) \in \mathfrak{H}^n$ we have $A \simeq A_\tau := \mathbb{C}^{2n}/\mathcal{I} \cdot v_\tau$, where we set $v_\tau = (\tau_1, 1, \ldots, \tau_n, 1)^t$. Once we have this, it is clear that the isomorphism identifying the lattice Λ with $\mathcal{I} \cdot v_\tau$ transforms ι into ι_τ, since an endomorphism of A is completely determined by its action on the lattice $\Lambda \simeq \mathcal{I} \cdot v_\tau$. At this point, we can assume that the given QM-abelian surface is $(A_\tau, \iota_\tau, \mathcal{L})$, and it remains to show that $\mathcal{L} = \mathcal{L}_\tau$. Equivalently, we can show that the Riemann form $E : \mathbb{C}^{2n} \times \mathbb{C}^{2n} \to \mathbb{R}$ corresponding to $\mathcal{L}$ is E_τ. On the one hand, observe that the linear map $B \to \mathbb{Q}$ given by $\beta \mapsto E(\beta \cdot v_\tau, v_\tau)$ is a trace form on B, hence by the non-degeneracy of $\mathrm{tr}_{B/\mathbb{Q}}$ there exists a unique $\alpha \in B$ such that $E(\beta \cdot v_\tau, v_\tau) = \mathrm{tr}_{B/\mathbb{Q}}(\alpha\beta)$ for any $\beta \in B$. On the other hand, since the Rosati involution induced by $\mathcal{L}$ restricts to ϱ on $\mathcal{O}$, it follows that $E(v_\tau, \beta \cdot v_\tau) = E(\beta^\varrho \cdot v_\tau, v_\tau) = \mathrm{tr}(\alpha\mu^{-1}\bar{\beta}\mu)$, which implies that $\alpha = \mu$. Then, if for $u, v \in \mathbb{C}^{2n}$ we choose as before $\gamma, \beta \in B \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathrm{M}_2(\mathbb{R})^n$ such that $u = \gamma \cdot v_\tau$ and $v = \beta \cdot v_\tau$, then

$$E(u, v) = E(\gamma \cdot v_\tau, \beta \cdot v_\tau) = E(\beta^\varrho\gamma \cdot v_\tau, v_\tau) = \mathrm{tr}_{B\otimes_{\mathbb{Q}}\mathbb{R}}(\mu\gamma\bar{\beta}) = E_\tau(u, v).$$

Finally, an isomorphism $(A_\tau, \iota_\tau, \mathcal{L}_\tau) \simeq (A_{\tau'}, \iota_{\tau'}, \mathcal{L}_{\tau'})$ between QM-abelian varieties corresponding to points $\tau, \tau' \in \mathfrak{H}^n$, respectively, is easily seen to be given by an element $\gamma \in \Gamma_B$ sending τ to τ'. □

As we are interested in the rational points of X_B over non-algebraically closed fields, recall that being $X_B/\mathbb{Q}$ a moduli variety the description of $X_B(k)$ for a field k containing $\mathbb{Q}$ involves the notion of *field of moduli*:

Definition 2.6. *Suppose that $(A, \iota, \mathcal{L})$ is an abelian variety with QM defined over an algebraic closure $\bar{k}$ of a field k of characteristic zero. Then the* field of moduli *of $(A, \iota, \mathcal{L})$ is the fixed field $M(A, \iota, \mathcal{L}) = \bar{k}^H$ by the subgroup*

$$H = \{\sigma \in \mathrm{Gal}\,(\bar{k}/k) : {}^\sigma(A, \iota, \mathcal{L}) \simeq (A, \iota, \mathcal{L})\} \subseteq \mathrm{Gal}\,(\bar{k}/k).$$

Note that here the isomorphism between ${}^\sigma(A, \iota, \mathcal{L})$ and $(A, \iota, \mathcal{L})$ is required to be an isomorphism of QM-abelian varieties in the sense explained after Definition 2.2, not just an isomorphism of the underlying abelian varieties. Then, by moduli considerations, for a field extension $k \subseteq K \subseteq \bar{k}$ the K-rational points of X_B can be described as follows:

$$X_B(K) = \left\{ (A, \iota, \mathcal{L}) \;\middle|\; \begin{array}{l} (A, \iota, \mathcal{L}) \text{ is an abelian variety with QM} \\ \text{by } (\mathcal{O}, \mathcal{I}, \varrho) \text{ defined over } \bar{k} \text{ and such that} \\ K \text{ contains the field of moduli of } (A, \iota, \mathcal{L}) \end{array} \right\}_{/\simeq}.$$

Remark 2.7. From the definition it is clear that the field of moduli $M(A, \iota, \mathcal{L})$ of $(A, \iota, \mathcal{L})$ is contained in every field of definition of $(A, \iota, \mathcal{L})$, but this does not implies that $(A, \iota, \mathcal{L})$ admits a model rational over $M(A, \iota, \mathcal{L})$. Thus, the points of $X_B(K)$ corresponding to abelian varieties with QM by $\mathcal{O}$ which are defined over K (this means in particular that $\iota : \mathcal{O} \hookrightarrow \mathrm{End}_K(A)$ and $\mathcal{L}$ contains a divisor rational over K) form a possibly strict subset of $X_B(K)$. In fact, while for every elliptic curve over $\bar{\mathbb{Q}}$ the field of moduli is a field of definition, a theorem of Shimura states that for a *generic* principally polarized abelian variety over $\bar{\mathbb{Q}}$ of even dimension, the field of moduli is not a field of definition (see [**Shi72**]).

1.1. Shimura curves. Suppose that B is an indefinite quaternion algebra over $\mathbb{Q}$, which corresponds to the case $n = 1$ above, let $\mathcal{O} \subseteq B$ be a maximal order and ϱ a positive involution on B, which as before has to be conjugate to the canonical conjugation.

Now the left $\mathcal{O}$-ideal $\mathcal{I}$ in the quaternionic datum becomes superfluous, since by Corollary 1.32 the only class in $\mathrm{Pic}_\ell(\mathcal{O})$ is the trivial one. Moreover, also by Corollary 1.32 all maximal orders in B are conjugate, and this implies that for two distinct choices $\mathcal{O}, \mathcal{O}'$ of a maximal order in B the corresponding Shimura curves are isomorphic. Therefore, the Shimura curve X_B is now determined by the datum $(B, \mathcal{O}, \varrho)$. Note also that since the involution ϱ is conjugated to the canonical involution in B, from these observations it follows that $(B, \mathcal{O}, \varrho)$ is essentially determined by B, and therefore the notation X_B makes sense.

Then, we can adapt the general definition of QM-abelian variety to this case as follows:

Definition 2.8. *An* abelian surface with quaternionic multiplication by $(B, \mathcal{O}, \varrho)$ *(or with QM by* $\mathcal{O}$*, for short), is a triplet* $(A, \iota, [\mathcal{L}])$ *where*

- A *is an abelian surface (i.e. an abelian variety of dimension* 2*),*
- $\iota : \mathcal{O} \hookrightarrow \operatorname{End}(A)$ *is a ring monomorphism,*
- $[\mathcal{L}]$ *is a weak polarization on* A *such that the Rosati involution* $'$ *defined by* $[\mathcal{L}]$ *on* $\operatorname{End}^0(A) = \operatorname{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ *restricts to* ϱ *in* $\iota(\mathcal{O})$*, i.e.* $' \,_{|\iota(\mathcal{O})} = \varrho \circ \iota$*,*

We need to explain why we consider a weak polarization instead of an actual polarization. First of all, given two polarizations $\mathcal{L}, \mathcal{L}'$ on A, consider the corresponding isogenies $\varphi_{\mathcal{L}}, \varphi_{\mathcal{L}'} : A \to A^{\vee}$. The polarizations $\mathcal{L}$ and $\mathcal{L}'$ are said to be $\mathbb{Q}$-equivalent if there exists $c \in \mathbb{Q}^{\times}$ such that $\varphi_{\mathcal{L}'} = c \cdot \varphi_{\mathcal{L}}$ in $\operatorname{Hom}(A, A^{\vee}) \otimes_{\mathbb{Z}} \mathbb{Q}$. Then, a *weak polarization* on A is a $\mathbb{Q}$-equivalence class of polarizations, and $[\mathcal{L}]$ denotes the weak polarization defined by $\mathcal{L}$. Since the Rosati involution associated to a polarization $\mathcal{L}$ depends only on its $\mathbb{Q}$-equivalence class $[\mathcal{L}]$, the above definition of QM-abelian surface makes sense.

Then, identifying a point $\tau \in \mathfrak{H}$ with its class in $\Gamma_B \setminus \mathfrak{H}$, the uniformization map described by Shimura leads to a one-to-one correspondence

$$\tau \in \mathcal{O}^1 \setminus \mathfrak{H} \mapsto [(A_\tau, \iota_\tau, [\mathcal{L}_\tau])] \in X_B(\mathbb{C}) \text{ where}$$

- $A_\tau = \mathbb{C}^2/\mathcal{O} \cdot v_\tau$ with $v_\tau = (\tau, 1)^t$,
- $\iota_\tau : \mathcal{O} \hookrightarrow \operatorname{End}(A_\tau)$ is the natural map,
- $\mathcal{L}_\tau$ is the polarization induced by the Riemann form E_τ given by

$$E_\tau(x \cdot v_\tau, y \cdot v_\tau) = \operatorname{tr}(\mu x \bar{y}), \quad \text{for } x, y \in \mathcal{O}.$$

The key point is that by a result of J. S. Milne (see [**Mil79**]), the weak polarization $[\mathcal{L}]$ of a QM-abelian surface $(A, \iota, [\mathcal{L}])$ is completely determined by the datum $(B, \mathcal{O}, \varrho)$. More precisely:

Proposition 2.9 (Milne)**.** *Suppose* $(B, \mathcal{O}, \varrho)$ *is as above, and let* A *be an abelian surface equipped with an injection* $\iota : \mathcal{O} \hookrightarrow \operatorname{End}(A)$*. Then there is a unique weak polarization* $[\mathcal{L}]$ *on* A *such that* $(A, \iota, [\mathcal{L}])$ *is a QM-abelian surface with respect to* $(B, \mathcal{O}, \varrho)$*.*

As a consequence, from now on we will often consider QM-abelian surfaces just as pairs (A, ι), dropping the weak polarization off. The difference in the higher-dimensional case is that one needs to single out a polarization.

Then, given two QM-abelian surfaces (A_1, ι_1) and (A_2, ι_2) with respect to the same datum $(B, \mathcal{O}, \varrho)$, an isomorphism $(A_1, \iota_i) \xrightarrow{\simeq} (A_2, \iota_2)$ is an isomorphism $\alpha : A_1 \to A_2$ of the underlying abelian surfaces such that $\alpha\iota_1(\beta) = \iota_2(\beta)\alpha$ for every $\beta \in \mathcal{O}$. The condition on the corresponding unique weak polarizations is automatically satisfied. Therefore, the field of moduli $M(A, \iota)$ of a QM-abelian surface (A, ι) defined over the algebraic closure $\bar{k}$ of a field k of characteristic zero is defined as before: it is the fixed field $\bar{k}^H$ by the subgroup

$$H = \{\sigma \in \operatorname{Gal}(\bar{k}/k) : {}^{\sigma}(A, \iota) \simeq (A, \iota)\} \subseteq \operatorname{Gal}(\bar{k}/k).$$

And analogously, for a field extension $k \subseteq K \subseteq \bar{k}$, the K-rational points of the curve X_B can be described as

$$X_B(K) = \left\{ (A, \iota) \;\middle|\; \begin{array}{l} (A, \iota) \text{ is an abelian surface with QM} \\ \text{by } (B, \mathcal{O}, \varrho) \text{ defined over } \bar{k} \text{ and such that} \\ K \text{ contains the field of moduli of } (A, \iota) \end{array} \right\}_{/\simeq}.$$

By a theorem of Jordan (see [**Jor86**, Theorem 1.1] or Theorem 4.2 below), an abelian surface (A, ι) with quaternionic multiplication corresponding to a point $P \in X_B(K)$ admits a model rational over K if and only if K splits the quaternion algebra B.

Example 2.10. Let $B = B_6$ be the rational quaternion division algebra of discriminant 6. An equation for the canonical model of X_B over $\mathbb{Q}$ was found by A. Kurihara, and it is $x^2 + y^2 + 3 = 0$. Directly from this equation we see that $(\sqrt{-7}, 2) \in X_B(\mathbb{Q}(\sqrt{-7}))$. This implies the existence of an abelian surface (A, ι) with quaternionic multiplication by B with

$\mathbb{Q}(\sqrt{-7})$ as field of moduli. But this abelian surface cannot admit a model rational over $\mathbb{Q}(\sqrt{-7})$ according to Jordan's result, since $\mathbb{Q}(\sqrt{-7})$ does not split B.

Remark 2.11. Although we have presented here only the basic notions about Shimura curves, there are many interesting topics regarding them. There is a good treatment of the arithmetic concerning Shimura curves in Jordan's PhD. Thesis [**Jor81**]. And, from a different point of view, for example, there is the problem of computing hyperbolic fundamental domains for Shimura curves (see, e.g., [**AB04**], [**Als00**]).

2. The Atkin-Lehner group of $\mathcal{O}$

We keep the notations of the previous section, and we still fix a quaternionic datum $(\mathcal{O}, \mathcal{I}, \varrho)$ and consider the Shimura curve X_B attached to it. We denote by $\mathrm{Pic}(F)$ the class group of fractional ideals of F up to principal ideals and, similarly, $\mathrm{Pic}_+(F)$ stands for the narrow class group of fractional ideals of F up to totally positive principal ideals aR_F, $a \in F_+^\times$.

Define the groups $\mathcal{O}^\times \supseteq \mathcal{O}_+^\times \supseteq \mathcal{O}^1$ of units in $\mathcal{O}$, units in $\mathcal{O}$ of totally positive reduced norm and units in $\mathcal{O}$ of reduced norm 1, respectively. By the Hasse-Schilling-Mass Theorem ([**Vig80**, p. 90]), there is an exact sequence

$$1 \to \mathcal{O}^1 \to \mathcal{O}_+^\times \xrightarrow{\mathrm{n}} R_{F,+}^\times \to 1.$$

Fixed the notations, in order to motivate the definition of the Atkin-Lehner groups, let us explain from the isomorphism (3) how the Shimura variety comes naturally equipped with a special family of automorphisms. Recall that by the Noether-Skolem Theorem, the group of automorphisms of $\mathcal{O}$ is $\mathrm{Norm}_{B^\times}(\mathcal{O})/F^\times$, where $\mathrm{Norm}_{B^\times}(\mathcal{O})$ is the normalizer of $\mathcal{O}$ in $B^\times$. Under the embedding $B \hookrightarrow B \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathrm{M}_2(\mathbb{R})^n$, the group $B_+^\times$ of units in B of totally positive reduced norm can be regarded as a subgroup of $\mathrm{GL}_2^+(\mathbb{R})^n$. Then, an element $\alpha \in B_+^\times$ acts by Moebius transformations on $\mathfrak{H}^n$, and its action descends to an action on $X_B(\mathbb{C}) \simeq \Gamma_B \setminus \mathfrak{H}^n$ if and only if $\alpha \in \mathrm{Norm}_{B_+^\times}(\mathcal{O}^1)$, the normalizer of $\mathcal{O}^1$ in $B_+^\times$. Since $\mathrm{Norm}_{B_+^\times}(\mathcal{O}) \subseteq \mathrm{Norm}_{B_+^\times}(\mathcal{O}^1)$, it is then natural to consider the following groups:

Definition 2.12. *The* Atkin-Lehner group W of $\mathcal{O}$ *is defined to be*

$$W = \mathrm{Norm}_{B^\times}(\mathcal{O})/F^\times\mathcal{O}^\times,$$

and the positive Atkin-Lehner groups *are*

$$W_+ = \mathrm{Norm}_{B_+^\times}(\mathcal{O})/F^\times\mathcal{O}_+^\times \quad \textit{and} \quad W^1 = \mathrm{Norm}_{B_+^\times}(\mathcal{O})/F^\times\mathcal{O}^1.$$

The Atkin-Lehner group W can be identified with the group of principal two-sided $\mathcal{O}$-ideals under the map $\omega \mapsto \mathcal{O} \cdot \omega$, and it is a finite abelian 2-group. Indeed, the reduced norm $\mathrm{n} : B^\times \to F^\times$ induces an isomorphism (see [**Vig80**, Théorème III.5.7])

$$W \simeq (\mathbb{Z}/2\mathbb{Z})^t, \quad \text{for some } t \leq 2r,$$

and any class $[\omega] \in W$ can be represented by an element $\omega \in \mathcal{O}$ whose reduced norm $\mathrm{n}(\omega)$ is supported at the prime ideals $\mathfrak{p}$ dividing $\mathfrak{D}$. Besides, the group W_+ may and will be regarded as the subgroup $W_+ = \{[\omega] \in W : \mathrm{n}(\omega) \in F_+^\times\}$ of W, being the full W if $\mathrm{Pic}_+(F) \simeq \mathrm{Pic}(F)$. By the exact sequence written above, we obtain the exact sequence

$$1 \to R_{F,+}^\times/R_F^{\times 2} \to W^1 \to W_+ \to 1,$$

where a totally positive unit $u \in R_{F,+}^\times$ is mapped to any $\alpha_u \in \mathcal{O}_+^\times$ with $\mathrm{n}(\alpha_u) = u$. In this way,

$$W^1 \simeq R_{F,+}^\times/R_F^{\times 2} \times W_+ \simeq (\mathbb{Z}/2\mathbb{Z})^s, \quad \text{for some } s \leq (n-1) + 2r,$$

where the bound for s follows from Dirichlet's Unit Theorem (see [**Neu99**, p. 42]) and the inclusion $W_+ \subseteq W$.

The action of the positive Atkin-Lehner group W^1 can be interpreted in terms of moduli, as is done in [**Jor81**] for the case of curves and in [**Rot04b**] for the general case. This interpretation relies on the fact that W^1 can be regarded as a subgroup of automorphisms of the Shimura variety X_B, as follows from the motivation above: the action of $B_+^\times$ on $\mathfrak{H}^n$ descends to a free action of W^1 on $X_B(\mathbb{C})$, for any choice of the left $\mathcal{O}$-ideal $\mathcal{I}$ and the positive involution ϱ. Since all the (nontrivial) elements of W^1 have order two:

Definition 2.13. *The* Atkin-Lehner involutions *of X_B are the involutions defined by the elements $[\omega] \in W^1$ in the way explained above. By slight abuse of notation, we will sometimes consider the elements in W^1 as involutions.*

So fix $[\omega] \in W^1$ an Atkin-Lehner involution which, for ease of notation we identify with a representative ω of it, and let $P = [(A, \iota, \mathcal{L})]$ be the isomorphism class of a polarized abelian variety with QM by $\mathcal{O}$ (i.e. a closed point of X_B). Then, using the uniformization map described before, the action of $\omega \in W^1$ keeps the isomorphism class of the underlying abelian variety A, but it conjugates the QM structure $\iota : \mathcal{O} \hookrightarrow \mathrm{End}(A)$ and switches the polarization $\mathcal{L}$. More precisely, $\omega(P) = [(A, \iota_\omega, \mathcal{L}_\omega)]$ where $\iota_\omega : \mathcal{O} \hookrightarrow \mathrm{End}(A)$ is given by $\beta \mapsto \omega^{-1}\iota(\beta)\omega$ and $\mathcal{L}_\omega := \frac{1}{\mathrm{n}(\omega)}\omega^*(\mathcal{L})$. In terms of the first Chern class of $\mathcal{L}$, regarded as an alternate bilinear form $E : V \times V \to \mathbb{R}$, with $V = \mathrm{Lie}(A(\mathbb{C}))$, we have that E_ω is given by

$$(u, v) \longmapsto E((\omega/\mathrm{n}(\omega))(u), \omega(v)).$$

The action of ω described in this way is independent of the choice of a representative. Moreover, from this interpretation $W^1 \subseteq \mathrm{Aut}(X_B)$ acts on X_B as a subgroup of algebraic involuting automorphisms over $\mathbb{Q}$ because the solution to a moduli problem, if exists, is unique up to isomorphism. So that we can regard $W^1 \subseteq \mathrm{Aut}_{\mathbb{Q}}(X_B)$.

Example 2.14. Let us recover the case $F = \mathbb{Q}$ corresponding to Shimura curves and particularize the Atkin-Lehner groups just introduced to this context. As we have quoted, the subgroup W_+ coincides with the full Atkin-Lehner group W because both $\mathrm{Pic}(\mathbb{Q})$ and $\mathrm{Pic}_+(\mathbb{Q})$ are trivial. Moreover, since the only positive unit in the ring of integers $\mathbb{Z}$ is 1, we have clearly $\mathcal{O}_+^\times = \mathcal{O}^1$ in this case. Hence in the case $F = \mathbb{Q}$ the three Atkin-Lehner groups coincide, $W = W_+ = W^1$, and we speak of *the* Atkin-Lehner group W_D of $\mathcal{O}$, where $D = \mathrm{disc}(B) = p_1 \cdots p_{2r}$ for some pairwise distinct primes $p_1, \dots, p_{2r}$. In this case, since maximal orders in B are all conjugate, the Atkin-Lehner group depends essentially on B, which is determined up to isomorphism by its reduced discriminant D.

Furthermore, in this case $W_D \simeq (\mathbb{Z}/2\mathbb{Z})^{2r}$, where $2r$ is the number of distinct primes dividing D, and a set of representatives for W_D is any set of elements α_m in $\mathrm{Norm}_{B_+^\times}(\mathcal{O}) \cap \mathcal{O}$ whose reduced norms $\mathrm{n}(\alpha_m) = m$ range over all the distinct positive divisors m of D, one for each of them (see [**Jor81**, Proposition 1.2.4]). Under such a choice, we can write $W_D = \{\omega_m : m|D, m > 0\}$ where, following standard notation, ω_m denotes the Atkin-Lehner involution induced by α_m. Then, these involutions satisfy $\omega_m \cdot \omega_{m'} = \omega_{mm'/(m,m')^2}$, and this shows in particular that W_D is generated by the involutions $\omega_{p_1}, \dots, \omega_{p_{2r}}$.

The moduli interpretation of the Atkin-Lehner involutions is now easier to describe in detail than in the general case. Consider the isomorphism class of a QM-abelian surface $P_\tau = [(A, \iota, [\mathcal{L}])_\tau] = [(A_\tau, \iota_\tau, [\mathcal{L}_\tau])]$ corresponding to a point $\tau \in \mathfrak{H}$. Using Shimura's parametrization, if $\alpha_m \in \mathrm{Norm}_{B_+^\times}(\mathcal{O}) \cap \mathcal{O}$ has reduced norm m dividing D, then the Atkin-Lehner involution ω_m maps P_τ to $P_{\alpha_m\tau}$. But observe that we have an isomorphism

$$g : A_{\alpha_m\tau} = \mathbb{C}^2/\mathcal{O} \cdot v_{\alpha_m\tau} \simeq \mathbb{C}^2/\mathcal{O}\alpha_m \cdot v_\tau \xrightarrow{\alpha_m^{-1}} \mathbb{C}^2/\mathcal{O} \cdot v_\tau = A_\tau.$$

It is easily checked that this isomorphism satisfies $g \circ \iota_{\alpha_m\tau}(\beta) = \iota_\tau(\alpha_m^{-1}\beta\alpha_m) \circ g$ for all $\beta \in \mathcal{O}$. Now, starting with ι define $\iota_{\alpha_m} : \mathcal{O} \hookrightarrow \mathrm{End}(A)$ by $\iota_{\alpha_m}(\beta) = \iota(\alpha_m^{-1}\beta\alpha_m)$. By the result of Milne quoted in the previous section, there exists a unique weak polarization $[\mathcal{L}_{\alpha_m}]$ such that $(A, \iota_{\alpha_m}, [\mathcal{L}_{\alpha_m}])$ is a QM-abelian surface. A simple calculation involving the Rosati involution shows that $[\mathcal{L}_{\alpha_m}] = [\alpha_m^*\mathcal{L}]$. Therefore, we can describe the action of ω_m on X_B dropping the point τ off as

$$\omega_m([A, \iota, [\mathcal{L}]]) = [(A, \iota_{\alpha_m}, [\alpha_m^*\mathcal{L}])], \quad \text{where } \alpha_m \in \mathrm{Norm}_{B_+^\times}(\mathcal{O}) \text{ has reduced norm } m.$$

Example 2.15. In [**BFGR06**, Table 1], explicit equations for some Shimura curves and the Atkin-Lehner involutions on them are given. For example, if X_6 is the Shimura curve defined by the rational quaternion algebra B_6 of discriminant 6, an affine equation for (the canonical model over $\mathbb{Q}$ of) X_6 is

$$x^2 + y^2 + 3 = 0.$$

In terms of this equation, $\omega_2(x, y) = (-x, -y)$ and $\omega_3(x, y) = (x, -y)$. Therefore, $\omega_6(x, y) = \omega_2 \cdot \omega_3(x, y) = (-x, y)$.

3. Forgetful maps into Hilbert modular varieties

Suppose that $(A, \iota, \mathcal{L})$ is a primitively polarized abelian variety with quaternionic multiplication by $(\mathcal{O}, \mathcal{I}, \varrho)$ as before. We have not yet mentioned that the type $(1, d_2, \dots, d_g)$ of the polarization $\mathcal{L}$ depends only on the triplet $(\mathcal{O}, \mathcal{I}, \varrho)$; this is due to the fact that $X_{(\mathcal{O},\mathcal{I},\varrho)}$ is connected. Therefore, since it does not depend on the particular triplet $(A, \iota, \mathcal{L})$ we obtain a natural morphism

$$\begin{array}{rccc} \pi\colon & X_{(\mathcal{O},\mathcal{I},\varrho)} & \longrightarrow & \mathcal{A}_{g,(1,d_2,\dots,d_g)} \\ & (A, \iota, \mathcal{L}) & \longmapsto & (A, \mathcal{L}) \end{array}$$

from the Shimura variety $X_{(\mathcal{O},\mathcal{I},\varrho)}$ to the moduli space $\mathcal{A}_{g,(1,d_2,\dots,d_g)}$ of g-dimensional polarized abelian varieties of type $(1, d_2, \dots, d_g)$. This map π amounts to *forget* the quaternionic endomorphism structure and, as it is shown in [**Rot04b**], it factors through certain Hilbert modular varieties. We are especially interested in the forgetful map from $X_{(\mathcal{O},\mathcal{I},\varrho)}$ to the Hilbert modular variety defined by a totally real Eichler pair:

Definition 2.16. *An* Eichler pair (S, φ) *for the order* $\mathcal{O}$ *is an order* S *over the ring of integers* R_F *of* F *in a quadratic extension* L *of* F*, together with an* R_F*-optimal embedding* $\varphi : S \hookrightarrow \mathcal{O}$*, i.e. such that* $\varphi(S) = \varphi(L) \cap \mathcal{O}$*. The Eichler pair* (S, φ) *is said to be totally real if* L *is.*

Then, given a totally real Eichler pair (S, φ), let us denote by $\mathcal{H}_S$ the *Hilbert modular variety* that classifies isomorphism classes of *abelian varieties with real multiplication by* S, that is, of triplets $(A, i, \mathcal{L})$ where

- A is an abelian variety of dimension $[L : \mathbb{Q}] = 2n$,
- $i : S \hookrightarrow \mathrm{End}(A)$ is a ring monomorphism and
- $\mathcal{L}$ is a polarization of type $(1, d_2, \dots, d_g)$ on A.

$\mathcal{H}_S$ is a $2n$-dimensional, non-complete scheme defined over $\mathbb{Q}$. If $(A, \iota, \mathcal{L})$ is an abelian variety with QM by $\mathcal{O}$, composing the embedding φ with the quaternionic structure ι we obtain a ring homomorphism $i = \iota \circ \varphi : S \hookrightarrow \mathrm{End}(A)$, so that the map $(A, \iota, \mathcal{L}) \mapsto (A, \iota\circ\varphi, \mathcal{L})$ defines a morphism

$$\pi_{(S,\varphi)} : X_{(\mathcal{O},\mathcal{I},\varrho)} \longrightarrow \mathcal{H}_S$$

attached to the Eichler pair (S, φ), which consists in restricting the quaternionic multiplication by $\mathcal{O}$ to a real multiplication by the order S. The difference with the forgetful map $X_{(\mathcal{O},\mathcal{I},\varrho)} \to \mathcal{A}_{g,(1,d_2,\dots,d_g)}$ is that not all the quaternionic multiplication is forgotten, we still preserve the multiplication coming from S.

Being $\mathcal{H}_S/\mathbb{Q}$ a modular variety, if k is a field of characteristic zero then a k-rational point of $\mathcal{H}_S$ corresponds to an abelian variety with real multiplication by S with field of moduli contained in k, rather than admitting a model rational over k. Although the notion of field of moduli here is analogous to the case of abelian varieties with quaternionic multiplication, we write down the precise definition because later this notion will play an important role in our problem:

Definition 2.17. *With the above notations, suppose that* $(A, i, \mathcal{L})$ *is an abelian variety with real multiplication by* S *defined over an algebraic closure* $\overline{k}$ *of a field of characteristic zero.*

Then the field of moduli *of $(A,i,\mathcal{L})$ is the fixed field $M(A,i,\mathcal{L})=\bar{k}^H$ by the subgroup*

$$H=\{\sigma\in\mathrm{Gal}\,(\bar{k}/k):{}^{\sigma}(A,i,\mathcal{L})\simeq(A,i,\mathcal{L})\}\subseteq\mathrm{Gal}\,(\bar{k}/k).$$

Remark 2.18. The difference with the QM case comes from the notion of isomorphism of abelian varieties with real multiplication. If $(A,i,\mathcal{L})$ is such an abelian variety and $\sigma\in\mathrm{Gal}\,(\bar{k}/k)$, then an isomorphism ${}^{\sigma}(A,i,\mathcal{L})\simeq(A,i,\mathcal{L})$ means an isomorphism $\alpha_\sigma:{}^{\sigma}A\to A$ of the underlying abelian varieties such that $\alpha_\sigma^*(\mathcal{L})={}^{\sigma}\mathcal{L}$ and such that $i(s)\circ\alpha_\sigma=\alpha_\sigma\circ{}^{\sigma}i(s)$ for all $s\in S$. So the difference with the QM case is that this commutativity condition is asked only for the elements in the quadratic order S embedded in $\mathcal{O}$, instead of for all the elements in $\mathcal{O}$. In the same direction, if $(A,i,\mathcal{L})$ is defined over a field extension K/k this means in particular that $i:S\hookrightarrow\mathrm{End}_K(A)$. In other words, the endomorphisms arising from S are defined over K. However, if $\pi_{(S,\varphi)}$ maps a QM-abelian variety $(A,\iota,\mathcal{L})$ to $(A,i,\mathcal{L})$, then the endomorphisms arising from $\mathcal{O}$ via ι may not be all of them defined over K, but rather over some larger field extension.

For a totally real Eichler pair (S,φ), let us denote by $\tilde{X}_{B/(S,\varphi)}\subset\mathcal{H}_S$ the image under $\pi_{(S,\varphi)}$ of $X_B=X_{(\mathcal{O},\mathcal{I},\varrho)}$ in the Hilbert modular variety $\mathcal{H}_S$. The key point is that this forgetful map $\pi_{(S,\varphi)}$ factors through a quotient of $X_{(\mathcal{O},\mathcal{I},\varrho)}$ by a certain subgroup of Atkin-Lehner involutions, namely the *twisting involutions*, which are studied in the next section.

As a final comment, note that in an analogous way to how we have defined $\pi_{(S,\varphi)}$, we can also define a forgetful map π_F from X_B to $\mathcal{H}_F$, the Hilbert modular variety which classifies polarized abelian varieties of type $(1,d_2,\dots,d_g)$ of dimension $2n$ together with a homomorphism $R_F\hookrightarrow\mathrm{End}(A)$, just by forgetting the quaternionic endomorphism structure but preserving the multiplication by R_F. The relation between $\pi_F:X_B\to\mathcal{H}_F$ and the forgetful maps $\pi_{(S,\varphi)}:X_B\to\mathcal{H}_S$ arising from the Eichler pairs for the order $\mathcal{O}$ is also studied in [**Rot04b**].

4. Polarizations and twisting involutions

We have quoted above that the type of the polarizations in the triplets $(A,\iota,\mathcal{L})$ parametrized by the Shimura variety $X_{(\mathcal{O},\mathcal{I},\varrho)}$ is determined by the datum $(\mathcal{O},\mathcal{I},\varrho)$. More precisely, we have the following result from [**Rot03**]:

Proposition 2.19 (Rotger)**.** *The polarizations of the abelian varieties $(A,\iota,\mathcal{L})$ with quaternionic multiplication parametrized by $X_{(\mathcal{O},\mathcal{I},\varrho)}$ are* principal *if and only if:*

- $\mathrm{disc}(B)=(D)$ *is a principal ideal of F, generated by a totally positive element $D\in F_+^\times$,*
- $\mathrm{n}(\mathcal{I})$ *and the codifferent $\{x\in F:\mathrm{tr}_{F/\mathbb{Q}}(xR_F)\subseteq\mathbb{Z}\}$ of F over $\mathbb{Q}$ lie in the same ideal class in* $\mathrm{Pic}(F)$*,*
- *the positive anti-involution on B is $\varrho=\varrho_\mu:B\to B$, $\beta\mapsto\mu^{-1}\bar{\beta}\mu$ for some $\mu\in\mathcal{O}$ such that $\mu^2+D=0$.*

From now on, we will restrict ourselves to *principally* polarized abelian varieties, so that we assume the conditions on $(\mathcal{O},\mathcal{I},\varrho)$ from the above proposition. In particular, $\mathrm{disc}(B)=(D)$ for some $D\in F_+^\times$ and $\varrho=\varrho_\mu$ with $\mu\in\mathcal{O}$ satisfying $\mu^2+D=0$. Then $(\mathcal{O},\mathcal{I},\varrho)$ is said to be of *principal type*, and $\mathcal{A}_g$ will stand for $\mathcal{A}_{g,(1,\dots,1)}$. These assumptions are satisfied if, for example, $h_+(F)=1$. Since later we will restrict ourselves to the case of Shimura curves, corresponding to $F=\mathbb{Q}$, this hypothesis will be automatically satisfied.

As mentioned at the end of the last section, the forgetful map $\pi_{(S,\varphi)}:X_B\to\mathcal{H}_S$ factors through a quotient by a certain subgroup of Atkin-Lehner involutions. Before introducing them, we need the notion of a *twist* of the pair $(\mathcal{O},\mu)$:

Definition 2.20. *We say that an element $\chi\in\mathcal{O}\cap\mathrm{Norm}_{B^\times}(\mathcal{O})$ is a* twist *of $(\mathcal{O},\mu)$ if $\chi^2+\mathrm{n}(\chi)=0$ (i.e., χ is a pure quaternion) and $\mu\chi=-\chi\mu$. Therefore,*

$$B=F+F\mu+F\chi+F\mu\chi=\left(\frac{-D,-n(\chi)}{F}\right).$$

Moreover, a pair $(\mathcal{O},\mu)$ *is said to be* twisting *if it admits some twist* χ*, and similarly, a quaternion algebra* B *is* twisting *if it contains a twisting pair* $(\mathcal{O},\mu)$*.*

Lemma 2.21. *A totally indefinite quaternion algebra* B *over* F *is twisting if and only if*

$$B\simeq\left(\frac{-D,m}{F}\right)\quad \textit{for some } m\in F_+^\times,\quad m|D.$$

Proof. Indeed, suppose that $(\mathcal{O},\mu)$ is a twisting pair of B, $\mu\in\mathcal{O}$, $\mu^2+D=0$, and let $\chi\in\mathcal{O}\cap\mathrm{Norm}_{B^\times}(\mathcal{O})$ be a twist of $(\mathcal{O},\mu)$. Then, the class of χ in W can be represented by an element $\chi'\in\mathcal{O}\cap\mathrm{Norm}_{B^\times}(\mathcal{O})$ whose norm divides D. We can write

$$\chi'=\chi a\gamma,\quad \text{for some } a\in F^\times,\gamma\in\mathcal{O}^\times.$$

Then consider $\chi'':=\chi'\gamma^{-1}=\chi a$. Since both χ', γ^{-1} belong to $\mathcal{O}\cap\mathrm{Norm}_{B^\times}(\mathcal{O})$, the same is true for χ''. Moreover, from the equality $\chi''=\chi a$ we see that χ'' is still a pure quaternion and $\mu\chi''=-\chi''\mu$, since $a\in F^\times$. Hence taking $m=-\mathrm{n}(\chi'')=-\mathrm{n}(\chi')\mathrm{n}(\gamma^{-1})$, we have $B\simeq(\frac{-D,m}{F})$ with m dividing D, since γ is a unit. And m is forced to be totally positive by the indefiniteness of B. This proves one direction, and the other one is clear. □

Example 2.22. It is easy to give some examples in the case $F=\mathbb{Q}$:

(1) Let B_{15} be the indefinite rational quaternion algebra of discriminant 15. Since $B_{15}\simeq(\frac{-15,3}{\mathbb{Q}})$, B_{15} is twisting.
(2) Let B_D be the indefinite rational quaternion division algebra of discriminant $D=2{\cdot}3{\cdot}5{\cdot}13$. One checks that $B_D\simeq(\frac{-D,2}{\mathbb{Q}})\simeq(\frac{-D,5}{\mathbb{Q}})$, and that B_D is not represented in this way for other proper divisors m of D distinct from 2 and 5. In particular, B_D is twisting.

Now let $[\omega]\in W^1$ be an Atkin-Lehner involution represented by an element $\omega\in\mathrm{Norm}_{B^\times}(\mathcal{O})$. It may happen that the class of ω in the full Atkin-Lehner group W is represented by a twist $\chi\in\mathcal{O}\cap\mathrm{Norm}_{B^\times}(\mathcal{O})$ of the pair $(\mathcal{O},\mu)$, and whether it is or it is not is a condition that does not depend on the choice of the representative ω of $[\omega]\in W^1$. Then,

Definition 2.23. *An Atkin-Lehner involution* $[\omega]\in W^1$ *is called a* twisting involution *with respect to the pair* $(\mathcal{O},\mu)$ *if the class of* ω *in the full Atkin-Lehner group* W *is represented by a twist* $\chi\in\mathcal{O}\cap\mathrm{Norm}_{B^\times}(\mathcal{O})$ *of* $(\mathcal{O},\mu)$*.*

Remark 2.24. Since B is totally indefinite, an element $\chi\in B_+^\times$ will never be a twist of the pair $(\mathcal{O},\mu)$. Indeed, for the isomorphism $B\simeq(\frac{-D,-\mathrm{n}(\chi)}{F})$ it is necessary that $\mathrm{n}(\chi)$ be totally negative, hence twisting involutions $[\omega]\in W^1$ are always represented by twists $\chi\in B^\times$ of totally negative reduced norm.

Definition 2.25. *The subgroup* V_0 *of* W^1 *generated by the twisting involutions of the pair* $(\mathcal{O},\mu)$ *is called the* twisting subgroup *attached to* $(\mathcal{O},\mu)$*. In general, for a subring* $S\subseteq\mathcal{O}$*,* $V_0(S)$ *denotes the subgroup of* W^1 *generated by the twisting involutions represented by twists lying in* S*.*

Given a totally real Eichler pair (S,φ), the twisting subgroup $V_0(\varphi(S))$ plays a crucial role in factoring the map $\pi_{(S,\varphi)}$ through a quotient of $X_{(\mathcal{O},\mathcal{I},\varrho)}$. But in order to understand better how this group looks like, and how the forgetful map π_F also factors through a certain quotient of $X_{(\mathcal{O},\mathcal{I},\varrho)}$, it is useful to deal with the *stable group* attached to $(\mathcal{O},\mu)$. Although we do not need it for our purposes, we briefly introduce it and quote some useful facts that show its close relation with the twisting group:

Definition 2.26. *Denote by* $\Omega(\mathcal{O},\mu)=\{\xi\in F(\mu)\cap\mathcal{O}:\xi^f=1,f\geq 1\}$ *the finite group of roots of unity in the CM-order* $F(\mu)\cap\mathcal{O}$*. Then the* stable group *attached to* $(\mathcal{O},\mu)$ *is the subgroup* $W_0=V_0\cdot U_0$ *of* W^1 *generated by the twisting group and*

$$U_0=\mathrm{Norm}_{F(\mu)^\times}(\mathcal{O})/F^\times\Omega(\mathcal{O},\mu).$$

Remark 2.27. Note that U_0 really is a subgroup of W^1. Indeed, since $n(\mu) = D$ is totally positive and $\mathrm{tr}(\mu) = 0$, one checks easily that all the elements in $F(\mu)^\times$ have totally positive reduced norm. Hence $\mathrm{Norm}_{F(\mu)^\times}(\mathcal{O}) \subseteq \mathrm{Norm}_{B_+^\times}(\mathcal{O})$ is a subgroup. On the other hand, if two elements $\omega, \omega' \in \mathrm{Norm}_{F(\mu)^\times}(\mathcal{O})$ are $F^\times\mathcal{O}^1$-equivalent, then they are already $F^\times\Omega(\mathcal{O},\mu)$-equivalent. This is due to the fact that $\Omega(\mathcal{O},\mu) = F(\mu) \cap \mathcal{O}^1$, and leads to an inclusion $U_0 \subseteq W^1$.

Since both V_0 and W_0 are subgroups of W^1, they are isomorphic to a direct product of certain number of copies of $(\mathbb{Z}/2\mathbb{Z})$. Indeed, in [**Rot04a**] a detailed description of them is given. More precisely, for any principally polarized pair $(\mathcal{O},\mu)$ as above, we have that $U_0 \simeq (\mathbb{Z}/2\mathbb{Z})^{\omega_{odd}}$, where $\omega_{odd} = |\{\xi \in F(\mu) \cap \mathcal{O} : \xi^f = 1, f \text{ odd}\}|$. So in the case of $(\mathcal{O},\mu)$ being a non-twisting pair, we have $W_0 \simeq (\mathbb{Z}/2\mathbb{Z})^{\omega_{odd}}$. However, if $(\mathcal{O},\mu)$ is twisting, U_0 is a subgroup of V_0 and $V_0/U_0 \simeq U_0$, hence $W_0 \simeq V_0 \simeq (\mathbb{Z}/2\mathbb{Z})^{2\omega_{odd}}$.

Example 2.28. Following our previous examples, suppose $F = \mathbb{Q}$, and write as above

$$W = W_D = \{\omega_m : m|D, m > 0\}$$

for the (full) Atkin-Lehner group of $\mathcal{O}$. First of all, observe that $\mu \in \mathcal{O} \cap \mathrm{Norm}_{F(\mu)^\times}(\mathcal{O})$, with $\mu^2 + D = 0$, so that it defines an involution in the subgroup U_0 of W_D, which is represented by the full Atkin-Lehner involution ω_D, since $\mathrm{n}(\mu) = D$. Hence $\langle\omega_D\rangle \subseteq U_0$. But now observe that the ring of integers of the quadratic extension $\mathbb{Q}(\mu) \simeq \mathbb{Q}(\sqrt{-D})$ does not have nontrivial units ($D \neq 1, 3$ because B is indefinite), and therefore $\omega_{odd} = 1$ in this case. Hence $U_0 = \langle\omega_D\rangle$. By the results quoted above, if $(\mathcal{O},\mu)$ is a non-twisting pair we have $W_0 = U_0 = \langle\omega_D\rangle \simeq \mathbb{Z}/2\mathbb{Z}$. On the other hand, if $(\mathcal{O},\mu)$ is twisting we have $U_0 \subseteq V_0 = W_0 \simeq (\mathbb{Z}/2\mathbb{Z})^2$, which implies the existence of another twisting involution ω_d, for some positive proper divisor d of D, such that $V_0 = W_0 = \langle\omega_d, \omega_D\rangle \simeq (\mathbb{Z}/2\mathbb{Z})^2$. Hence $V_0 = W_0 = \{1, \omega_d, \omega_{D/d}, \omega_D\}$.

Recovering the quaternion algebra B_D of the last example, the stable group of a non-twisting pair of B_D is $W_0 = \langle\omega_D\rangle$, while for the stable group of a twisting pair we have two possibilities: either $W_0 = \langle\omega_2, \omega_D\rangle$ or $W_0 = \langle\omega_5, \omega_D\rangle$.

Before stating the precise result telling us how the forgetful maps $\pi_{(S,\varphi)}$ factor through certain quotients of $X_{(\mathcal{O},\mathcal{I},\varrho)}$, we need to introduce the notion of *Heegner point*. As a motivation for the definition, recall the following well-known result:

Proposition 2.29. *With the above notations for F, B, $\mathcal{O}$, let k be a field of characteristic zero. Let A be an abelian variety over $\bar{k}$ of dimension $2n$ such that* $\mathrm{End}(A)$ *contains an order isomorphic to $\mathcal{O}$. Then, one and only one of the following is satisfied:*

- *A is simple, or*
- *A is isogenous to A_0^2 for some simple abelian variety A_0 of dimension n.*

Indeed, in the first case $\mathrm{End}(A) \simeq \mathcal{O}$*, while in the second one* $\mathrm{End}(A_0)$ *is an order in a CM-field L over F, and* $\mathrm{End}(A)$ *can be identified with an order in* $\mathrm{M}_2(L)$*.*

These only two cases lead to the definition of Heegner (or CM) point:

Definition 2.30. *A closed point $[(A,\iota,\mathcal{L})]$ on $X_B = X_{(\mathcal{O},\mathcal{I},\varrho)}$, as well as its image on $\tilde{X}_{B/(S,\varphi)}$, is called a* Heegner point *(or* CM-point*) if* $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \mathrm{M}_2(L)$ *for a CM-field L over F.*

The set of Heegner points on these varieties is discrete and dense, and the generic case is the non-Heegner case, that is, $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q} = B$.

Finally, the important role of twisting involutions is clear from the next result appearing in [**Rot04b**]:

Theorem 2.31 (Rotger)**.** *Let $(\mathcal{O},\mathcal{I},\varrho)$ be a quaternionic datum of principal type, and let $X_B = X_{(\mathcal{O},\mathcal{I},\varrho)}$ be the corresponding Shimura variety. Let also (S,φ) be a totally real Eichler* *pair. Then, the map $\pi_{(S,\varphi)} : X_B \to \mathcal{H}_S$ is a quasifinite*[1] *map that factors over $\mathbb{Q}$ into the projection $X_B \to X_B/V_0(\varphi(S))$ of X_B onto its quotient by the finite 2-group $V_0(\varphi(S))$ and a birational morphism $b_{(S,\varphi)} : X_B/V_0(\varphi(S)) \dashrightarrow \tilde{X}_{B/(S,\varphi)}$ into the image of X_B in $\mathcal{H}_S$ by $\pi_{(S,\varphi)}$. Moreover, $b^{-1}_{(S,\varphi)}$ is defined on the whole $\tilde{X}_{B/(S,\varphi)}$ but a finite set $\mathcal{T}_{(S,\varphi)}$ of Heegner points.*

The relevance of this theorem relies not only on the fact that the forgetful map factors through the twisting subgroup $V_0(\varphi(S))$, but also on the fact that the image of X_B by $\pi_{(S,\varphi)}$ in $\mathcal{H}_S$ is birationally equivalent to the quotient $X_B/V_0(\varphi(S))$. In particular, there is no subgroup G of W^1 larger than $V_0(\varphi(S))$ such that the forgetful map $\pi_{(S,\varphi)}$ factors through the quotient of X_B by G.

5. Rational points of the Atkin-Lehner quotient by a twisting involution

Theorem 2.31 allows us to interpret the points in an Atkin-Lehner quotient $X_B/\langle\omega\rangle$ of $X_B = X_{(\mathcal{O},\mathcal{I},\rho)}$ by a twisting involution in terms of moduli. So let $[\omega] \in W^1$ be a twisting involution, represented by an element $\omega \in \mathcal{O} \cap \mathrm{Norm}_{B_+^\times}(\mathcal{O})$ such that $\mathrm{n}(\omega) = m \in F_+^\times$ and $m|D$, and let $\chi \in \mathcal{O} \cap \mathrm{Norm}_{B^\times}(\mathcal{O})$ be a twist of it, satisfying $\chi^2 = m$. Then the field $F' = F(\chi) \simeq F(\sqrt{m})$ is a totally real quadratic extension of F, and its ring of integers $S = R_{F'}$ is an optimally embedded order. Choosing an optimal embedding $\varphi : S \hookrightarrow \mathcal{O}$, (S,φ) is a totally real Eichler pair and we can apply the above theorem. Then we have

$$X_B/\langle\omega\rangle \longrightarrow X_B/V_0(\varphi(S)) \overset{b_{(S,\varphi)}}{\dashrightarrow} \tilde{X}_{B/(S,\varphi)} \subset \mathcal{H}_S,$$

where we have composed first with the natural projection $X_B/\langle\omega\rangle \to X_B/V_0(\varphi(S))$. In this way, a point in $X_B/\langle\omega\rangle$ defines an isomorphism class of abelian varieties with real multiplication by S.

Now let k be a field of characteristic zero, and consider the sets of k-rational points $X_B/\langle\omega\rangle(k)$ and $\tilde{X}_{B/(S,\varphi)}(k)$. By the moduli interpretation of the Hilbert modular variety, the points in the second set correspond to isomorphism classes of principally polarized abelian varieties with real multiplication by S, $(A, i : S \hookrightarrow \mathrm{End}(A), \mathcal{L})$, with $\mathrm{End}(A) \supseteq \mathcal{O}$ and k containing its field of moduli.

If $P \in X_B/\langle\omega\rangle(k)$, since the above maps are defined over $\mathbb{Q}$, it defines a point $Q \in \tilde{X}_{B/(S,\varphi)}(k)$, which corresponds to the isomorphism class $[(A,i,\mathcal{L})]$ of a principally polarized abelian variety $(A,i,\mathcal{L})$ with real multiplication by S, with $\mathrm{End}(A) \supseteq \mathcal{O}$, and such that *its field of moduli is contained in k*. Note that here we find again the important role of the field of moduli, like in the case of the moduli interpretation of the Shimura variety X_B.

So we have proved the following:

Corollary 2.32. *With the above notations, if the quotient variety $X_B/\langle\omega\rangle$ has a k-rational point then there exists a principally polarized abelian variety $(A,i,\mathcal{L})$ with real multiplication by S, with $\mathrm{End}(A) \supseteq \mathcal{O}$, such that its field of moduli is contained in k.*

5.1. The case of Shimura curves. Assume now that $F = \mathbb{Q}$, so that X_B is the Shimura curve parametrizing abelian surfaces with quaternionic multiplication by $(B,\mathcal{O},\varrho)$, and write $W_D = \{\omega_m : m|D, m > 0\}$ for the Atkin-Lehner group of $\mathcal{O}$ as before.

If the pair $(\mathcal{O},\mu)$ is twisting, it follows from Example 2.28 that $V_0 = W_0 = \langle\omega_d,\omega_D\rangle \simeq (\mathbb{Z}/2\mathbb{Z})^2$ for some positive proper divisor d of D. Hence the twisting involutions are $\omega_d, \omega_{D/d}$ and ω_D. Let ω_m be one of them (so $m = d, D/d$ or D), and choose $\chi_m \in \mathcal{O} \cap \mathrm{Norm}_{B^\times}(\mathcal{O})$ a twist of ω_m. Therefore, $\chi_m^2 = m$, and $\mathbb{Q}(\chi_m) \simeq \mathbb{Q}(\sqrt{m})$ is a totally real quadratic field

[1] Here, a morphism between two schemes of not necessarily the same dimension is said to be *quasifinite* if its fibres are finite.

whose ring of integers $S = R_{\mathbb{Q}(\sqrt{m})}$ is optimally embedded in $\mathcal{O}$. In other words, there exists an embedding $\varphi : S \hookrightarrow \mathcal{O}$ such that (S, φ) is a totally real Eichler pair.

Since the only twisting involution in $V_0(\varphi(S))$ is ω_m, now the diagram in Theorem 2.31 reads as follows:

$$\begin{tikzcd}
X_B \arrow[rr, "\pi_{(S,\varphi)}"] \arrow[ddr, "\pi_m"'] & & \mathcal{H}_S \\
& & \tilde{X}_{B/(S,\varphi)} \arrow[u, hook] \\
& X_B/\langle\omega_m\rangle \arrow[ur, dashed, "b_{(S,\varphi)}"'] &
\end{tikzcd}$$

Therefore, using the moduli interpretation of both X_B and $\mathcal{H}_S$, we obtain:

Proposition 2.33. *With notations as before, if ω_m is a twisting involution on X_B, then the Atkin-Lehner quotient $X_B^{(m)} := X_B/\langle\omega_m\rangle$ (which is defined over $\mathbb{Q}$) is a solution to the moduli problem of classifying principally polarized abelian surfaces $(A, i : S \hookrightarrow \mathrm{End}(A))$ with real multiplication by the ring of integers of $\mathbb{Q}(\sqrt{m})$, and such that $\mathcal{O} \subseteq \mathrm{End}(A)$.*

As a consequence, if k is a field containing $\mathbb{Q}$ and $k \subseteq K \subseteq \bar{k}$ is a field extension, then the K-rational points of $X_B^{(m)}$ have the following interpretation:

$$X_B^{(m)}(K) = \left\{ \ (A,i) \ \left| \ \begin{array}{l} (A,i) \text{ is an abelian surface with real multiplication} \\ \text{by } R_{\mathbb{Q}(\sqrt{m})} \text{ defined over } \bar{k}, \text{ with } \mathcal{O} \subseteq \mathrm{End}(A), \\ \text{and such that } K \text{ contains the field of moduli of } (A,i) \end{array} \right. \right\}_{/\simeq} .$$

Chapter 3
Obstructions to the existence of rational points

This chapter is a brief introduction to some techniques for the study of obstructions to the existence of rational points on algebraic varieties. Classically, the first and most famous obstruction of this kind is the so-called *Hasse principle* or *local-global principle.* Roughly speaking, an algebraic variety X over a global field k is said to satisfy the Hasse principle over k if for the existence of a k-rational point on X it is necessary and sufficient that X has a k_v-rational point for every place v of k. In other words, if

$$X(k) \neq \emptyset \iff X(k_v) \neq \emptyset \text{ for all places } v \text{ of } k.$$

As an example, by the Theorem of Hasse-Minkowski quadratic forms over number fields are known to satisfy the Hasse principle (see [**Ser73**, Ch. IV, Thm. 8] for the case over $\mathbb{Q}$), and this is also true in the general case of global fields. However, there are so many examples in the literature of algebraic varieties violating it.

In this chapter we introduce and relate some other (cohomological) obstructions to the existence of rational points on an algebraic variety, which are finer than the Hasse principle. We focus mainly on the Brauer-Manin obstruction and how it is related to the descent obstruction. This relation, especially in the form in which we present the main theorem of descent theory in the last section of the chapter, is one of the key points in the proof of our main result.

This is not intended to be a detailed exposition on the topic, but rather an introduction to some techniques that we need later on for our purposes. For this reason, we omit lots of details and proofs which are beyond the scope of this work, for which we give several references throughout the chapter. There is a very good survey of B. Poonen [**Poo**] on the topic, which is plenty of extra references for the interested reader.

1. Choosing a good cohomology theory

From Theorem 1.36 we know that the Brauer group of a field k has a cohomological interpretation. Namely, if $G_k = \mathrm{Gal}\,(k^s/k)$, there is an isomorphism of abelian groups

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

where the right-hand side is the second Galois cohomology group of k with coefficients in the multiplicative group $\mathbb{G}_m$. With an appropriate cohomology theory, this interpretation of the Brauer group will lead us to define the Brauer group of an arbitrary scheme.

In this section we present briefly the *étale* (and *fppf*) cohomology, following the exposition from Chapter 6 of [**Poo**]. For the details, we refer to the classical texts with the foundational material on this topic, as for example [**Del77**], [**Mil80**].

Before that, let us motivate why we need "alternative" cohomology theories. Suppose X is a compact complex manifold. Then, one can define as usual the singular cohomology groups $\mathrm{H}^i(X,\mathbb{Z}), \mathrm{H}^i(X,\mathbb{Z}/n\mathbb{Z})$ and so on, or one can even define cohomology of coherent analytic sheaves. But these cohomology theories use the analytic topology on X, which we are not able to work with in general when dealing with varieties over fields other than $\mathbb{C}$.

In order to measure the success of a new cohomology theory, we should check if it gives the answers we expect from the classical theories (such as singular cohomology) for proper varieties over $\mathbb{C}$ (see for example [**Har77**, Appendix C] for the case of ℓ-adic cohomology). If we consider the Zariski topology, for example, we will get the right answers for cohomology of coherent sheaves, but it is not a fine enough topology for giving the correct answers for constant coefficients: for a sufficiently nice complex curve X of genus g, it turns out that using the Zariski topology $\mathrm{H}^1(X,\mathbb{Z}) = 0$ because the constant sheaf $\mathbb{Z}$ is *flasque*, while using singular cohomology $\mathrm{H}^1(X(\mathbb{C}),\mathbb{Z}) \simeq \mathbb{Z}^{2g}$.

When working with schemes, A. Grothendieck noticed that sometimes one does not need to know the open sets of the topology; for many purposes, it suffices to have a notion of open covering. Grothendieck took this idea one step further obtaining sufficiently fine 'topologies'[1] on a scheme, built up from a notion of 'open covering' which need not consist of actual open sets. More precisely,

Definition 3.1. *Let $\mathcal{C}$ be a category, and consider all families of morphisms $\{U_i \to U\}_{i\in I}$ in $\mathcal{C}$ having a common target. A* Grothendieck topology *on $\mathcal{C}$ is a set $\mathcal{T}$ consisting on some of these families (which are called the* open coverings *of $\mathcal{T}$), satisfying:*

(i) *Isomorphisms are open coverings.*
(ii) *An open covering of an open covering is again an open covering.*
(iii) *A base extension of an open covering is an open covering.*

Then a pair $(\mathcal{C},\mathcal{T})$ as in the definition is called a *site*, and to a scheme X one can associate, among others, the *Zariski* site X_{Zar}, the *étale* site $X_{\text{ét}}$, the *fppf* site X_{fppf} and the *fpqc* site X_{fpqc}. Each of these sites is finer than the previous one, so that one has morphisms of sites

$$X_{\mathrm{fpqc}} \to X_{\mathrm{fppf}} \to X_{\text{ét}} \to X_{\mathrm{Zar}},$$

where a morphism of sites $(\mathcal{C}',\mathcal{T}') \to (\mathcal{C},\mathcal{T})$ is a functor in the opposite direction $\mathcal{C} \to \mathcal{C}'$ taking open coverings to open coverings.

The étale site $X_{\text{ét}}$ is defined by considering $\mathcal{C}$ to be the category $\textbf{Ét}_X$ of schemes U equipped with an étale morphism $U \to X$, and in which morphisms are X-morphisms. In this category morphisms are automatically étale. Then a covering is a family $\{\phi_i : U_i \to U\}$ of morphisms in $\mathcal{C}$ such that $\bigcup \phi_i(U_i) = U$ as topological spaces. As for the *fppf* site X_{fppf}, it is obtained starting with the category $\mathcal{C} = \textbf{Schemes}_X$ of X-schemes, and an open covering is by definition a family $\{\phi_i : U_i \to U\}$ of X-morphisms such that $\coprod U_i \to U$ is faithfully flat and locally of finite presentation ('*fppf*' stands for the french terminology 'fidèlement plat et de présentation finie'). In a similar way one defines the *fpqc* site, where '*fpqc*' stands for 'fidèlement plat quasi-compact' (see [**Poo**, §6.2] for the details).

With this new idea of topology on a scheme, one can define the notions of presheaf and sheaf in the category $\mathcal{C}$ of a site $(\mathcal{C},\mathcal{T})$. Besides the constant presheaves, for a subcategory $\mathcal{C}$ of the category $\textbf{Schemes}_X$ of X-schemes some particularly interesting examples of abelian presheaves are those defined by

$$\begin{aligned}\mathbb{G}_a(U) &:= \mathcal{O}(U),\\ \mathbb{G}_m(U) &:= \mathcal{O}(U)^\times,\\ \mu_n(U) &:= \{s \in \mathcal{O}(U)^\times : s^n = 1\}.\end{aligned}$$

And for a X-scheme Y, we also have the functor of points h_Y defined by $h_Y(U) := \mathrm{Hom}_X(U,Y)$, which is a presheaf of sets (in fact, it is a sheaf on the four sites mentioned above).

[1] These Grothendieck *topologies* are not topologies in the usual sense.

Now we fix a scheme X, and write $X_\bullet$ for either X_{Zar}, $X_{\text{ét}}$ or X_{fppf}. It can be proven that the category of abelian sheaves on $X_\bullet$ has enough injectives, so that we can define cohomology groups as usual in terms of derived functors:

Definition 3.2. *For each integer $q \geq 0$, the functor*

$$\begin{array}{rcl} \{\textit{abelian sheaves on } X_\bullet\} & \longrightarrow & \mathbf{Ab} \\ \mathcal{F} & \longmapsto & \mathrm{H}^q_\bullet(X,\mathcal{F}) \end{array}$$

from the category of abelian sheaves on $X_\bullet$ to the category of abelian groups is defined to be the q^{th} derived functor of the (left exact) global sections functor

$$\begin{array}{rcl} \{\textit{abelian sheaves on } X_\bullet\} & \longrightarrow & \mathbf{Ab} \\ \mathcal{F} & \longmapsto & \mathcal{F}(X). \end{array}$$

For an abelian sheaf $\mathcal{F}$ on $X_\bullet$, the abelian group $\mathrm{H}^q_\bullet(X,\mathcal{F})$ is called the q^{th} Zariski / étale / fppf cohomology group *of $\mathcal{F}$.*

In particular, every short exact sequence of abelian sheaves on $X_\bullet$ induces a long exact sequence in cohomology, just like in the classical cohomology theories.

Example 3.3. *Étale cohomology and Galois cohomology.* Fix a field k and a separable closure k^s of it. The only field extensions L/k for which the morphism of affine schemes $\mathrm{Spec}(L) \to \mathrm{Spec}(k)$ is étale are the finite separable extensions.

For a sheaf $\mathcal{F}$ on $(\mathrm{Spec}(k))_{\text{ét}}$, define $\mathcal{F}(k^s) := \varinjlim \mathcal{F}(\mathrm{Spec}(L))$, where L ranges over all finite separable extensions of k. Note that $\mathcal{F}(k^s)$ is a G_k-set in a natural way, where $G_k = \mathrm{Gal}\,(k^s/k)$, since we can take the direct limit over finite Galois extensions getting the same result. The functor $\mathcal{F} \mapsto \mathcal{F}(k^s)$ from the category of sheaves of sets on $(\mathrm{Spec}(k))_{\text{ét}}$ to the category of G_k-sets is shown to be an equivalence of categories, by which the global section functor $\mathcal{F} \mapsto \mathcal{F}(k)$ corresponds to the functor taking a G_k-set M to its set of G_k-invariants M^{G_k}. Moreover, this equivalence of categories restricts to an equivalence

$$\{\text{abelian sheaves on } (\mathrm{Spec}(k))_{\text{ét}}\} \to \{G_k\text{-modules}\},$$

and as a consequence one gets natural isomorphisms

$$\mathrm{H}^q_{\text{ét}}(\mathrm{Spec}(k),\mathcal{F}) \simeq \mathrm{H}^q(G_k,\mathcal{F}(k^s)), \quad \text{for each integer } q \geq 0,$$

between étale cohomology and Galois cohomology. Therefore, we can think of étale cohomology as a generalization of Galois cohomology for arbitrary schemes.

In general, if $(\mathcal{C},\mathcal{T})$ is a site and $U \in \mathcal{C}$, for an abelian presheaf on $(\mathcal{C},\mathcal{T})$ one can define the Čech cohomology groups $\check{\mathrm{H}}^q(\mathcal{U},\mathcal{F})$ of an open covering $\mathcal{U}$ of U in terms of Čech q-cocycles and Čech q-coboundaries. By ordering the open coverings of U by refinement and taking the direct limit, one defines the *q^{th} Čech cohomology group of U with coefficients in $\mathcal{F}$* by $\check{\mathrm{H}}^q(U,\mathcal{F}) := \varinjlim \check{\mathrm{H}}^q(\mathcal{U},\mathcal{F})$.

These Čech cohomology groups do not coincide in general with the cohomology groups defined via derived functors. For example, $\check{\mathrm{H}}^0(U,\mathcal{F}) \simeq \mathrm{H}^0(U,\mathcal{F}) = \mathcal{F}(U)$ and $\check{\mathrm{H}}^1(U,\mathcal{F}) \simeq \mathrm{H}^1(U,\mathcal{F})$, but $\check{\mathrm{H}}^2(U,\mathcal{F}) \hookrightarrow \mathrm{H}^2(U,\mathcal{F})$. Here cohomology groups are taken with respect to the fixed site.

However, for the case of the étale site on a scheme X there is the following result due to M. Artin (see [**Mil80**, Theorem III.2.17] for a proof):

Theorem 3.4 (M. Artin)**.** *Let X be a quasi-compact scheme such that every finite subset of X is contained in an open affine subset (this is true if X is quasi-projective over an affine scheme). If $\mathcal{F}$ is a sheaf on $X_{\text{ét}}$, then there are canonical isomorphisms*

$$\check{\mathrm{H}}^q_{\text{ét}}(X,\mathcal{F}) \simeq \mathrm{H}^q_{\text{ét}}(X,\mathcal{F})$$

for every integer $q \geq 0$.

In view of the next section, we also quote the next result about the cohomology of $\mathbb{G}_m$:

Proposition 3.5. *Let X be a scheme. Then*

(i) $\mathrm{H}^0_{\mathrm{Zar}}(X,\mathbb{G}_m) \simeq \mathrm{H}^0_{\text{ét}}(X,\mathbb{G}_m) \simeq \mathrm{H}^0_{\mathrm{fppf}}(X,\mathbb{G}_m) \simeq \mathcal{O}_X(X)^\times$.

(ii) $\mathrm{H}^1_{\mathrm{Zar}}(X,\mathbb{G}_m) \simeq \mathrm{H}^1_{\text{ét}}(X,\mathbb{G}_m) \simeq \mathrm{H}^1_{\mathrm{fppf}}(X,\mathbb{G}_m) \simeq \mathrm{Pic}(X)$.

And more generally, for any smooth commutative group scheme G over a scheme X, $\mathrm{H}^q_{\text{ét}}(X,G) \simeq \mathrm{H}^q_{\mathrm{fppf}}(X,G)$ for every integer $q \geq 0$.

The statement (i) is just the definition. Part (ii) is proved in [**Poo**, Proposition 6.6.1] and the last statement follows from [**Gro68**, Théorème 11.7].

2. The Brauer group of a scheme

From the cohomological interpretation of the Brauer group of a field from Chapter 1, and from the Example 3.3 of the previous section, for a field k we have isomorphisms

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

Since the right-hand side makes sense if we replace $\mathrm{Spec}(k)$ by an arbitrary scheme, the following definition is natural:

Definition 3.6. *For any scheme X, the* (cohomological) Brauer group *of X (also called* Grothendieck-Brauer group*) is defined by*

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

And for a commutative ring R, we put $\mathrm{Br}(R) := \mathrm{Br}(\mathrm{Spec}(R))$.

Remark 3.7. We can also use *fppf* cohomology, because of Proposition 3.5.

The functoriality of cohomology groups 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 there is an induced group homomorphism $\mathrm{Br}(Y) \to \mathrm{Br}(X)$.

Proposition 3.8. *Let X be a regular integral noetherian scheme. If $k(X)$ denotes the function field of X, the induced morphism $\mathrm{Br}(X) \to \mathrm{Br}(k(X))$ is injective. In particular, since $\mathrm{Br}(k(X))$ is a Galois cohomology group, $\mathrm{Br}(X)$ is a torsion abelian group.*

2.1. The Azumaya Brauer group.

Just as in the case of the Brauer group of a field k, which can be defined as the set of similarity classes of finite-dimensional central simple algebras, one can define the *(Azumaya) Brauer group* $\mathrm{Br}_{Az}(X)$ of a scheme X in terms of Azumaya algebras on X. As well as matrix algebras over a field k are of the form $\mathrm{End}(V)$ for some finite-dimensional vector space V over k, one can generalize this notion over a scheme X by thinking of the $\mathcal{O}_X$-algebras $\mathrm{End}_{\mathcal{O}_X}(\mathcal{E}) := \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{E},\mathcal{E})$ for some locally free $\mathcal{O}_X$-module $\mathcal{E}$, where $\mathcal{O}_X$ is the structure sheaf of X. With this intuitive idea, *Azumaya algebras* on a scheme X can be regarded as a generalization of central simple algebras over a field k (see [**Poo**, §6.6.3] for the detailed definition). Then, using a suitable equivalence relation among Azumaya algebras one defines the Azumaya Brauer group $\mathrm{Br}_{Az}(X)$ of a scheme X, and Br_{Az} is a contravariant functor from the category of schemes to the category of abelian groups. As a first important fact, one has:

Proposition 3.9. *An Azumaya algebra on X that is locally free of rank n^2 defines an element of $\mathrm{Br}_{Az}(X)$ that is killed by n. In particular, if X is a scheme with finitely many components, then $\mathrm{Br}_{Az}(X)$ is a torsion abelian group.*

In order to compare the cohomological Brauer group with the Azumaya Brauer group, recall that central simple algebras of dimension n^2 over a field k are classified up to isomorphism by $\mathrm{H}^1(k,\mathrm{PGL}_n)$ (see Remark 1.38). In a similar way, using Čech cohomology and *fpqc* descent, Azumaya algebras of rank n^2 over a scheme X are classified by $\mathrm{H}^1(X,\mathrm{PGL}_n)$. Then, the short exact sequence of sheaves (on the sites $X_{\text{ét}}$ or X_{fppf})

$$0 \to \mathbb{G}_m \to \mathrm{GL}_n \to \mathrm{PGL}_n \to 0$$

gives rise via the connecting homomorphism of the associated long exact sequence to a map $\mathrm{H}^1(X, \mathrm{PGL}_n) \to \mathrm{H}^2(X, \mathbb{G}_m) = \mathrm{Br}(X)$. Hence, each Azumaya algebra of rank n^2 gives rise to an element of $\mathrm{Br}(X)$. For Azumaya algebras of non-constant rank, one can use the same construction on each open and closed subset of X where the rank is constant, since they have locally constant rank.

This map we have just described leads us to think about a nice comparison between $\mathrm{Br}_{Az}(X)$ and $\mathrm{Br}(X)$. In general, these groups are not isomorphic, but for the case we are interested in they are. The whole picture is summarized in the following theorem:

Theorem 3.10. *For any scheme X, the above map $\mathrm{Br}_{Az}(X) \to \mathrm{Br}(X)$ is an injective homomorphism. If X has an invertible sheaf (e.g., if X is quasi-projective over $\mathrm{Spec}(A)$ for some noetherian ring A), then this injection induces an isomorphism $\mathrm{Br}_{Az}(X) \simeq \mathrm{Br}(X)_{tors}$. In particular, if X is a regular quasi-projective variety over a field, then $\mathrm{Br}_{Az}(X) \simeq \mathrm{Br}(X)_{tors} = \mathrm{Br}(X)$.*

3. The Brauer-Manin obstruction

Let k be a global field (for example, a number field) and let X be a k-variety[2]. If $x \in X(k)$ is a k-rational point, we can regard it as a morphism of schemes $x : \mathrm{Spec}(k) \to X$, and by functoriality this morphism induces a group homomorphism $\mathrm{Br}(X) \to \mathrm{Br}(k)$. If $A \in \mathrm{Br}(X)$, let us denote by $A(x) \in \mathrm{Br}(k)$ the image of A under this map. We can do the same locally at each place of k. That is, for a place v of k and a k_v-rational point $x_v : \mathrm{Spec}(k_v) \to X$, consider the induced group homomorphism $\mathrm{Br}(X) \to \mathrm{Br}(k_v)$ and denote by $A(x_v) \in \mathrm{Br}(k_v)$ the image of an element $A \in \mathrm{Br}(X)$ under this map. Then, the key property of these group homomorphisms is the following (see [**Poo**, Proposition 8.3.1]):

Lemma 3.11. *If $\{x_v\} \in X(\mathbb{A}_k)$, then $A(x_v) = 0$ for almost all places v of k.*

If we recall the map $\mathrm{inv}_v : \mathrm{Br}(k_v) \to \mathbb{Q}/\mathbb{Z}$ from Chapter 1, then

$$\begin{aligned} \mathrm{Br}(X) \times X(\mathbb{A}_k) &\longrightarrow \mathbb{Q}/\mathbb{Z} \\ (A, \{x_v\}) &\longmapsto \langle A, \{x_v\} \rangle := \sum_v \mathrm{inv}_v(A(x_v)) \end{aligned} \tag{4}$$

is a well-defined pairing, since the above lemma ensures that the sum is finite. Now, fix $A \in \mathrm{Br}(X)$ and consider the commutative diagram

$$\begin{tikzcd} & X(k) \arrow[r, hook] \arrow[d, "A"'] & X(\mathbb{A}_k) \arrow[d, "A"'] & & \\ 0 \arrow[r] & \mathrm{Br}(k) \arrow[r] & \bigoplus_v \mathrm{Br}(k_v) \arrow[r, "\sum \mathrm{inv}_v"] & \mathbb{Q}/\mathbb{Z} \arrow[r] & 0, \end{tikzcd}$$

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

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

This argument using the pairing (4) leads to the definition of the Brauer set of the k-variety X. First, for each element $A \in \mathrm{Br}(X)$ put

$$X(\mathbb{A}_k)^A := \{\{x_v\} \in X(\mathbb{A}_k) : \langle A, \{x_v\} \rangle = 0\}.$$

Definition 3.12. *The* Brauer set *of X is defined to be*

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

[2] We use the term *k-variety* as a synonym of *variety over k*. And by a variety over a field k we understand a separated scheme X of finite type over $\mathrm{Spec}(k)$.

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

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

By construction, we thus obtain:

Corollary 3.13. *For any k-variety X, we have*

$$X(k) \subseteq X(\mathbb{A}_k)^{\mathrm{Br}}.$$

Therefore, for a k-variety X we have a chain of inclusions $X(k) \subseteq X(\mathbb{A}_k)^{\mathrm{Br}} \subseteq X(\mathbb{A}_k)$. One hopes the last inclusion to be strict in many cases, so that looking for the emptiness of the Brauer set would be a better criterion for the non-existence of rational points on X than looking for the emptiness of $X(\mathbb{A}_k)$.

Definition 3.14. *We say that there is a* Brauer-Manin obstruction to the local-global principle *for X if $X(\mathbb{A}_k) \neq \emptyset$ but $X(\mathbb{A}_k)^{\mathrm{Br}} = \emptyset$.*

Moreover, for a class of smooth, projective and geometrically integral varieties X over global fields, 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 family. In relation with this parlance one finds several conjectures in the literature which are still open. One of them is attributed to Poonen (see [**Poo06**]) and deals with the case of curves:

Conjecture 3.15 (Poonen)**.** *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.*

Since the problem of finding obstructions to the Hasse principle is closely related to the Hilbert's 10th Problem and undecidability, it is natural to ask if it is possible to effectively compute the Brauer-Manin obstruction. J.-L Colliot-Thélène, D. Kanevsky and J.-J. Sansuc ([**CT86**]) 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 is the only one for this family of varieties.

Another conjecture attributed to Colliot-Thélène in this direction is the following:

Conjecture 3.16 (Colliot-Thélène)**.** *The Brauer-Manin obstruction to the local-global principle is the only one for the class of smooth, proper, geometrically integral and rationally connected varieties over number fields.*

This conjecture appears as Conjecture 3.2 in [**PV04**] and has a long history (see Remark 3.3 in the same reference).

4. Torsors and descent

Now we move on to descent theory, and first we need to define what are *torsors*. These objects are the fundamental ingredient of the descent obstruction, to be introduced later. First we define torsors over a field, and then we generalize them to torsors over an arbitrary base scheme, giving a cohomological interpretation in each case.

Let k be a field, and let G be an algebraic group over k. Being G both a group and a k-variety, we say that G equipped with the right action of itself by translation is *the trivial k-torsor under G*, and we denote it by $\mathbf{G}$. Generalizing this idea to arbitrary k-varieties, we get the definition of a torsor over a field:

Definition 3.17. *A* (right) k-torsor under G *(or a* principal homogeneous space of G*) is a k-variety X equipped with a right action of G such that X_{k^s} equipped with its right G_{k^s}-action is isomorphic to $\mathbf{G}_{k^s}$ (here, the isomorphism must respect the right actions of G_{k^s}). A* morphism of k-torsors *under G is just a G-equivariant morphism of k-schemes.*

Note 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".

By definition, we have that

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

and therefore

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

Intuitively, k-torsors under G are analogous to cosets of a group G in some larger group, or to translates of a subspace G in some larger vector space. In order to trivialize 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 exist over the ground field. Indeed, we have:

Proposition 3.18. *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 $\mathrm{H}^1(k, G)$.*

Generalizing k-torsors under an algebraic k-group G, there is the notion of torsors under a group scheme G over a general base scheme, which can be thought as families of torsors.

Definition 3.19. *Let G be a group scheme over S such that the structure morphism $G \to S$ is fppf (a fppf group scheme, for short). 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*

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

is an isomorphism.

As we have said above, k-torsors under an algebraic group G are classified by the Galois cohomology group $\mathrm{H}^1(k, G)$. Moreover, by using Example 3.3 and Proposition 3.5 from the last chapter we have

$$\frac{\{k\text{-torsors under } G\}}{k\text{-isomorphism}} \simeq \mathrm{H}^1_{\text{ét}}(\mathrm{Spec}(k), G) \simeq \mathrm{H}^1_{\text{fppf}}(\mathrm{Spec}(k), G).$$

Now, one can relate S-torsors under an *fppf* group scheme G over S with $\check{\mathrm{H}}^1_{\text{fppf}}(S, G)$ (as a pointed set), but in general this relation is not as clear as the above one. Instead of classifying torsors under G, it turns out that $\check{\mathrm{H}}^1_{\text{fppf}}(S, G)$ classifies isomorphism classes of what are called *torsors sheaves* under G (see [**Mil80**, Proposition III.4.6]), and one has an injection

$$\frac{\{S\text{-torsors under } G\}}{S\text{-isomorphism}} \hookrightarrow \frac{\{S\text{-torsor sheaves under } G\}}{S\text{-isomorphism}} \simeq \check{\mathrm{H}}^1_{\text{fppf}}(S, G). \tag{5}$$

If G is commutative, then $\mathrm{H}^1_{\text{fppf}}(S, G)$ is defined and indeed we have an isomorphism of groups $\check{\mathrm{H}}^1_{\text{fppf}}(S, G) \simeq \mathrm{H}^1_{\text{fppf}}(S, G)$. Moreover, it is often true that torsor sheaves are representable by torsor schemes, so that the above injection is an isomorphism under some extra conditions (see [**Poo**, Theorem 6.5.10]). For example, when any of the following ones is satisfied:

(a) $G \to S$ is an affine morphism.
(b) G is smooth and separated over S, and $\dim(S) \leq 1$.
(c) G is smooth and proper over S with geometrically connected fibres, and is regular.

Hence, in these cases, we have that

$$\frac{\{S\text{-torsors under } G\}}{S\text{-isomorphism}} \simeq \check{\mathrm{H}}^1_{\mathrm{fppf}}(S,G).$$

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 will mean a right *fppf* X-torsor under the base extension G_X. We will write simply $\mathrm{H}^1(X,G)$ for the pointed set $\check{\mathrm{H}}^1_{\mathrm{fppf}}(X,G)$.

Let $Z \xrightarrow{f} X$ be an X-torsor under an algebraic group G over k, and denote by ζ its class in $\mathrm{H}^1(X,G)$ (using (5)). For a k-rational point $x \in X(k)$, the fibre $Z_x \to x$ is a k-torsor under G, and thus it defines a class in $\mathrm{H}^1(k,G)$, which we denote by $\zeta(x)$. In other words, x can be thought as a morphism of schemes $x : \mathrm{Spec}(k) \to X$, hence by functoriality it defines a morphism in cohomology $\mathrm{H}^1(X,G) \to \mathrm{H}^1(k,G)$ sending ζ to $\zeta(x)$. Summing up, the torsor $Z \to X$ gives us an "evaluation" map

$$\begin{array}{ccc} X(k) & \longrightarrow & \mathrm{H}^1(k,G) \\ x & \longmapsto & \zeta(x). \end{array}$$

Remark 3.20. This map makes explicit a fact quoted before without details, namely that a torsor $Z \to X$ can be thought as a family of k-torsors parametrized by X.

This evaluation map allows us to partition the set $X(k)$ by packing together the rational points whose fibres define the same class in $\mathrm{H}^1(k,G)$. That is,

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

Now the key point is that the right-hand side can be reinterpreted by introducing the notion of *twisted torsor*:

Theorem 3.21. *Let k be a field and let X be a k-variety. Suppose that $f : Z \to X$ is an X-torsor under an affine algebraic group G over k, and denote by $\zeta \in \mathrm{H}^1(X,G)$ its class. For each $\tau \in \mathrm{H}^1(k,G)$ one can define a "twisted torsor" $f^\tau : Z^\tau \to X$ such that $\{x \in X(k) : \zeta(x) = \tau\} = f^\tau(Z^\tau(k))$. In particular,*

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

Proof. We assume G is commutative. First we relate $f(Z(k))$ with the neutral element of $\mathrm{H}^1(k,G)$. By Proposition 3.18, 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 neutral 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 by 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 G is commutative, we can consider a cocycle representing $\zeta - \tau_X \in \mathrm{H}^1(X,G)$, which gives rise to a torsor $f^\tau : Z^\tau \to X$ under G (because G is affine). Then, if $x \in X(k)$ we have $(\zeta - \tau_X)(x) = \zeta(x) - \tau$ and

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

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

For the case where G is non-commutative, the construction of Z^τ is more technical and we refer the reader to [**Poo**, Theorem 8.2.1]. □

From now on assume that k is a number field, and let S be a finite set of places of k. For each place v of k, the inclusion of fields $k \hookrightarrow k_v$ induces a map in *fppf* cohomology $\mathrm{H}^1(k,G) \to \mathrm{H}^1(k_v,G)$, which coincides with the restriction map of Galois cohomology given by the inclusion $\mathrm{Gal}\,(k_v^s/k_v) \hookrightarrow \mathrm{Gal}\,(k^s/k)$ as a decomposition group. For $\tau \in \mathrm{H}^1(k,G)$, we denote by $\tau_v \in \mathrm{H}^1(k_v,G)$ its image.

In this situation, many of the twisted torsors f^τ do not contribute in the decomposition of $X(k)$ of the last theorem. The relevant ones are indexed by the *Selmer set*:

Definition 3.22. *The* Selmer set *of the torsor $f : Z \to X$ is the following subset of $\mathrm{H}^1(k,G)$:*

$$\mathrm{Sel}_{Z,S}(k,G) := \{\tau \in \mathrm{H}^1(k,G) : Z^\tau(k_v) \neq \emptyset \textit{ for all } v \notin S\}.$$

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

$$X(k) = \bigsqcup_{\tau\in\mathrm{Sel}_{Z,S}(k,G)} f^\tau(Z^\tau(k)). \tag{6}$$

Remark 3.23. Note that this is true for any finite set S of places of k.

Then, what makes this decomposition interesting is the following strong result (see [**Poo**, Theorem 8.2.5]):

Theorem 3.24. *If k is a number field and X is proper over k, then $\mathrm{Sel}_{Z,S}(k,G)$ is finite.*

With the above notations, the finiteness of the Selmer set when X is proper implies that the decomposition (6) is a finite union. This makes especially interesting the descent obstruction, which we now explain.

Recall that $X(\mathbb{A}_k)$ can be identified with $\prod_v' X(k_v)$, where the restricted product is taken with respect to the sets $X(R_v)$, where R_v is the ring of integers of k_v. Then, the set $X(k)$ can be embedded diagonally into $X(\mathbb{A}_k)$, and we write as usual $\{x_v\}$ for the image of a point $x \in X(k)$. A torsor $f : Z \to X$ under an affine algebraic group G over k imposes restrictions on the image of $X(k)$ into $X(\mathbb{A}_k)$. More precisely, using the evaluation map the commutative diagram

$$\begin{tikzcd} X(k) \arrow[r, hook] \arrow[d] & X(\mathbb{A}_k) \arrow[d] \\ \mathrm{H}^1(k,G) \arrow[r] & \prod_v \mathrm{H}^1(k_v,G) \end{tikzcd} \tag{7}$$

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

$$X(\mathbb{A}_k)^f := \left\{ \{x_v\} \in X(\mathbb{A}_k) \text{ whose image in } \prod_v \mathrm{H}^1(k_v,G) \text{ comes from } \mathrm{H}^1(k,G) \right\}.$$

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

$$X(\mathbb{A}_k)^f = \bigcup_{\tau\in\mathrm{H}^1(k,G)} f^\tau(Z^\tau(\mathbb{A}_k)), \tag{8}$$

and here we can replace $\mathrm{H}^1(k,G)$ by $\mathrm{Sel}_{Z,\emptyset}(k,G)$.

We can repeat this argument for all the X-torsors under some affine algebraic group G over k, so that the restrictions sum up, and defining

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

we get inclusions

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

Definition 3.25. *We say that there is a* descent obstruction to the local-global principle *for X if $X(\mathbb{A}_k) \neq \emptyset$ but $X(\mathbb{A}_k)^{\mathrm{descent}} = \emptyset$.*

5. Descent obstruction versus Brauer-Manin obstruction

In this section we compare the obstructions to the existence of rational points we have presented along the chapter. It turns out that the descent obstruction is stronger than the Brauer-Manin obstruction.

From section 2.1 of this chapter, we have a map

$$\mathrm{H}^1(X, \mathrm{PGL}_n) \to \mathrm{Br}(X)[n],$$

since an Azumaya algebra of rank n^2 is killed by n. But observe that $\mathrm{H}^1(X, \mathrm{PGL}_n)$ also classifies isomorphism classes of X-torsors under the affine group PGL_n. This observation is the starting point to compare the descent obstruction with the Brauer-Manin obstruction. The technical part is achieved by the following lemma.

Lemma 3.26. *Let k be a global field and X a k-variety. Let $f : Z \to X$ be an X-torsor under PGL_n for some integer $n \geq 1$. If $A \in \mathrm{Br}(X)$ denotes the image of its class in $\mathrm{H}^1(X, \mathrm{PGL}_n)$, then $X(\mathbb{A}_k)^f = X(\mathbb{A}_k)^A$.*

Proof. We must show that $\{x_v\} \in X(\mathbb{A}_k)^f$ if and only if $\{x_v\} \in X(\mathbb{A}_k)^A$. So start taking any $\{x_v\} \in X(\mathbb{A}_k)$. Then all comes from the commutative diagram

$$\begin{tikzcd}
\mathrm{H}^1(X, \mathrm{PGL}_n) \arrow[r] \arrow[d, "\{x_v\}"] & \mathrm{Br}(X)[n] \arrow[d, "\{x_v\}"'] \\
\prod_v \mathrm{H}^1(k_v, \mathrm{PGL}_n) \arrow[r, "\sim"] & \prod_v \mathrm{Br}(k_v)[n] \\
\mathrm{H}^1(k, \mathrm{PGL}_n) \arrow[r, "\sim"] \arrow[u, "\mathrm{res}_1"] & \mathrm{Br}(k)[n]. \arrow[u, "\mathrm{res}_2"']
\end{tikzcd}$$

Here, the vertical arrows going down are evaluation at $\{x_v\}$, while res_1 and res_2 are induced by $k \to k_v$. The middle horizontal bijection identifies the images of res_1 and res_2. Therefore, the class of f in $\mathrm{H}^1(X, \mathrm{PGL}_n)$ maps down to $\mathrm{im}(\mathrm{res}_1)$ if and only if $A \in \mathrm{Br}(X)[n]$ maps down to $\mathrm{im}(\mathrm{res}_2)$. Equivalently, $\{x_v\} \in X(\mathbb{A}_k)^f$ if and only if $\{x_v\} \in X(\mathbb{A}_k)^A$, as we desired. □

In view of this lemma, and imitating the definition of $X(\mathbb{A}_k)^{\mathrm{descent}}$, we should define

$$X(\mathbb{A}_k)^{\mathrm{PGL}} := \bigcap_{\substack{n \geq 1 \\ f: Z \to X \text{ under } \mathrm{PGL}_n}} X(\mathbb{A}_k)^f.$$

Proposition 3.27. *Let k be a global field. Let X be a regular quasi-projective k-variety. Then*

$$X(\mathbb{A}_k)^{\mathrm{descent}} \subseteq X(\mathbb{A}_k)^{\mathrm{PGL}} = X(\mathbb{A}_k)^{\mathrm{Br}}.$$

In particular, the descent obstruction is stronger than the Brauer-Manin obstruction.

Proof. Under the hypotheses, $\mathrm{Br}(X)$ is torsion (see Theorem 3.10), so that every $A \in \mathrm{Br}(X)$ is in the image of the map $\mathrm{H}^1(X, \mathrm{PGL}_n) \to \mathrm{Br}(X)[n]$ for some n. Therefore, applying the above lemma we get

$$X(\mathbb{A}_k)^{\mathrm{Br}} = \bigcap_{A \in \mathrm{Br}(X)} X(\mathbb{A}_k)^A = \bigcap_{\substack{n \geq 1 \\ f: Z \to X \text{ under } \mathrm{PGL}_n}} X(\mathbb{A}_k)^f = X(\mathbb{A}_k)^{\mathrm{PGL}}.$$

On the other hand, each PGL_n is an affine algebraic group, so by definition the inclusion $X(\mathbb{A}_k)^{\mathrm{descent}} \subseteq X(\mathbb{A}_k)^{\mathrm{PGL}}$ holds and the theorem follows. □

Remark 3.28. This comparison between the obstructions gives rise to an obvious question: is the descent obstruction strictly stronger than the Brauer-Manin obstruction? In other words, are there examples of regular quasi-projective varieties over a field k for which $X(\mathbb{A}_k)^{\mathrm{Br}} \neq \emptyset$ but $X(\mathbb{A}_k)^{\mathrm{descent}} = \emptyset$? In this direction, 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 the *étale-Brauer obstruction* (to be introduced below) to explain the emptiness of $X(\mathbb{Q})$.

5.1. The étale-Brauer obstruction. By Proposition 3.27, we have seen that the descent obstruction is stronger than the Brauer-Manin obstruction for a regular quasi-projective variety over a global field. Now we present a combination of the ideas leading to these obstructions that gives rise to a new kind of obstruction, named the *étale-Brauer obstruction*, which roughly speaking is defined by applying the Brauer-Manin obstruction to certain étale covers of X.

So let k be a global field and X a k-variety. If $f : Z \to X$ is a torsor under an affine algebraic group G, recall that $X(k)$ can be recovered by the sets of k-rational points on the twists of Z, that is (see Theorem 3.21):

$$X(k) = \bigsqcup_{\tau \in \mathrm{H}^1(k,G)} f^\tau(Z^\tau(k)) \subseteq \bigcup_{\tau \in \mathrm{H}^1(k,G)} f^\tau(Z^\tau(\mathbb{A}_k)).$$

In fact, recall that the right-hand side equals $X(\mathbb{A}_k)^f$, which is the contribution of the torsor f in the descent obstruction. Now, if we replace $Z^\tau(\mathbb{A}_k)$ by $Z^\tau(\mathbb{A}_k)^{\mathrm{Br}}$ we can expect to obtain a better "upper bound" for $X(k)$. Then, the *étale-Brauer set* of X is defined to be

$$X(\mathbb{A}_k)^{\text{ét},\mathrm{Br}} := \bigcap_{\substack{\text{finite étale } G \\ f:Z\to X \text{ under } G}} \bigcup_{\tau \in \mathrm{H}^1(k,G)} f^\tau(Z^\tau(\mathbb{A}_k)^{\mathrm{Br}}),$$

which is obtained from applying the Brauer-Manin obstruction to all X-torsors under finite étale group schemes.

Definition 3.29. *We say that there is an* étale-Brauer obstruction to the local-global principle *for X if $X(\mathbb{A}_k) \neq \emptyset$ but $X(\mathbb{A}_k)^{\text{ét},\mathrm{Br}} = \emptyset$.*

In the same fashion, we can also define possibly smaller subsets

$$X(\mathbb{A}_k)^{\text{ét},\text{descent}} := \bigcap_{\substack{\text{finite étale } G \\ f:Z\to X \text{ under } G}} \bigcup_{\tau \in \mathrm{H}^1(k,G)} f^\tau(Z^\tau(\mathbb{A}_k)^{\text{descent}}),$$

or even $X(\mathbb{A}_k)^{\text{descent},\text{descent}}$ and so on.

Remark 3.30. In a recent article [**Poo10**], for any global field k of characteristic not equal to 2, Poonen constructs a threefold X over k such that $X(k) = \emptyset$ but $X(\mathbb{A}_k)^{\text{ét},\mathrm{Br}} \neq \emptyset$. Then, in the same direction of Remark 3.28, he asked if such a counterexample to the Hasse principle could be explained by the descent obstruction. And more generally, he asked whether one always has the inclusion

$$X(\mathbb{A}_k)^{\text{ét},\mathrm{Br}} \subseteq X(\mathbb{A}_k)^{\text{descent}}.$$

As an answer to the questions arising from Remarks 3.28 and 3.30, it has been recently proved that the étale-Brauer obstruction is equivalent to the descent obstruction for certain varieties over number fields. In particular, the counterexample to the Hasse principle proposed by Poonen cannot be explained in terms of descent:

Theorem 3.31 (Demarche-Skorobogatov)**.** *Let k be a number field, and let X be a smooth, projective, geometrically integral k-variety. Then*

$$X(\mathbb{A}_k)^{\text{ét},\mathrm{Br}} = X(\mathbb{A}_k)^{\text{ét},\text{descent}} = X(\mathbb{A}_k)^{\text{descent}}.$$

Observe that it suffices to show the following chain of inclusions:

$$X(\mathbb{A}_k)^{\text{descent}} \subseteq X(\mathbb{A}_k)^{\text{ét},\text{descent}} \subseteq X(\mathbb{A}_k)^{\text{ét},\mathrm{Br}} \subseteq X(\mathbb{A}_k)^{\text{descent}}.$$

The second inclusion can be deduced by applying Proposition 3.27 to étale covers of X. However, the first and third inclusions are more difficult. Chronologically, the third one was the first to be proved, and it was done by C. Demarche [**Dem09**], using some previous results of D. Harari and M. V. Borovoi. The idea is to show that the subset of $X(\mathbb{A}_k)$ cut out by the torsors under all connected affine algebraic groups equals $X(\mathbb{A}_k)^{\mathrm{Br}}$.

A little bit later, Skorobogatov proved the first inclusion in [**Sko09**], generalizing a result of M. Stoll. The essence of the idea is to show that if Y is an X-torsor under a finite étale group scheme, and Z is a Y-torsor under an affine algebraic group, then Z is dominated by some X-torsor under an even larger affine algebraic group; indeed, this is analogous to the fact that a Galois extension of a Galois extension of a field k is contained in some even larger Galois extension of k.

6. About the main theorem of descent theory

At this point we have already introduced the Brauer-Manin obstruction, as well as the usual obstructions coming from the theory of torsors and descent. Furthermore, we have seen how they are related, especially in Proposition 3.27 and Theorem 3.31.

In this last section of the chapter we adapt the main theorem of the descent theory of Colliot-Thélène and Sansuc (see [**Sko01**, Thm. 6.1.2]). For doing so, we need to introduce a few more concepts, starting with that of torsors under groups of *multiplicative type*.

So, suppose as usual that X is a projective variety over a number field k, and write $\overline{X}$ for the base extension $\overline{X} = X \times_k \bar{k}$. With analogous notations, a commutative algebraic k-group G 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 $n \geq 1$, where $\mathbb{G}_m$ is the multiplicative group. 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 $G_k = \mathrm{Gal}\,(\bar{k}/k)$. Indeed, $G \mapsto \widehat{G}$ gives an anti-equivalence of categories between the category of k-groups of multiplicative type and the category of continuous G_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 $\mathbb{G}_m$ is just a line bundle over X with the zero section removed, so these objects are parametrized by $\mathrm{Pic}(X) = \mathrm{H}^1(X, \mathbb{G}_m)$. In general, we already know that X-torsors under a commutative group G are classified by the étale cohomology group $\mathrm{H}^1(X, G)$. In this context, the canonical cup-pairing

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

gives us a map $\mathrm{H}^1(\overline{X}, \overline{G}) \to \mathrm{Hom}(\widehat{G}, \mathrm{Pic}(\overline{X}))$. Then, combining it with the natural map $\mathrm{H}^1(X, G) \to \mathrm{H}^1(\overline{X}, \overline{G})$ we get a map

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

The image of the class of a torsor $f : Y \to X$ under G under this map is called the *type* of the torsor, and we will denote it by *type*(Y, f). There is a nice and useful description of $\mathrm{H}^1(X, G)$, for G a k-group of multiplicative type, provided by the exact sequence of Colliot-Thélène and Sansuc (see [**Sko01**, Thm. 2.3.6]), which for projective k-varieties looks like follows:

$$0 \to \mathrm{H}^1(k, G) \to \mathrm{H}^1(X, G) \xrightarrow{\chi} \mathrm{Hom}_{G_k}(\widehat{G}, \mathrm{Pic}(\overline{X})) \to \mathrm{H}^2(k, G) \to \mathrm{H}^2(X, G). \tag{9}$$

Here the map χ takes the class of an X torsor under G to its type, up to sign.

Finally, we need to define the *algebraic* Brauer group of X, which leads to the so-called *algebraic part* of the Brauer-Manin obstruction. It is the subgroup

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

where $\mathrm{Br}(X) \to \mathrm{Br}(\overline{X})$ is induced by the natural map $\overline{X} \to X$. Note that we then have $X(\mathbb{A}_k)^{\mathrm{Br}} \subseteq X(\mathbb{A}_k)^{\mathrm{Br}_1(X)}$.

And now, we present the main theorem of Colliot-Thélène and Sansuc announced before, which tells us that the information given by torsors under groups of multiplicative type can also be obtained via the Brauer-Manin obstruction. In our context, the result can be stated as follows (see [**Sko01**, Thm. 6.1.2] for the general statement):

Theorem 3.32 (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 G_k-submodules of $\mathrm{Pic}(\overline{X})$ of finite type.

We want to note 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 (9) we have that all torsors of a given type can be obtained from one such torsor by *twisting*. Hence, fixed a type λ, the union of the sets $f(Y(\mathbb{A}_k))$ over the torsors $f : Y \to X$ of type λ is just the union of the sets $f^\tau(Y^\tau(\mathbb{A}_k))$ where τ runs in $\mathrm{H}^1(k, G)$. Therefore, if one shows that for a torsor $f : Y \to X$ under G of a certain type no twist of f (including f itself) has points everywhere locally, then according to the theorem we will have $X(\mathbb{A}_k)^{\mathrm{Br}_1(X)} = \emptyset$, hence also $X(\mathbb{A}_k)^{\mathrm{Br}} = \emptyset$.

Remark 3.33. As a final comment, after introducing several kinds of obstructions and comparing them, with special attention to Proposition 3.27 and Theorems 3.31 and 3.32, we want to make a remark on Conjecture 3.15. It is only stated for curves, so that the examples of Skorobogatov and Poonen in dimension 2 and 3 are not in contradiction with the hope that this conjecture holds true, as well as they show that a generalization to higher dimensional varieties is not possible. On the other hand, if the conjecture holds true, since the Brauer-Manin obstruction is the least finer obstruction among the introduced ones, it will follow that all of them represent the same obstruction for curves.

Chapter 4
The work of B. W. Jordan

After the algebro-geometric incursion of the last chapter, we come back to Shimura varieties. In fact, from now on we restrict ourselves to Shimura curves. In this chapter, we review part of the work of Jordan in both his PhD. Thesis [**Jor81**] and [**Jor86**].

The first section is devoted to explain the main results of [**Jor86**] in which we are interested. They are results concerning the existence of rational points over imaginary quadratic fields on the Shimura curve X_B defined by an indefinite rational quaternion algebra B. Rather than going into the details of the proofs, we study in the remaining sections the main ingredients of Jordan's results: the canonical torsion subgroups of the QM-abelian surfaces parametrized by X_B and the Shimura covering of X_B attached to a prime factor of $D = \mathrm{disc}(B)$. These objects are also crucial in Skorobogatov's work and, moreover, we should generalize them to our context in later chapters.

1. Rational points on Shimura curves

Let B be an indefinite rational quaternion division algebra, and denote by $X_B = X_B/\mathbb{Q}$ the canonical model over $\mathbb{Q}$ of the Shimura curve defined by a fixed datum $(B, \mathcal{O}, \varrho)$, as at the end of the first section of Chapter 2. For the study of rational points on the curve X_B over certain fields, the following result due to Shimura is of great importance (see [**Shi75**, Theorem 0]):

Theorem 4.1 (Shimura)**.** *The Shimura curve X_B defined by an indefinite rational quaternion division algebra B has no real points, i.e. $X_B(\mathbb{R}) = \emptyset$.*

In fact, Shimura proved this statement also for higher-dimensional Shimura varieties. As a consequence, we get that X_B has no K-rational points for any totally real number field K.

In [**Jor86**], Jordan studied the problem of identifying the number fields K such that $X_B(K) = \emptyset$, with special interest in imaginary quadratic fields (the next step after Theorem 4.1). In other words, he worked for a description of the set

$$\mathrm{D} = \left\{ (B, K) \;\middle|\; \begin{array}{l} B \text{ an indefinite rational quaternion} \\ \text{division algebra,} \\ K \text{ a number field, } X_B(K) = \emptyset \end{array} \right\}.$$

This is clearly a problem about the arithmetic of Shimura curves, strongly related to the study of the local-global principle on them. Indeed, an obvious subset of D is the set

$$\mathrm{D}_{\mathrm{local}} = \left\{ (B, K) \in \mathrm{D} \;\middle|\; \begin{array}{l} \text{there exists a valuation } v \text{ of } K \text{ with} \\ X_B(K_v) = \emptyset, \text{ where } K_v \text{ is the completion} \\ \text{of } K \text{ with respect to } v \end{array} \right\}.$$

Theorem 4.1 together with results from [**JL85**] (see also [**Jor86**, Theorem 0]) for the non-archimedean case determine $\mathrm{D}_{\mathrm{local}}$, so that Jordan focuses on the study of $\mathrm{D}_{\mathrm{global}} = \mathrm{D} \setminus \mathrm{D}_{\mathrm{local}}$, which can be regarded as a measure of the failure of the Hasse principle for X_B.

As we have pointed before, the notion of field of moduli plays an important role in the study of rational points on X_B. Namely, if k is a field of characteristic zero and $P \in X_B(k)$, then P corresponds to a QM-abelian surface (A, ι) whose field of moduli $M(A, \iota)$ is contained in k, but it does not need to have a model rational over k. In this direction, one of the main theorems in [**Jor86**] is the following really neat condition for a QM-abelian surface to be defined over its field of moduli:

Theorem 4.2 (Jordan)**.** *Suppose k is a field of characteristic zero and (A, ι) is a QM-abelian surface corresponding to a point $P \in X_B(k)$, so that its field of moduli $M(A, \iota)$ is contained in k. Then (A, ι) has a model rational over k if and only if k splits B.*

The necessity of the condition is easily explained: if (A', ι') is a model rational over k for (A, ι), then the action of $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ on holomorphic 1-forms gives rise to an injection $B \hookrightarrow \mathrm{End}_k(\mathrm{H}^0(A', \Omega^1_{/k})) \simeq \mathrm{M}_2(k)$, and hence k splits B. And for the converse, Jordan uses the splitting of the cotangent space $\mathrm{H}^0(A, \Omega^1_{/k})$ induced by the splitting of B by k and a theorem of Shimura (see [**Jor86**, §1]).

Once Theorem 4.2 is established, the problem of deciding whether a given pair $(B, K) \in \mathrm{D}$ translates into a problem on the arithmetic of QM-abelian surfaces. Moreover, one has two cases to deal with arising from the theorem:

(1) K splits B,
(2) K fails to split B.

In the second one, $(B, K) \notin \mathrm{D}$ if and only if there exists a QM-abelian surface (A, ι) whose field of moduli $M(A, \iota)$ is contained in K, but which has no model rational over K. It turns out that Theorem 4.1 together with results from [**JL85**] almost cover this case, and therefore this case is not pursued in [**Jor86**].

For the first case, $(B, K) \notin \mathrm{D}$ if and only if there exists a QM-abelian surface (A, ι) rational over K. The strategy consists on providing necessary conditions for the existence of a QM-abelian surface rational over a field K. Then, whenever one can prove the impossibility of fulfilling one of these conditions it follows that $X_B(K) = \emptyset$, assuming that K splits B. In this direction, the following result is obtained for the case of imaginary quadratic fields:

Theorem 4.3 (Jordan)**.** *If K is imaginary quadratic of class number not equal to 1, then there are only finitely many B such that K splits B and $X_B(K) \neq \emptyset$.*

Remark 4.4. By a result of Shimura, the case of class number 1 is more simple: if K is imaginary quadratic of class number 1 and K splits B, then $X_B(K) \neq \emptyset$.

For the proof of Theorem 4.3, it is a key point to understand the canonical torsion subgroups C_p of a QM-abelian surface (A, ι) attached to the prime factors p of D, as well as the isogeny characters associated to them. These objects were already introduced in Jordan's PhD. Thesis ([**Jor81**]), and some properties about them are established using the theory of abelian surfaces with quaternionic multiplication over finite and local fields (which is reviewed in sections 2 and 3 of [**Jor86**]). From these properties, Jordan proves that the L-function of a QM-abelian surface satisfies certain congruences that conduce finally to the proof of Theorem 4.3. It is also worth to mention that the proof of the above theorem given by Jordan is inspired by the celebrated work of B. Mazur in [**Maz78**].

There is another application in Jordan's article that shows explicitly how the arithmetic of B appears in deciding whether $X_B(K)$ is empty or not. Using the notation from [**Sko05**], for a prime number q, let $P(q)$ be the set of prime factors of the non-zero integers in the set $\{a, a \pm q, a \pm 2q, a^2 - 3q^2\}_{|a| \leq 2q}$. If $q \neq 2$, define $\mathcal{B}(q)$ to be the set of indefinite rational quaternion algebras such that $\mathbb{Q}(\sqrt{-q})$ does not split B, and set also $\mathcal{B}(2)$ to be the set of indefinite rational quaternion algebras such that neither $\mathbb{Q}(\sqrt{-1})$ nor $\mathbb{Q}(\sqrt{-2})$ splits B. Finally, define $\mathcal{C}(q) \subset \mathcal{B}(q)$ to be the set of the indefinite rational quaternion algebras in $\mathcal{B}(q)$ with reduced discriminant divisible by a prime $p \notin P(q)$, and note that $\mathcal{B}(q) \setminus \mathcal{C}(q)$ is finite. Then, we have:

Theorem 4.5 (Jordan)**.** *If K is an imaginary quadratic field in which q is ramified, and $B \in \mathcal{C}(q)$ is split by K, then $X_B(K) = \emptyset$.*

Example 4.6. Consider the indefinite rational quaternion algebra B_{39} of discriminant 39. On the one hand, neither $\mathbb{Q}(\sqrt{-1})$ nor $\mathbb{Q}(\sqrt{-2})$ splits B_{39}, and on the other hand $\mathbb{Q}(\sqrt{-13})$ splits B_{39}. Then, applying the above result for $q = 2$, noting that $P(2) = \{2, 3, 5, 7, 11\}$, we get $X_{B_{39}}(\mathbb{Q}(\sqrt{-13})) = \emptyset$. Indeed, it can be shown that $(B_{39}, \mathbb{Q}(\sqrt{-13})) \in \mathrm{D}_{\mathrm{global}}$, so that $X_{B_{39}}$ is a counterexample to the Hasse principle over $\mathbb{Q}(\sqrt{-13})$.

2. Canonical torsion subgroups and isogeny characters

Now we introduce certain torsion subgroups of the abelian surfaces parametrized by the Shimura curve X_B defined by a fixed quaternionic datum $(B, \mathcal{O}, \varrho)$ as in the previous section. We then assume that the indefinite rational quaternion algebra B is division, which implies $D = \operatorname{disc}(B) > 1$. The material presented here is essentially a review of [**Jor81**, Chapter 4, §3]. Through all this section, let (A, ι) be a QM-abelian surface *defined* over a field k of characteristic zero parametrized by X_B. Recall that, in particular, $\iota : \mathcal{O} \hookrightarrow \operatorname{End}_k(A)$.

In order to understand the torsion subgroups of A, it is important to understand first the subgroups $A[\ell]$ of ℓ-torsion of A for a prime ℓ. In this direction we have the following result due to Morita:

Proposition 4.7 (Morita)**.** *For any prime ℓ, the Tate module $T_\ell(A)$ is free of rank 1 over $\mathcal{O}_\ell = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. Moreover, the commutant of $\mathcal{O}_\ell$ in $\operatorname{End}(T_\ell(A))$ is a subalgebra of $\mathrm{M}_4(\mathbb{Z}_\ell)$ isomorphic to $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$.*

We will use especially the following consequence:

Corollary 4.8. *For any prime ℓ, $A[\ell]$ is free of rank 1 over $\mathcal{O}/\ell\mathcal{O}$.*

Now we fix a rational prime p. Then, recall that $B_p = B \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is isomorphic either to the (unique) quaternion division algebra over $\mathbb{Q}_p$, which we denote by $\mathbb{H}_p$, or to the matrix algebra $\mathrm{M}_2(\mathbb{Q}_p)$, depending on whether p divides D or not, respectively. If $L_p/\mathbb{Q}_p$ denotes the unique unramified quadratic extension of $\mathbb{Q}_p$ and $\sigma \in \operatorname{Gal}(L_p/\mathbb{Q}_p)$ is the nontrivial element, $\mathbb{H}_p$ can be regarded as a subalgebra of $\mathrm{M}_2(L_p)$ by the following description:

$$\mathbb{H}_p \simeq \left\{ \begin{pmatrix} a & b \\ p\,{}^\sigma b & {}^\sigma a \end{pmatrix} : a, b \in L_p \right\} \subseteq \mathrm{M}_2(L_p).$$

And with this presentation, the unique maximal order of $\mathbb{H}_p$ corresponds to

$$\left\{ \begin{pmatrix} a & b \\ p\,{}^\sigma b & {}^\sigma a \end{pmatrix} : a, b \in R_{L_p} \right\},$$

where R_{L_p} stands for the ring of integers of L_p. This dichotomy is translated into the structure of $\mathcal{O}/p\mathcal{O}$:

(i) If $p \nmid D$, then $\mathcal{O}/p\mathcal{O} \simeq \mathrm{M}_2(\mathbb{F}_p)$.

(ii) If $p|D$, then

$$\mathcal{O}/p\mathcal{O} \simeq \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \alpha^p \end{pmatrix} : \alpha, \beta \in \mathbb{F}_{p^2} \right\} \subseteq \mathrm{M}_2(\mathbb{F}_{p^2}).$$

Moreover, these remarks allow us to give an explicit description of the ideals of the $\mathbb{F}_p$-algebra $\mathcal{O}/p\mathcal{O}$:

Proposition 4.9. *Let p be a rational prime.*

(i) *If $p \nmid D$, then the $\mathbb{F}_p$-algebra $\mathcal{O}/p\mathcal{O}$ has exactly $p+1$ non-zero proper left-ideals, which are given by*

$$\mathrm{M}_2(\mathbb{F}_p) \begin{pmatrix} a & 1 \\ a & 1 \end{pmatrix}, \ \textit{for } a \in \mathbb{F}_p, \quad \textit{and} \quad \mathrm{M}_2(\mathbb{F}_p) \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}.$$

(ii) *If $p|D$, then the $\mathbb{F}_p$-algebra $\mathcal{O}/p\mathcal{O}$ has exactly one non-zero proper left ideal, which is given by*

$$\left\{ \begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} : x \in \mathbb{F}_{p^2} \right\} \subseteq \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \alpha^p \end{pmatrix} : \alpha, \beta \in \mathbb{F}_{p^2} \right\} \simeq \mathcal{O}/p\mathcal{O}.$$

The proof of these statements is an easy exercise in terms of matrices. Now the key observation is that since $A[p]$ is a free module of rank 1 over $\mathcal{O}/p\mathcal{O}$, the non-zero proper left ideals of the $\mathbb{F}_p$-algebra $\mathcal{O}/p\mathcal{O}$ are in bijection with the non-zero proper $\mathcal{O}$-submodules of $A[p]$. So the above proposition can be translated into terms of modules and submodules:

Corollary 4.10. *Let p be a rational prime and (A, ι) a QM-abelian surface.*

(i) *If $p \nmid D$, then the $A[p]$ has exactly $p+1$ non-zero proper $\mathcal{O}$-submodules.*

(ii) *If $p|D$, then $A[p]$ has exactly one non-zero proper $\mathcal{O}$-submodule.*

Definition 4.11. *For a prime divisor p of D, the* canonical torsion subgroup of (A, ι) at *p is the unique non-zero proper $\mathcal{O}$-submodule of $A[p]$, and it is denoted by C_p. Its order is p^2.*

In general, for any divisor $d|D$ there exists a unique non-zero proper $\mathcal{O}$-submodule C_d of $A[d]$, which has order d^2. It is called *the canonical torsion subgroup of (A, ι) of reduced order d.*

Proposition 4.12. *If the QM-abelian surface (A, ι) is defined over a field k and C_d is its canonical torsion subgroup of reduced order d, where d is any divisor of D, then C_d is rational over k.*

Proof. More generally, if $\alpha \in \mathrm{Aut}_{\mathcal{O}}(A[d])$ then $\alpha(C_d) \subseteq A[d]$ is a non-zero proper $\mathcal{O}$-submodule of order d^2. By uniqueness, it is C_d. In particular, this holds for any choice of $\alpha \in \mathrm{Im}(\mathrm{Gal}\,(\bar{k}/k) \to \mathrm{Aut}_{\mathcal{O}}(A[d]))$ and the statement follows. □

Remark 4.13. For a prime p dividing D and a QM-abelian surface (A, ι), the construction of the canonical torsion subgroup $C_p \subseteq A[p]$ can be achieved from another perspective, as is done in Skorobogatov's review in [**Sko05**]. It follows from [**Vig80**, p. 86] that there is a unique two-sided ideal $I(p) \subseteq \mathcal{O}$ of reduced norm p, which consists exactly of the elements in $\mathcal{O}$ of reduced norm divisible by p. Then we can consider the kernel of the action of $I(p)$ on A,

$$A[I(p)] = \ker(I(p) : A \to A) = \bigcap_{\beta \in I(p)} \ker(\beta : A \to A) = \{x \in A : \beta \cdot x = 0 \ \forall \beta \in I(p)\},$$

which is an $\mathcal{O}$-submodule of $A[p]$ canonically isomorphic to $\mathcal{O}/I(p) \simeq \mathbb{F}_{p^2}$. Hence by the uniqueness of C_p we have $C_p = A[I(p)]$. As we will see, this approach will be very useful later.

Now we move on to define the isogeny characters, for which we need the action of Galois on the torsion subgroups $A[p]$. From now on we fix a prime p dividing D.

The first observation is that we can consider different structures on the p-torsion subgroup $A[p]$ when working with the Galois action on it. First of all, $A[p]$ is a free $\mathcal{O}/p\mathcal{O}$-module of rank 1. But from the description

$$\mathcal{O}/p\mathcal{O} \simeq \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \alpha^p \end{pmatrix} : \alpha, \beta \in \mathbb{F}_{p^2} \right\} \subseteq \mathrm{M}_2(\mathbb{F}_{p^2})$$

we can define a monomorphism of $\mathbb{F}_p$-algebras

$$\begin{array}{rcl} i : \mathbb{F}_{p^2} & \longrightarrow & \mathcal{O}/p\mathcal{O} \\ \alpha & \longmapsto & \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^p \end{pmatrix} \end{array}$$

which gives $A[p]$ the structure of an $\mathbb{F}_{p^2}$-vector space. Note that $A[p]$ has also a natural structure of an $\mathbb{F}_p$-vector space. Then, the inclusions

$$\mathbb{F}_p \hookrightarrow \mathbb{F}_{p^2} \overset{i}{\hookrightarrow} \mathcal{O}/p\mathcal{O}$$

lead to natural inclusions

$$\mathrm{Aut}_{\mathcal{O}}(A[p]) \hookrightarrow \mathrm{Aut}_{\mathbb{F}_{p^2}}(A[p]) \hookrightarrow \mathrm{Aut}_{\mathbb{F}_p}(A[p]).$$

Now, since the action of $\mathrm{Gal}\,(\bar{k}/k)$ on $A[p]$ commutes with the action of $\mathcal{O}/p\mathcal{O}$, it commutes also with the action of $\mathbb{F}_{p^2}$, making commutative the following diagram:

$$\begin{tikzcd}
& \mathrm{Aut}_{\mathbb{F}_p}(A[p]) \simeq \mathrm{GL}_4(\mathbb{F}_p) \\
\mathrm{Gal}\,(\bar{k}/k) \arrow[ur, "T"] \arrow[r, "\widetilde{T}"] \arrow[dr, "\tau"'] & \mathrm{Aut}_{\mathbb{F}_{p^2}}(A[p]) \simeq \mathrm{GL}_2(\mathbb{F}_{p^2}) \arrow[u, hook] \\
& \mathrm{Aut}_{\mathcal{O}}(A[p]) \simeq (\mathcal{O}/p\mathcal{O})^{\times} \arrow[u, hook]
\end{tikzcd}$$

The two isomorphisms at the top follow from the fact that $A[p]$ is a vector space over $\mathbb{F}_p$ (resp. $\mathbb{F}_{p^2}$) of dimension 4 (resp. 2). On the other hand, the isomorphism $\mathrm{Aut}_{\mathcal{O}}(A[p]) \simeq (\mathcal{O}/p\mathcal{O})^{\times}$ can be constructed easily. Indeed, since $A[p]$ is free of rank 1 over $\mathcal{O}/p\mathcal{O}$, we can choose $x \in A[p]$ such that $A[p] = \mathcal{O}/p\mathcal{O} \cdot x$. Then, for every $f \in \mathrm{Aut}_{\mathcal{O}}(A[p])$, there exists a (uniquely determined) $m_f \in (\mathcal{O}/p\mathcal{O})^{\times}$ such that $f(x) = m_f x$, and the assignation $f \mapsto m_f$ establishes the claimed isomorphism.

Now let $\sigma \in \mathrm{Gal}\,(\bar{k}/k)$ and suppose that

$$\tau(\sigma) = \begin{pmatrix} \alpha & \beta \\ 0 & \alpha^p \end{pmatrix} \in (\mathcal{O}/p\mathcal{O})^{\times}.$$

Then we have

$$\tau(\sigma)\left[\begin{pmatrix} \delta & \gamma \\ 0 & \delta^p \end{pmatrix} \cdot x\right] = \begin{pmatrix} \delta & \gamma \\ 0 & \delta^p \end{pmatrix} \cdot \begin{pmatrix} \alpha & \beta \\ 0 & \alpha^p \end{pmatrix} x \quad \text{for all } \begin{pmatrix} \delta & \gamma \\ 0 & \delta^p \end{pmatrix} \in \mathcal{O}/p\mathcal{O}.$$

In order to go up and describe the representation $\widetilde{T}$, first note that we can choose as a basis for $A[p]$ as an $\mathbb{F}_{p^2}$-vector space the couple

$$\left\{x, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} x\right\}.$$

Then we can write

$$\begin{aligned}
\tau(\sigma)x &= \begin{pmatrix} \alpha & \beta \\ 0 & \alpha^p \end{pmatrix} x = i(\alpha)x + i(\beta)\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} x, \\
\tau(\sigma)\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} x &= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ 0 & \alpha^p \end{pmatrix} x = i(\alpha^p)\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} x.
\end{aligned}$$

From this it follows that, in the chosen basis, the representation $\widetilde{T}$ is then of the form

$$\begin{pmatrix} (\rho_p)^p & 0 \\ * & \rho_p \end{pmatrix} \text{ for some character } \rho_p : \mathrm{Gal}\,(\bar{k}/k) \longrightarrow \mathbb{F}_{p^2}^{\times}.$$

But now we see that this character ρ_p gives the action of $\mathrm{Gal}\,(\bar{k}/k)$ on

$$\mathcal{O}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} x,$$

which is a non-zero proper $\mathcal{O}$-submodule of $A[p]$, hence the canonical torsion subgroup C_p attached to the prime p, which is rational over k. We call

$$\rho_p : \mathrm{Gal}\,(\bar{k}/k) \longrightarrow \mathbb{F}_{p^2}^{\times} \simeq \mathrm{Aut}_{\mathcal{O}}(C_p)$$

the *canonical isogeny character* at p.

As for the representation T, these facts allow us to ensure that the characteristic polynomial of $T(\sigma) \in \mathrm{Aut}_{\mathbb{F}_p}(A[p])$, for $\sigma \in \mathrm{Gal}\,(\bar{k}/k)$, is given by

$$[(x-\rho_p(\sigma))(x-(\rho_p(\sigma))^p)]^2.$$

3. The Shimura covering attached to a prime factor of disc(B)

The goal of this section is to describe how to attach a cyclic étale covering of X_B to a prime factor p of $D = \mathrm{disc}(B)$, following [**Jor81**, Chapter 5, §1]. Therefore, we may assume as before that $D > 1$, which excludes the classical case $B \simeq \mathrm{M}_2(\mathbb{Q})$. As a consequence, recall that the Shimura curve X_B is already compact. Moreover, in this section the Shimura curve X_B is rather considered as a Riemann surface.

We start by recalling the notion of covering of a connected curve over $\mathbb{C}$, since Riemann surfaces are non-singular complex algebraic curves. Although in many topology texts only étale (unramified) coverings are considered, it will be useful for us to define the notion of covering in a broader sense:

Definition 4.14. *Let X be a connected curve over $\mathbb{C}$. A (branched)* covering *of X is a pair (Y, f) consisting of a curve Y and a surjective morphism $f : Y \to X$. The covering (Y, f) is said to be* finite *if f is finite. A* morphism of coverings $(Y_1, f_1) \to (Y_2, f_2)$ *is a morphism of curves $g : Y_1 \to Y_2$ such that $f_1 = f_2 \circ g$.*

A covering (Y, f) of X is called *étale* (or unramified) if f is étale. When considering a covering $f : Y \to X$ of topological spaces, this amounts to say that every point $x \in X$ has an open neighborhood U such that $f^{-1}(U)$ is a disjoint union of open subsets V_j of Y for which the restrictions $f_{|V_j} : V_j \to U$ are all homeomorphisms; in particular, f is a local homeomorphism. The category of étale coverings of X will be denoted by $\mathbf{\acute{E}tCov}_X$.

Among the étale coverings of a topological space X, there is one of particular interest: the *universal covering*. An étale covering $f : Y \to X$ is said to be the universal covering of X if it satisfies the following universal property: for every covering $g : Z \to X$ with Z connected, and every choice of points $y_0 \in Y, z_0 \in Z$ such that $f(y_0) = g(z_0)$, there exists a unique continuous fibre-preserving mapping $h : Y \to Z$ such that $h(y_0) = z_0$. In other words, the universal covering factors through any other étale covering from a connected topological space. This universal property implies that a connected topological space X has at most one universal covering up to isomorphism. For connected manifolds, the universal covering always exists (see for example [**Mas77**, Theorem 10.2]).

By the definitions, the automorphisms of a covering (Y, f) are exactly the automorphisms of Y which preserve the fibres of f. So the group of automorphisms of (Y, f), denoted by $\mathrm{Aut}(Y/X)$, acts on each fibre of the covering. When this action is transitive, the covering is said to be *regular* or *Galois*. This terminology corresponds to an analogy between the classification of intermediate coverings of the universal covering and Galois theory. The elements of $\mathrm{Aut}(Y/X)$ are also called *covering transformations* or *deck transformations*.

To be more precise, suppose X is a Riemann surface. Then X has a universal (étale) covering $\widetilde{X}$, on which the topological group $\pi_1(X)$ of X acts by path lifting. Then the following result particularizes [**Sza09**, Theorem 2.3.4]:

Theorem 4.15. *Let $\pi_1(X)$ be the topological fundamental group of $X(\mathbb{C})^{an}$. Let $\pi_1(X)$-* **Sets** *be the category of sets equipped with a left action of $\pi_1(X)$. Then, there exists a natural equivalence of categories*

$$\mathbf{\acute{E}tCov}_X \longrightarrow \pi_1(X)\text{-}\mathbf{Sets}.$$

Under this equivalence, connected étale coverings of X correspond to transitive $\pi_1(X)$-sets, i.e., to conjugacy classes of subgroups of $\pi_1(X)$. With such a subgroup H of $\pi_1(X)$, there is associated the algebraization of the covering of Riemann surfaces $\widetilde{X}/H \to X$.

In particular, the universal covering corresponds to the trivial subgroup and the trivial covering $id : X \to X$ corresponds to the whole group $\pi_1(X)$. From these results it follows that the group of covering transformations of the universal covering $\mathrm{Aut}(\widetilde{X}/X)$ is isomorphic to $\pi_1(X)$. As for the Galois coverings intermediate to the universal covering, these correspond to the normal subgroups of $\pi_1(X)$. Given such a covering $Y \to X$, corresponding to a normal subgroup N of $\pi_1(X)$, then $\mathrm{Aut}(\widetilde{X}/Y) = N$ and $\mathrm{Aut}(Y/X) = \pi_1(X)/N$.

Now we sketch how to obtain a cyclic étale covering of a Riemann surface. So let X be a Riemann surface and let $H \subseteq \mathrm{Hom}(\pi_1(X), \mathbb{Q}/\mathbb{Z}) \simeq \mathrm{H}^1(X, \mathbb{Q}/\mathbb{Z})$ (singular cohomology) be a cyclic subgroup of order n. This subgroup H determines a normal subgroup of index n of $\pi_1(X)$, namely

$$\ker(H) := \bigcap_{f\in H} \ker(f : \pi_1(X) \to \mathbb{Q}/\mathbb{Z}) \subseteq \pi_1(X),$$

which therefore defines a cyclic étale covering Y_H of the universal covering $\widetilde{X}/X$ of X, with $\mathrm{Aut}(\widetilde{X}/Y_H) \simeq \ker(H) \subseteq \pi_1(X) \simeq \mathrm{Aut}(\widetilde{X}/X)$.

Conversely, given a cyclic étale covering Y/X of degree n, we can define a cyclic subgroup $S(Y/X)$ of $\mathrm{H}^1(X, \mathbb{Q}/\mathbb{Z})$ of order n by means of the exact sequence

$$0 \longrightarrow S(Y/X) \longrightarrow \mathrm{H}^1(X, \mathbb{Q}/\mathbb{Z}) \longrightarrow \mathrm{H}^1(Y, \mathbb{Q}/\mathbb{Z}).$$

That is, $S(Y/X)$ is the kernel of the morphism $\mathrm{H}^1(X, \mathbb{Q}/\mathbb{Z}) \to \mathrm{H}^1(Y, \mathbb{Q}/\mathbb{Z})$ in cohomology induced by the covering map $Y \to X$. These two associations are inverse one to each other, so that cyclic subgroups of $\mathrm{H}^1(X, \mathbb{Q}/\mathbb{Z})$ of order n bijectively correspond to cyclic étale covers of X of order n.

This process applies to the case of Shimura curves, and allows us to attach a cyclic étale covering to every prime divisor p of the discriminant of the rational quaternion algebra defining X_B. Recall that we have fixed the datum $(B, \mathcal{O}, \varrho)$ at the outset. Let p be a prime divisor of D, L_p the unique quadratic unramified extension of $\mathbb{Q}_p$ and denote by σ the nontrivial element in $\mathrm{Gal}\,(L_p/\mathbb{Q}_p)$. Then fix an isomorphism

$$\psi : \mathcal{O} \otimes \mathbb{Z}_p \xrightarrow{\simeq} \left\{ \begin{pmatrix} x & y \\ p\,{}^{\sigma}y & {}^{\sigma}x \end{pmatrix} : x, y \in R_{L_p} \right\} \subseteq \mathrm{M}_2(R_{L_p}),$$

where R_{L_p} is the ring of integers of L_p, and set $\mathrm{P}\mathcal{O}^1 = \mathcal{O}^1/\{\pm 1\}$.

Definition 4.16. *The* Nebentypus character of $\mathcal{O}$ at p *is the character*

$$\varepsilon'_p : \mathcal{O} \otimes \mathbb{Z}_p \longrightarrow \mathbb{F}_{p^2}$$

defined using the above isomorphism by the condition

$$\varepsilon'_p(\gamma) = x \mod p \in \mathbb{F}_{p^2} \quad \textit{if} \quad \psi(\gamma) = \begin{pmatrix} x & y \\ p\,{}^{\sigma}y & {}^{\sigma}x \end{pmatrix} \quad \textit{with } x, y \in R_{L_p}.$$

The Nebentypus character of $\mathrm{P}\mathcal{O}^1$ at p *is then the character*

$$\varepsilon_p : (\mathcal{O} \otimes \mathbb{Z}_p)^\times/\{\pm 1\} \longrightarrow \mathbb{F}_{p^2}^\times/\{\pm 1\}$$

induced by ε'_p.

Remark 4.17. Note that while the Nebentypus character ε'_p of $\mathcal{O}$ at p depends on the chosen isomorphism ψ, the pair $\{\varepsilon_p, \varepsilon_p^p\}$ does not.

Now let $\mathcal{E} \subseteq \mathrm{P}\mathcal{O}^1$ be the subgroup generated by the elliptic elements, and denote by $\pi_p : \mathbb{F}_{p^2}^\times \to \mathbb{F}_{p^2}^\times/\{\pm 1\}$ the natural projection. Since every subgroup of the multiplicative group $\mathbb{F}_{p^2}^\times \simeq \mathbb{Z}/(p^2-1)\mathbb{Z}$ is cyclic, $\pi_p^{-1}(\varepsilon_p(\mathcal{E})) \subseteq \mathbb{F}_{p^2}^\times$ must be cyclic. The next result shows that its order depends only on the arithmetic of B. More precisely, it depends on whether the imaginary quadratic fields $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$ split B or not.

Proposition 4.18. *With the above notations,*

$$\pi_p^{-1}(\varepsilon_p(\mathcal{E})) = \begin{cases} \mu_{12} & \textit{if both } \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3}) \textit{ split } B, \\ \mu_6 & \textit{if } \mathbb{Q}(\sqrt{-3}) \textit{ splits } B \textit{ and } \mathbb{Q}(\sqrt{-1}) \textit{ does not,} \\ \mu_4 & \textit{if } \mathbb{Q}(\sqrt{-1}) \textit{ splits } B \textit{ and } \mathbb{Q}(\sqrt{-3}) \textit{ does not,} \\ \mu_2 & \textit{if neither } \mathbb{Q}(\sqrt{-1}) \textit{ nor } \mathbb{Q}(\sqrt{-3}) \textit{ split } B, \end{cases}$$

where here $\mu_k = \mu_k(\mathbb{F}_{p^2}^\times) = \{\zeta \in \mathbb{F}_{p^2}^\times : \zeta^k = 1\}$.

Proof. The statement follows from observing that the reduced trace of an elliptic element has to be -1, 0 or 1, according to the standard characterization of elliptic elements of $\mathrm{PSL}_2(\mathbb{R})$ (see [**Jor81**, Proposition 5.1.3]). □

If for a quadratic field K we set

$$\left(\frac{B}{K}\right) = \begin{cases} 1 & \text{if } K \text{ splits } B, \\ 0 & \text{if } K \text{ does not split } B, \end{cases}$$

then the order $e(p,B) = |\pi_p^{-1}(\varepsilon_p(\mathcal{E}))|$ of $\pi_p^{-1}(\varepsilon_p(\mathcal{E}))$ is given by the following expression:

$$e(p,B) = \begin{cases} 2\left(1 + 2\left(\frac{B}{\mathbb{Q}(\sqrt{-3})}\right)\right)\left(1 + \left(\frac{B}{\mathbb{Q}(\sqrt{-1})}\right)\right) & \text{if } p > 3, \\ 2\left(1 + \left(\frac{B}{\mathbb{Q}(\sqrt{-1})}\right)\right) & \text{if } p = 3, \\ 1 + 2\left(\frac{B}{\mathbb{Q}(\sqrt{-3})}\right) & \text{if } p = 2. \end{cases}$$

The four cases from the proposition can be reduced to only two in the cases $p = 2, 3$, just by excluding the non-possible orders, and this leads to the simplified expressions for these particular instances.

Note that for $p \neq 2$ the integer $e(p,B)$ is always even. And since for the case $p = 2$ the subgroup $\{\pm 1\} \subseteq \mathbb{F}_{p^2}^\times$ might be understood just as the trivial subgroup $\{1\}$, we can consider the natural projection $\mathbb{F}_{p^2}^\times/\{\pm 1\} \to \mathbb{F}_{p^2}^\times/\mu_{e(p,B)}$. Set $n(p,B) = (p^2-1)/e(p,B)$, which is the order of the cyclic group $\mathbb{F}_{p^2}^\times/\mu_{e(p,B)}$. Then the composition of the Nebentypus character of $\mathrm{P}\mathcal{O}^1$ at p with this projection leads to the following definition:

Definition 4.19. *The* reduced Nebentypus character *of* $\mathrm{P}\mathcal{O}^1$ *at* p*, which we denote by* $\widetilde{\varepsilon}_p$*, is defined as the character making commutative the following diagram:*

$$\begin{tikzcd} \mathrm{P}\mathcal{O}^1 \arrow[r, "\varepsilon_p"] \arrow[dr, "\widetilde{\varepsilon}_p"'] & \mathbb{F}_{p^2}^\times/\{\pm 1\} \arrow[d] \\ & \mathbb{F}_{p^2}^\times/\mu_{e(p,B)} \simeq \mathbb{Z}/n(p,B)\mathbb{Z} \end{tikzcd}$$

Now observe that by Proposition 4.18, the elements in $\varepsilon_p(\mathcal{E}) \subseteq \mathbb{F}_{p^2}^\times/\{\pm 1\}$ all come from $\mu_{e(p,B)} \subseteq \mathbb{F}_{p^2}^\times$, hence the reduced Nebentypus character $\widetilde{\varepsilon}_p$ of $\mathrm{P}\mathcal{O}^1$ at p factors through the subgroup $\mathcal{E}$ and we can regard it as having source in $\mathrm{P}\mathcal{O}^1/\mathcal{E}$.

Finally we need a somehow technical lemma in order to obtain our covering:

Lemma 4.20. $\mathrm{P}\mathcal{O}^1/\mathcal{E}$ *is a quotient of* $\pi_1(X_B)$.

Proof. Consider first the natural projection $f : \mathfrak{H} \to X_B = \mathrm{P}\mathcal{O}^1\backslash\mathfrak{H}$, and define $S \subset \mathfrak{H}$ to be the (discrete) set of elliptic points with respect to $\mathrm{P}\mathcal{O}^1$. Denote by S' the image of S by f, which is by definition the set of elliptic points of X_B. Note that S' is a finite set of points because X_B is compact. Since the branch locus of f consists precisely of the elliptic points of X_B, it is readily seen that the restriction of f to $\mathfrak{H} - S$ induces an étale covering, which we still denote by f,

$$f : \mathfrak{H} - S \longrightarrow X_B - S'.$$

Moreover, it is also clear that $\mathrm{P}\mathcal{O}^1$ is the group of automorphisms of this covering (by continuity, every automorphism of this covering extends uniquely to an automorphism of the (branched) covering $\mathfrak{H} \to X_B$, which has $\mathrm{P}\mathcal{O}^1$ as a group of covering transformations, and conversely every automorphism of the latter covering restricts to an automorphism of the former one). Now, if we denote by $\widetilde{X_B - S'}$ the universal étale covering of $X_B - S'$, since $\mathfrak{H} - S$ is connected we have a chain of étale coverings

$$\widetilde{X_B - S'} \longrightarrow \mathfrak{H} - S \longrightarrow X_B - S'.$$

In particular, $\widetilde{X_B - S'}$ is also the universal covering of $\mathfrak{H} - S$ and

$$\mathrm{Aut}(\widetilde{X_B - S'}/\mathfrak{H} - S) = \pi_1(\mathfrak{H} - S)$$

is a normal subgroup of $\pi_1(X_B - S')$, because the action of $\mathrm{P}\mathcal{O}^1$ on the fibres of $\mathfrak{H} - S \longrightarrow X_B - S'$ is transitive. Therefore we have

$$\mathrm{Aut}(\mathfrak{H} - S/X_B - S') = \pi_1(X_B - S')/\pi_1(\mathfrak{H} - S). \tag{10}$$

Observe that here $\pi_1(\mathfrak{H} - S)$ has to be regarded as a subgroup of $\pi_1(X_B - S')$ via the monomorphism $f_* : \pi_1(\mathfrak{H} - S) \to \pi_1(X_B - S')$ induced by f. If for each $\tau \in S$ we denote by δ_τ a sufficiently small counterclockwise loop in $\mathfrak{H}$ around τ, so that its complement in $\mathfrak{H}$ consists of two connected components, one of them containing τ and the other one containing $S - \tau$, then by the Seifert-van Kampen Theorem the fundamental group $\pi_1(\mathfrak{H} - S)$ is the free group generated by these elements δ_τ with $\tau \in S$. But now, since locally around each elliptic point $\tau \in S$ the covering map f is like $z \mapsto z^{e_Q}$, where e_Q is the ramification index of $Q = f(\tau)$ and z is a local coordinate, we see that

$$N := f_* \pi_1(\mathfrak{H} - S) = \langle \gamma_Q^{e_Q} : Q \in S' \rangle,$$

where γ_Q is a sufficiently small counterclockwise loop in X_B around Q. Then (10) can be written more precisely as

$$\mathrm{P}\mathcal{O}^1 = \mathrm{Aut}(\mathfrak{H} - S/X_B - S') = \pi_1(X_B - S')/N.$$

Finally, since S' is a finite set of points in X_B it is clear that every loop γ in X_B can be modified homotopically to a loop not passing by any point in S'. In this way we get a natural morphism $\pi_1(X_B) \to \pi_1(X_B - S')$, and using the above relation it can be shown that this map defines a surjection from $\pi_1(X_B)$ to $\mathrm{P}\mathcal{O}^1/\mathcal{E}$. □

So, in view of this lemma we can even regard the reduced Nebentypus character as

$$\widetilde{\varepsilon}_p : \pi_1(X) \longrightarrow \mathbb{Z}/n(p, B)\mathbb{Z},$$

that is, as an element of $\mathrm{H}^1(\pi_1(X_B), \mathbb{Z}/n(p, B)\mathbb{Z})$ of order $n(p, B)$. Then, by the procedure explained above, $\widetilde{\varepsilon}_p$ gives rise to a cyclic étale covering

$$Z_{B,p} \longrightarrow X_B$$

of degree $n(p, B)$ of the curve X_B.

Definition 4.21. *The cyclic étale covering $Z_{B,p} \longrightarrow X_B$ of degree $n(p, B)$ is* the Shimura covering *at p of the Shimura curve X_B.*

It is worthwhile relating this Shimura covering $Z_{B,p}$ with the canonical torsion subgroup C_p we have introduced before, as is done in [**Jor81**]. First consider the Nebentypus character $\varepsilon_p : \mathrm{P}\mathcal{O}^1 \to \mathbb{F}_{p^2}^\times$, and define $\Gamma(p) \subseteq \mathrm{P}\mathcal{O}^1$ to be its kernel. Then $X_{B,p} := \Gamma(p) \setminus \mathfrak{H}$ is a cyclic Galois covering of X_B (cf. [**Sij10**, p. 91]) with $\mathrm{Aut}(X_{B,p}/X_B) \simeq \mathbb{F}_{p^2}^\times/\{\pm 1\} \simeq \mathbb{Z}/\frac{p^2-1}{2}\mathbb{Z}$.

This subgroup $\Gamma(p)$ is closely related with the two-sided ideal $I(p)$. Indeed, using the definition of the Nebentypus character ε_p it follows that regarding $\Gamma(p)$ as a subgroup of $\mathcal{O}^1$ it consists of the elements in $\mathcal{O}^1$ which are congruent to 1 modulo $I(p)$. That is, $\Gamma(p) = (1 + I(p))/\{\pm 1\}$ (note that this is really a multiplicative group).

In terms of moduli for QM-abelian surfaces, recall that X_B parametrizes QM-abelian surfaces $(A, \iota : \mathcal{O} \hookrightarrow \mathrm{End}(A))$, and any of these abelian surfaces has a canonical torsion subgroup C_p attached to each prime divisor p of D. Then, the Galois covering $X_{B,p}$ parametrizes isomorphism classes of triplets (A, ι, x_p), where $x_p \in C_p$ is a generator of the canonical subgroup C_p of (A, ι) as an $\mathcal{O}$-module. In this situation, the Shimura covering $Z_{B,p}/X_B$ at p is the maximal étale covering of X_B intermediate to the covering $X_{B,p}/X_B$ (see [**Jor81**, p. 110]).

Example 4.22. Let B be the rational quaternion algebra of discriminant $11 \cdot 17$. Let $Z_{B,11}$ and $Z_{B,17}$ be the Shimura coverings of X_B at the primes 11 and 17 respectively. For computing the degree of these coverings it suffices to know whether the quadratic fields $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-3})$ do split B or not.

In general, by the criterion of Hasse, we know that a quadratic field K splits a rational quaternion algebra B if and only if every prime which ramifies in B fails to split in K (see Theorem 1.26). And on the other hand, if d_K denotes the discriminant of K and p is an odd prime not dividing d_K, then p fails to split in K if and only if d_K is not congruent to a square modulo p. Therefore, since $d_{\mathbb{Q}(\sqrt{-1})} = -4$ and $d_{\mathbb{Q}(\sqrt{-3})} = -3$, it is enough to know whether -4 and -3 are squares modulo 11 and 17 or not. For the case of $-4 = d_{\mathbb{Q}(\sqrt{-1})}$ we have that

$$\left(\frac{-4}{17}\right) = \left(\frac{-1}{17}\right) = 1$$

because $17 \equiv 1 \pmod 4$. This means that 17 splits in $\mathbb{Q}(\sqrt{-1})$, hence $\mathbb{Q}(\sqrt{-1})$ does not split B. As for the case $-3 = d_{\mathbb{Q}(\sqrt{-3})}$, it is not a square neither modulo 11 nor 17, so that both 11 and 17 fail to split in $\mathbb{Q}(\sqrt{-3})$, which then splits B.

Then, with the same notations as before, we have $e(11, B) = e(17, B) = 6$, which means that the degrees of the Shimura coverings at the primes 11 and 17 are $n(11, B) = 20$ and $n(17, B) = 48$, respectively.

Chapter 5
Following A. N. Skorobogatov

This chapter begins with a brief exposition of the interpretation of Jordan's results worked out by Skorobogatov [**Sko05**] in terms of descent. The consequence of this interpretation is that the counterexamples to the Hasse principle arising from Jordan's results [**Jor86**] can be accounted for by the Brauer-Manin obstruction.

As in the previous chapter, let B be an indefinite rational quaternion division algebra, and consider the Shimura curve X_B defined by a fixed datum $(B, \mathcal{O}, \varrho)$.

One of the main ingredients in Skorobogatov's work is an étale subcovering of the Shimura covering $X_{B,p} \to X_B$ attached to a prime factor p of the reduced discriminant D of B introduced by Jordan. As we show in the second section, these coverings can be used to obtain coverings of an Atkin-Lehner quotient $X_B^{(m)}$ of X_B in a natural way. This gives us a hope to prove that the Brauer-Manin obstruction explains some counterexamples to the Hasse principle involving Atkin-Lehner quotients of X_B, but now over $\mathbb{Q}$ instead of over an imaginary quadratic field, using the work of V. Rotger [**Rot08**].

In the third section of this chapter we state the main result of this thesis, which will be proved in Theorem 7.31.

1. Interpretation of Jordan's results using descent

As we have explained, Jordan's work on global points on Shimura curves is based on the modular interpretation and exploits the properties of the canonical torsion subgroups of QM-abelian surfaces and their isogeny characters.

More recently, Skorobogatov [**Sko05**] has interpreted Jordan's approach in terms of descent. This interpretation leads him to explain several counterexamples to the Hasse principle for which there was no explanation before. He finds that they are accounted for by the Brauer-Manin obstruction.

The main idea is to consider the Shimura covering $X_{B,p}$ of X_B attached to a prime factor p of $D = \mathrm{disc}(B)$, which has been introduced in the last chapter. This Galois covering parametrizes triplets (A, ι, x_p), where (A, ι) is a QM-abelian surface and x_p is a generator of the canonical torsion subgroup C_p of A at p, considered as an $\mathcal{O}$-module. The Galois group of this covering is isomorphic to the cyclic group $\mathbb{F}_{p^2}^{\times 2} \simeq \mathbb{F}_{p^2}^{\times}/\{\pm 1\}$ of order $\frac{p^2-1}{2}$. Assuming $p \geq 5$, since 6 divides $\frac{p^2-1}{2}$ we have that $\mathbb{Z}/6\mathbb{Z}$ is a subgroup of $\mathbb{Z}/\frac{p^2-1}{2}\mathbb{Z}$, and Skorobogatov defines Y as the quotient of $X_{B,p}$ by $\mathbb{Z}/6\mathbb{Z}$. This is a cyclic étale subcovering of the maximal étale subcovering $Z_{B,p}$ of $X_{B,p}$ defined in the previous chapter, and in particular it is an X_B-torsor under the constant group scheme $\mathbb{F}_{p^2}^{\times 12} \simeq \mathbb{Z}/\frac{p^2-1}{12}\mathbb{Z}$.

This translation allows Skorobogatov to use the language of torsors and descent from Chapter 3 and to strengthen Jordan's results, in the sense that instead of finding sufficient conditions for the emptiness of $X_B(K)$ for certain quadratic fields K, he can conclude that

$X_B(\mathbb{A}_K)^{\mathrm{Br}} = \emptyset$. This difference implies that the counterexamples to the Hasse principle found by Jordan are accounted for by the Brauer-Manin obstruction.

For example, by adapting Theorem 6.1 in [**Jor86**] Skorobogatov proves the following:

Theorem 5.1 (Skorobogatov)**.** *Let B be an indefinite rational quaternion algebra ramified at a prime $p \geq 11$, $p \equiv 3 \mod 4$, and X_B be the Shimura curve defined by B. Assume that B is split by an imaginary quadratic field K in which p is inert, and denote by $\mathfrak{p}$ the unique prime of K over p. Assume also that there is no surjective homomorphism from the ray class group of K of conductor $\mathfrak{p}$ to the product of the class group Cl_K and $\mathbb{Z}/\frac{p^2-1}{12}\mathbb{Z}$. Then $X_B(\mathbb{A}_K)^{\mathrm{Br}} = \emptyset$.*

The basic idea behind the proofs in [**Sko05**] which is added to Jordan's arguments can be described as follows. Suppose that K is a number field and that $Q \in X_B(K)$ is a K-rational point on the Shimura curve X_B. The torsor $f : Y \to X_B$ under the constant group scheme $G = \mathbb{F}_{p^2}^{\times 12}$ is a torsor under a group of multiplicative type, since $\overline{G}$ can be regarded as the subgroup of roots of the unity of order $\frac{p^2-1}{12}$ in $\mathbb{G}_m$. The evaluation map induced by this torsor associates to Q the class $\phi_Q \in \mathrm{H}^1(K, G)$ of the K-torsor under G corresponding to its fibre. Analogously, if we are given instead of Q a family $\{Q_v\}_v$ of K_v-rational points on X_B (where v runs over the places of K), we get in the same way elements $\phi_{Q_v} \in \mathrm{H}^1(K_v, G)$. The ϕ_{Q_v} are indeed characters from $\mathrm{Gal}\,(\bar{K}_v/K_v)$ to G. Now recall from the last chapter the definition of the descent obstruction related to the torsor f by means of the commutative diagram

$$\begin{tikzcd}
X_B(K) \arrow[r, hook] \arrow[d] & X_B(\mathbb{A}_K) \arrow[d] \\
\mathrm{H}^1(K, G) \arrow[r] & \prod_v \mathrm{H}^1(K_v, G).
\end{tikzcd}$$

In words, if a rational point $Q \in X_B(K)$ does exist, then it has to be mapped to a family of local characters $\{\phi_{Q_v}\}_v \in \prod_v \mathrm{H}^1(K_v, G)$ coming from a global character in $\mathrm{H}^1(K, G)$.

So, in order to prove that there is a Brauer-Manin obstruction to the existence of rational points on X_B, the key argument of Skorobogatov reduces to the following: one may prove that no family of local characters $\{\phi_{Q_v}\}_v$ with[1] $Q_v \in X_B(K_v)$ comes from a global character of $\mathrm{Gal}\,(\bar{K}/K)$. If one succeeds, it follows that the descent subset $X_B(\mathbb{A}_K)^f \subseteq X_B(\mathbb{A}_K)$ associated to the torsor f is empty, and therefore no twist of the torsor f has points everywhere locally, by (8). At this point, one could conclude by saying that there is a descent obstruction to the existence of rational points on X_B, since $X_B(\mathbb{A}_K)^{\mathrm{descent}} \subseteq X_B(\mathbb{A}_K)^f = \emptyset$. However, by applying Theorem 3.32 (see the comments after its statement) one deduces actually that $X_B(\mathbb{A}_K)^{\mathrm{Br}}$ is empty, as desired. By the way, note that this is a stronger condition than the vanishing of the descent set $X_B(\mathbb{A}_K)^{\mathrm{descent}}$, by Proposition 3.27.

Moreover, the translation of the modular approach of Jordan's work to the language of torsors is also read in these local characters. If (A, ι) is a QM-abelian surface defined over K, the choice of a field isomorphism of $C_p = \mathcal{O}/I_p$ with $\mathbb{F}_{p^2}$ defines a character $\rho_{A,p} : \mathrm{Gal}\,(\bar{K}/K) \to \mathbb{F}_{p^2}^{\times}$ coming from the Galois action on C_p, namely the canonical isogeny character. Then, assuming that K splits B, if (A, ι) represents a K-rational point $Q \in X_B(K)$, then $\rho_{A,p}^{12} = \phi_Q$ ([**Sko05**, Lemma 2.1]).

Example 5.2. One of the examples discussed by Skorobogatov in [**Sko05**] refers to the Shimura curve X_B defined by the quaternion algebra B of discriminant $23 \cdot 107$, which is also considered in [**RSY05**]. The curve X_B has genus 193, and computations based on results from [**JL85**] show that X_B has points in all completions of $\mathbb{Q}(\sqrt{-23})$, but it turns out that $X_B(\mathbb{Q}(\sqrt{-23})) = \emptyset$, so that X_B is a counterexample to the Hasse principle over $\mathbb{Q}(\sqrt{-23})$.

[1] Here we assume that $X_B(\mathbb{A}_K) \neq \emptyset$, since otherwise there is nothing to prove.

In order to apply the above theorem for $p = 107$, one has that

$$\mathrm{Cl}^{(107)}_{\mathbb{Q}(\sqrt{-23})} \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/81\mathbb{Z} \times \mathbb{Z}/53\mathbb{Z}$$

and $\mathrm{Cl}_{\mathbb{Q}(\sqrt{-23})} \simeq \mathbb{Z}/3\mathbb{Z}$, so that

$$\mathbb{Z}/\frac{107^2-1}{12}\mathbb{Z} \times \mathrm{Cl}_{\mathbb{Q}(\sqrt{-23})} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/53\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

Then the hypothesis of the theorem are easily seen to hold, hence $X_B(\mathbb{A}_{\mathbb{Q}(\sqrt{-23})})^{\mathrm{Br}} = \emptyset$, and this counterexample to the Hasse principle is accounted for by the Brauer-Manin obstruction.

The other main result in [**Sko05**] takes Theorem 4.5 a step further. With the notations as in the previous chapter:

Theorem 5.3 (Skorobogatov)**.** *Let K be an imaginary quadratic field in which q is ramified, B a quaternion algebra in $\mathcal{C}(q)$ which is split by K, and X_B the Shimura curve defined by B. Then $X_B(\mathbb{A}_K)^{\mathrm{Br}} = \emptyset$.*

Example 5.4. As an application of this theorem, Skorobogatov recovers the example given by B_{39} and $\mathbb{Q}(\sqrt{-13})$ from the previous section. The corresponding Shimura curve $X_{B_{39}}$ has points everywhere locally over $\mathbb{Q}(\sqrt{-13})$, and for this particular case the property $X_{B_{39}}(\mathbb{A}_{\mathbb{Q}(\sqrt{-13})})^{\mathrm{Br}} = \emptyset$ was checked in [**SS03**], but using a conjectural equation for $X_{B_{39}}$ due to Kurihara. Applying the above theorem with $q = 2$ gives this result unconditionally. However, it is worthwhile mentioning here that the curve defined by the equation conjectured by Kurihara for $X_{B_{39}}$ is now known to be really isomorphic to the Shimura curve $X_{B_{39}}$, after the work of S. Molina in [**Mol10**].

2. Cyclic étale coverings of Atkin-Lehner quotients of X_B

Let m be a positive nontrivial divisor of $D = \mathrm{disc}(B)$, and consider the Atkin-Lehner involution ω_m. In order to apply the techniques of Skorobogatov [**Sko05**], but now to the Atkin-Lehner quotient $X_B^{(m)} = X_B/\langle\omega_m\rangle$ of the Shimura curve X_B by ω_m, we need to construct first a suitable étale covering.

A first approach would consist on looking to the natural quotient map $X_B \to X_B^{(m)}$. Composing it with the étale coverings $Z_{B,p} \to X_B$ constructed in the previous chapter, we get coverings $Z_{B,p} \to X_B^{(m)}$, but these ones are étale if and only if the Atkin-Lehner involution ω_m is unramified. By the formula for the number of fixed points of an Atkin-Lehner involution on X_B ([**Ogg83**]), we know that ω_m has no fixed points if and only if $(\frac{-m}{q}) = 1$ for some prime divisor q of $\mathrm{disc}(B)$. Then:

Proposition 5.5. *Assume $m|D$ is such that $(\frac{-m}{q}) = 1$ for some prime divisor q of D. Then the natural projection $X_B \to X_B^{(m)}$ is a double étale covering of $X_B^{(m)}$.*

This approach was used in [**RSY05**] (see for example Proposition 3.5), and we refer the reader there for the results obtained in this direction. It is important to note here that, by the criterion of Ogg mentioned above, the full Atkin-Lehner involution ω_D has always fixed points. Hence, the covering $X_B \to X_B^{(D)}$ is always ramified and the approach of [**RSY05**] cannot be used to study rational points on $X_B^{(D)}$. This is one of the reasons for trying to construct another covering of the Atkin-Lehner quotient $X_B^{(m)}$, which we want to be étale independently on the divisor m of D.

So the goal is to construct étale coverings $Z_{B,p}^{(m)} \to X_B^{(m)}$ from the already known ones $Z_{B,p} \to X_B$ in some way that does not depend on the nature of the involution ω_m. The basic idea behind our construction is that ω_m can be lifted to an involution $\hat{\omega}_m$ on the Galois covering $X_{B,p}$, which preserves the intermediate coverings of $X_{B,p} \to X_B$ arising as quotients of $X_{B,p}$ by subgroups of $\mathrm{Aut}(X_{B,p}/X_B) \simeq \mathbb{F}_{p^2}^\times/\{\pm 1\} \simeq \mathbb{Z}/\frac{p^2-1}{2}\mathbb{Z}$.

2.1. Lifting an Atkin-Lehner involution to $X_{B,p}$. The first step to achieve our goal, as we have said, is to lift the involution ω_m on X_B to an involution $\hat{\omega}_m$ on the covering $X_{B,p}$. By this we mean an involution $\hat{\omega}_m : X_{B,p} \to X_{B,p}$ making commutative the diagram

$$(11)\qquad \begin{tikzcd} X_{B,p} \arrow[r, "\hat{\omega}_m"] \arrow[d] & X_{B,p} \arrow[d] \\ X_B \arrow[r, "\omega_m"] & X_B \end{tikzcd}$$

where the vertical arrows are the covering map. Such a lift is constructed using the moduli interpretation of X_B and the explicit description of the action of the Atkin-Lehner involution ω_m on X_B by means of the Shimura correspondence explained in Example 2.14.

Recall from Chapter 2 that we have a uniformization map $\mathfrak{H} \to X_B(\mathbb{C})$ sending a point $\tau \in \mathfrak{H}$ to the isomorphism class of the QM-abelian surface $(A_\tau, \iota_\tau, [\mathcal{L}_\tau])$ where

- $A_\tau = \mathbb{C}^2/\mathcal{O} \cdot v_\tau$, with $v_\tau = (\tau, 1)^t$,
- $\iota_\tau : \mathcal{O} \hookrightarrow \mathrm{End}(A)$ is the natural map,
- $\mathcal{L}_\tau$ is the polarization induced by an explicit Riemann form E_τ.

With respect to this uniformization map, the action of ω_m is described by

$$\omega_m([(A, \iota, [\mathcal{L}])]) = [(A, \iota_{\alpha_m}, [\alpha_m^* \mathcal{L}])],$$

for any representative $\alpha_m \in \mathrm{Norm}_{B^\times}(\mathcal{O}) \cap \mathcal{O}$ of reduced norm m of ω_m, where the notations are as in Example 2.14.

Now we look to $X_{B,p} = \Gamma(p) \backslash \mathfrak{H}$. As we have already quoted, $X_{B,p}$ parametrizes isomorphism classes of quadruplets $(A, \iota, [\mathcal{L}], x_p)$ with $(A, \iota, [\mathcal{L}])$ as above and with x_p a generator of the canonical torsion subgroup $C_p \subseteq A[p]$ of A attached to p as an $\mathcal{O}$-module. Note that an isomorphism between two of these quadruplets $(A, \iota, [\mathcal{L}], x_p)$ and $(A', \iota', [\mathcal{L}'], x'_p)$ is just an isomorphism of QM-abelian surfaces $(A, \iota, [\mathcal{L}]) \simeq (A', \iota', [\mathcal{L}'])$ sending x_p to x'_p.

In order to generalize the above Shimura's description to obtain a uniformization map for the covering $X_{B,p}$, it suffices to choose a generator $x_{p,\tau}$ of the canonical subgroup C_p of A_τ at p, as an $\mathcal{O}$-module via the action defined by ι_τ. Being B a rational quaternion algebra, the two-sided $\mathcal{O}$-ideal $I(p)$ is principal, so let $\beta \in \mathcal{O}$ be a generator for $I(p)$: that is, $\beta \cdot \mathcal{O} = \mathcal{O} \cdot \beta = I(p)$. Then, define $x_{p,\tau}$ to be $\beta^{-1} \cdot (\tau, 1)^t$. Since B is division, this product makes sense when regarding β in $\mathrm{GL}_2(\mathbb{R})$. First of all, $x_{p,\tau}$ belongs to the p-torsion of A. Indeed, since β is a generator for $I(p)$ we can assume it has norm p, and then $\beta^{-1} = \frac{1}{p}\bar{\beta}$. Therefore $p \cdot x_{p,\tau} = \bar{\beta} \cdot (\tau, 1)^t \in \mathcal{O} \cdot (\tau, 1)^t$. And secondly, for checking that $x_{p,\tau}$ really is a generator of C_p, note that for $\gamma \in \mathcal{O}$ the condition $\gamma \cdot x_{p,\tau} \in \mathcal{O} \cdot (\tau, 1)^t$ is equivalent to saying that $\gamma \in \mathcal{O} \cdot \beta = I(p)$, so that $\mathcal{O} \cdot x_{p,\tau}$ is free of rank one over $\mathcal{O}/I(p)$. Hence, by uniqueness it is the canonical subgroup C_p.

In this way we have a uniformization map

$$\begin{array}{ccc} \mathfrak{H} & \longrightarrow & X_{B,p}(\mathbb{C}) \\ \tau & \longmapsto & ((A, \iota, [\mathcal{L}])_\tau, x_{p,\tau}) \end{array}$$

Being $\Gamma(p)$ a subgroup of $\mathrm{P}\mathcal{O}^1$, the $\mathrm{P}\mathcal{O}^1$-orbit of a point $\tau \in \mathfrak{H}$ breaks into (generically) different $\Gamma(p)$-orbits which are in correspondence with the points of $X_{B,p}$ in the fibre of $[(A, \iota, [\mathcal{L}])_\tau] \in X_B$. These points correspond to the non-isomorphic choices of a generator for C_p.

With this description of $X_{B,p}$, the action of α_m on $\mathfrak{H}$ inducing the Atkin-Lehner involution ω_m on X_B induces naturally also an involution on $X_{B,p}$ given by:

$$\begin{array}{rcl} \hat{\omega}_m : X_{B,p} & \longrightarrow & X_{B,p} \\ P = [((A, \iota, [\mathcal{L}])_\tau, x_{p,\tau})] & \longmapsto & \hat{\omega}_m(P) = [(A_{\alpha_m \tau}, \iota_{\alpha_m \tau}, [\alpha_m^* \mathcal{L}], x_{p, \alpha_m \tau})] \end{array}$$

If we want to drop the point τ off from the description, we can use again the isomorphism $g : A_{\alpha_m \tau} \to A_\tau$ induced by α_m^{-1} from Example 2.14. Since g is an isomorphism of

QM-abelian surfaces, it commutes with the QM structure, and then

$$g(x_{p,\alpha_m\tau}) = g(\beta^{-1}\cdot v_{\alpha_m\tau}) = \beta^{-1}\cdot g(v_{\alpha_m\tau}) = \beta^{-1}\cdot v_\tau = x_{p,\tau}.$$

Therefore, $\hat{\omega}_m$ can be described also as follows, without making explicit the point $\tau\in\mathfrak{H}$:

$$P = [(A,\iota,[\mathcal{L}],x_p)] \longmapsto \hat{\omega}_m(P) = [(A,\iota_{\alpha_m},[\alpha_m^*\mathcal{L}],x_p)]. \tag{12}$$

In fact, it seems natural that if we recover the underlying abelian variety the generator may not change. If we adopt (12) as the definition for $\hat{\omega}_m$, one can check easily that x_p still generates the canonical torsion subgroup C_p of the underlying abelian variety of $\hat{\omega}_m(P)$: since $\alpha_m\in\mathrm{Norm}_{B_+^\times}(\mathcal{O})$, one has that

$$\iota_{\alpha_m}(\mathcal{O})(x_p) = \iota(\alpha_m^{-1}\mathcal{O}\alpha_m)(x_p) = \iota(\mathcal{O})(x_p) = C_p,$$

using that x_p is a generator of C_p as an $\mathcal{O}$-module via ι.

Summing up, we have defined an involution $\hat{\omega}_m$ on $X_{B,p}$ lifting our original Atkin-Lehner involution ω_m without any restriction on m, and a commutative diagram like (11) holds.

Remark 5.6. From the description in (12), it is clear that $\hat{\omega}_m$ is an involution on $X_{B,p}$ because ω_m is an involution on X_B. Moreover, both $X_{B,p}$ and $\hat{\omega}_m(X_{B,p})$ are solutions to the same moduli problem and, since a moduli problem has at most one solution up to a unique isomorphism, this observation implies that $\hat{\omega}_m$ is a rational automorphism of $X_{B,p}$ over $\mathbb{Q}$. It was natural to expect this property because the Atkin-Lehner involutions ω_m are also rational.

2.2. A cyclic étale covering of $X_B^{(m)}$. Once we have the lifted Atkin-Lehner involution $\hat{\omega}_m : X_{B,p}\to X_{B,p}$, consider the quotient $X_{B,p}^{(m)} = X_{B,p}/\langle\hat{\omega}_m\rangle$. From the description of $\hat{\omega}_m$ in terms of moduli, it is clear that we have a commutative diagram

$$\begin{tikzcd}
X_{B,p} \arrow[dd] \arrow[dr] & \\
 & X_B \arrow[dd] \\
X_{B,p}^{(m)} \arrow[dr] & \\
 & X_B^{(m)}
\end{tikzcd}$$

where the diagonal arrows are covering maps. In particular, $X_{B,p}^{(m)}\to X_B^{(m)}$ is a covering of the Atkin-Lehner quotient $X_B^{(m)}$ with automorphism group isomorphic to the cyclic group $\mathbb{F}_{p^2}^{\times 2}\simeq\mathbb{F}_{p^2}/\{\pm 1\}$ of order $\frac{p^2-1}{2}$. But this covering is étale if and only if the covering $X_{B,p}\to X_B$ is étale, which is not true in general.

However, it is natural to expect the involution $\hat{\omega}_m$ to descend to $Z_{B,p}$, where $Z_{B,p}$ is the maximal étale subcovering of $X_{B,p}\to X_B$ introduced in Chapter 4. Indeed, the intermediate subcoverings of $X_{B,p}\to X_B$ arise as quotients of $X_{B,p}$ by subgroups of the cyclic group $\mathrm{Aut}(X_{B,p}/X_B)\simeq\mathbb{Z}/\frac{p^2-1}{2}\mathbb{Z}$, and as we show below in more generality, $\hat{\omega}_m$ descends to an involution on any of these coverings:

Proposition 5.7. *With the notations as before, for any subgroup $H\subseteq\mathrm{Aut}(X_{B,p}/X_B)\simeq\mathbb{Z}/\frac{p^2-1}{2}\mathbb{Z}$ the involution $\hat{\omega}_m$ descends to the quotient of $X_{B,p}$ by H.*

Proof. As we have seen above, if P is a closed point in $X_{B,p}$, regarded as a quadruplet $[(A_\tau,\iota_\tau,[\mathcal{L}_\tau],x_{p,\tau})]$ corresponding to a point $\tau\in\mathfrak{H}$, then the action of $\hat{\omega}_m$ can be described by

$$\hat{\omega}_m(P) = [(A_{\alpha_m\tau}, \iota_{\alpha_m\tau}, [\alpha_m^*(\mathcal{L}_\tau)], x_{p,\alpha_m\tau})],$$

for any $\alpha_m \in \mathrm{Norm}_{B_+^\times}(\mathcal{O}) \cap \mathcal{O}$ of reduced norm m. On the other hand, and using also the description of $X_{B,p}$ via the uniformization map, an automorphism $\gamma \in \mathrm{Aut}(X_{B,p}/X_B) = \mathrm{P}\mathcal{O}^1/\Gamma(p)$ acts by

$$\gamma(P) = [(A_{\gamma\tau}, \iota_{\gamma\tau}, [\gamma^*(\mathcal{L}_\tau)], x_{p,\gamma\tau})].$$

Having said this, we next show that for every $\gamma \in H$ there exists some $\gamma' \in H$ such that $\hat{\omega}_m(\gamma(P)) = \gamma'(\hat{\omega}_m(P))$, which proves the statement. Writing down the corresponding expressions, it suffices to show that $\alpha_m\gamma = \gamma'\alpha_m$ for some $\gamma' \in H$ or, equivalently, that $\alpha_m\gamma\alpha_m^{-1} \in H$. First observe that since α_m normalizes $\mathcal{O}^1$, it also normalizes $\mathrm{P}\mathcal{O}^1/\Gamma(p)$, hence asking for this condition makes sense. Secondly, since the order d of $\alpha_m\gamma\alpha_m^{-1}$ is the same as the order of γ and there is only one (cyclic) subgroup of order d of the cyclic group $\mathrm{Aut}(X_{B,p}/X_B)$, we have

$$\langle \alpha_m\gamma\alpha_m^{-1} \rangle = \langle \gamma \rangle \subseteq H,$$

hence $\alpha_m\gamma\alpha'_m \in H$ as we claimed. □

In particular, when $p \neq 2$, recall that the maximal étale subcovering $Z_{B,p} \to X_B$ of $X_{B,p} \to X_B$ can be expressed as the quotient of $X_{B,p}$ by the cyclic subgroup $\mathbb{Z}/\frac{e(p,B)}{2}\mathbb{Z} \subseteq \mathbb{Z}/\frac{p^2-1}{2}\mathbb{Z}$, where $e(p,B)$ is the integer defined in Chapter 4 in terms of the arithmetic of B.

Corollary 5.8. *The Atkin-Lehner involution $\hat{\omega}_m$ descends to the maximal étale subcovering $Z_{B,p} \to X_B$ of $X_{B,p} \to X_B$. Setting $Z_{B,p}^{(m)} := Z_{B,p}/\langle\hat{\omega}_m\rangle$, the cyclic covering $Z_{B,p}^{(m)} \to X_B^{(m)}$ is étale and makes commutative the diagram*

$$\begin{tikzcd}
Z_{B,p} \arrow[dr, "\text{ét}"] \arrow[dd] & \\
& X_B \arrow[dd] \\
Z_{B,p}^{(m)} \arrow[dr, "\text{ét}"] & \\
& X_B^{(m)}
\end{tikzcd}$$

where the vertical arrows are the natural quotient maps.

As a consequence, we have finally obtained a cyclic covering $Z_{B,p}^{(m)} \to X_B^{(m)}$ which is étale *independently* on the divisor m of D.

3. Statement of the main result

Once we have attached an étale covering of an Atkin-Lehner quotient $X_B^{(m)}$ of the Shimura curve X_B to each prime divisor p of $D = \mathrm{disc}(B)$, we can think about using these coverings to explain the non-existence of rational points on $X_B^{(m)}$. Indeed, if we assume that the involution ω_m is twisting, we know from Chapter 2 that the $\mathbb{Q}$-rational points on $X_B^{(m)}$ correspond to isomorphism classes of abelian surfaces with real multiplication by $\mathbb{Q}(\sqrt{m})$ whose field of moduli is $\mathbb{Q}$, and admitting quaternionic multiplication by B over $\bar{\mathbb{Q}}$.

More generally, Rotger considers in [**Rot08**] abelian varieties $A/\mathbb{Q}$ of GL_2-type over $\mathbb{Q}$ of dimension g, by which we mean that the ring $R = \mathrm{End}_{\mathbb{Q}}(A)$ is an order in a number field E of degree $[E : \mathbb{Q}] = g$, and such that $\mathrm{End}_{\bar{\mathbb{Q}}}(A)$ is an order $\mathcal{O}$ in a quaternion algebra over a totally real number field F. Fixed the pair $(\mathcal{O}, R)$, some necessary conditions are given for the existence of such an abelian variety. Therefore, the results in [**Rot08**] are in some sense analogous to the results of Jordan in [**Jor86**] reviewed in Chapter 4. In the particular case of dimension $g = 2$, these results can be read as results about the non-existence of $\mathbb{Q}$-rational points on $X_B^{(m)}$.

With this picture in mind, it is reasonable to think that the ideas used by Skorobogatov in [**Sko05**] to interpret Jordan's results in terms of descent can be applied to interpret Rotger's results in a similar way. Now one should expect the counterexamples to the Hasse principle for Atkin-Lehner quotients over $\mathbb{Q}$ arising from Rotger's work to be accounted for by the Brauer-Manin obstruction.

After explaining the results of Jordan, one of the main difficulties to deal with is clearly the question of when the field of moduli is a field of definition for the abelian surfaces with real multiplication parametrized by $X_B^{(m)}$. In the classical case of abelian surfaces (A, ι) with quaternionic multiplication corresponding to points in $X_B(k)$ for some characteristic zero field k, the condition given in Theorem 4.2 is very nice: it is necessary and sufficient for the abelian surfaces (A, ι) to admit a model rational over k that k splits B. Moreover, if this condition is satisfied then it is also satisfied for all the completions k_v of k. And this is a crucial point in [**Sko05**]. However, finding a similar condition for the abelian surfaces (A, i) parametrized by $X_B^{(m)}$ is, as far as we know, more complicated. So the first task we must face is to study the relation between the field of moduli and the field of definition of these abelian surfaces. This is the goal of the next chapter, and a criterion in the same direction as in the classical case is given in Theorem 6.9. Using a particular instance of this criterion, we will be able to prove a first approach to the main theorem of this thesis in Theorem 7.19.

The proof of Theorem 7.19 uses certain Galois representations attached to abelian surfaces with real multiplication parametrized by $X_B^{(m)}$ and defined over ℓ-adic fields, which were already introduced in [**Rot08**] but in a global context. As we will see in Chapter 7, the key point is that these representations are related to the local characters attached to the corresponding points in $X_B^{(m)}(\mathbb{Q}_\ell)$, by means of a suitable $X_B^{(m)}$-torsor defined from the étale covering $Z_{B,p}^{(m)} \to X_B^{(m)}$.

Then, the idea behind the proof of our main result is that for an abelian surface (A_ℓ, i_ℓ) corresponding to a point $Q_\ell \in X_B^{(m)}(\mathbb{Q}_\ell)$, for some prime ℓ, we are able to extend the above mentioned Galois representations to representations of the absolute Galois group $\mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$, even in the case where (A_ℓ, i_ℓ) does not admit a model rational over $\mathbb{Q}_\ell$. Using these *extended* Galois representations, to be introduced at the end of Chapter 7, we will prove finally our main result in Theorem 7.31.

Nevertheless, we want to state our main result in advance to close this chapter. For doing so, let us make some definitions. Firstly, the congruence conditions appearing in Theorem 4.5 and Theorem 5.3 will be now replaced, as in [**Rot08**], by defining a set of *exceptional primes* with respect to a fixed prime q as follows:

Definition 5.9. *For a rational prime q, let $P(q)$ be the set of prime factors of the non-zero integers in the set $\cup_{s,a}\{q, a^2 - sq, a^4 - 4a^2q + q^2\}$, where the union is over $s = 0, 1, 2, 3, 4$ and the integers a such that $|a| \leq 2\sqrt{q}$.*

And secondly, as in Theorem 5.3, we need to define a family of indefinite rational quaternion algebras. For a prime p and a positive squarefree integer m not divisible by p, let us denote by $\mathcal{Q}(pm)$ the set of indefinite rational quaternion algebras whose reduced discriminant is divisible by pm. Then, for a prime q define the following subfamily of $\mathcal{Q}(pm)$:

$$\mathcal{B}_{p,m}(q) = \left\{ B \in \mathcal{Q}(pm) \;\middle|\; \begin{array}{l} \mathbb{Q}(\sqrt{-q}) \text{ does not split } B \text{ and } q \text{ is not inert in any} \\ \text{imaginary quadratic field } K \text{ such that } K \text{ is} \\ \text{unramified away from } \operatorname{disc}(B) \end{array} \right\},$$

We should also define a subfamily $\mathcal{B}_{p,m}^{\mathrm{Br}}(q) \subseteq \mathcal{Q}(pm)$ by imposing a technical condition on the descent subset $X_B^{(m)}(\mathbb{A}_\mathbb{Q})^{f_p}$ relative to a suitable $X_B^{(m)}$-torsor to be constructed in the next chapter. A more precise definition of the families $\mathcal{B}_{p,m}(q)$ and $\mathcal{B}_{p,m}^{\mathrm{Br}}(q)$ is given in Definition 7.17, and some remarks are given about them.

Finally, the main result of this thesis, to be proved in Theorem 7.31, looks like follows:

Theorem 5.10. *Let B be an indefinite rational quaternion algebra of discriminant D, with $2 \nmid D$. Let ω_m be a twisting Atkin-Lehner involution on X_B, with $m \neq D$. Let $p \geq 5$ be a prime factor of D, $p \equiv 3 \mod 4$, such that $p \nmid m$. Let also q be a prime. Then,*

(1) *If $B \in \mathcal{B}_{p,m}(q)$ and $p \notin P(q)$, then $X_B^{(m)}(\mathbb{Q}) = \emptyset$.*
(2) *If $B \in \mathcal{B}^{\mathrm{Br}}_{p,m}(q)$ and $p \notin P(q)$, then $X_B^{(m)}(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} = \emptyset$.*

Let us mention that the most interesting case for applying Theorem 5.10 is when $X_B^{(m)}(\mathbb{A}_{\mathbb{Q}}) \neq \emptyset$. There is an explicit criterion in [**RSY05**, Theorem 3.1] for deciding whether this holds or not.

As we have explained above, the rest of this work is devoted to prove this result.

Chapter 6
Field of moduli and field of definition

As we have seen, the condition for an abelian surface with quaternionic multiplication by a quaternion algebra B to admit a model rational over a field k containing its field of moduli is very neat: it is necessary and sufficient that the field k splits B (see Theorem 4.2). However, for the case of abelian surfaces with real multiplication parametrized by the Atkin-Lehner quotient $X_B^{(m)}$ of X_B by a twisting involution a condition in the same direction becomes more complicated.

In this chapter we explore when an abelian surface parametrized by $X_B^{(m)}$ admits a model rational over its field of moduli, and we deal with two cases. First, we recover a result proved in [**BFGR06**] which gives us an answer when the abelian surface that we consider corresponds to a point $Q \in X_B^{(m)}(\mathbb{Q})$. And then, in the second section we should give a generalization of this result which is also valid when the field $\mathbb{Q}$ of rational numbers is replaced by either a number field or a finite extension of $\mathbb{Q}_\ell$ for some prime ℓ. However, we will be interested mainly in the case of the fields $\mathbb{Q}_\ell$.

It is well-known that abelian surfaces corresponding to Heegner points of $X_B^{(m)}$ always admit a model rational over its field of moduli. Therefore, in both sections of this chapter we should restrict to abelian surfaces parametrized by the non-Heegner locus of $X_B^{(m)}$.

1. Abelian surfaces parametrized by $X_B^{(m)}(\mathbb{Q})$

Dealing with the non-Heegner case, let us recover the higher-dimensional case for a while, in order to state a theorem due to W. Chi of important relevance. So let B be a totally indefinite quaternion division algebra over a totally real field F of degree $n = [F : \mathbb{Q}]$, and as usual fix a quaternionic datum $(\mathcal{O}, \mathcal{I}, \varrho)$.

Let $(A, \mathcal{L})/\mathbb{Q}$ be a polarized abelian variety of dimension $g = 2n$ admitting quaternionic multiplication by the fixed datum over $\bar{\mathbb{Q}}$. Since $X_B(\mathbb{Q}) = \emptyset$ by Theorem 4.1, note that the quaternionic multiplication cannot be defined over $\mathbb{Q}$. Assume moreover that $E = \operatorname{End}^0_{\mathbb{Q}}(A)$ is a number field of degree $g = [E : \mathbb{Q}]$, thus $R = \operatorname{End}_{\mathbb{Q}}(A)$ is an order in E, which is quadratic over F and a maximal subfield of B. This implies that A is an abelian variety of GL_2*-type over* $\mathbb{Q}$. These kind of abelian varieties were first introduced by K. A. Ribet in [**Rib92**] and studied by E. Pyle [**Pyl02**] (see also [**Rot08**], [**BFGR06**]).

Let also $K/\mathbb{Q}$ be the minimal field of definition of all the endomorphisms of $A \times \bar{\mathbb{Q}}$, that is, the minimal field K such that $\operatorname{End}_{\bar{\mathbb{Q}}}(A) = \operatorname{End}_K(A)$. Then $\mathcal{O} \simeq \operatorname{End}_K(A)$ and $B \simeq \operatorname{End}^0_K(A)$. It is possible to show that E is totally real and K is an imaginary quadratic field, so that we can write $E = F(\sqrt{m})$, $K = \mathbb{Q}(\sqrt{-d})$ for some $m \in F_+$ and some $d \in \mathbb{Q}$, $d > 0$. Briefly, this fact can be proved as follows. The Galois group $G_{\mathbb{Q}} = \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts naturally on the ring of endomorphisms $\mathcal{O} \simeq \operatorname{End}_K(A)$. For any $\sigma \in G_{\mathbb{Q}}$, the induced automorphism $B \to B$ is described, by the Noether-Skolem Theorem, by $\beta \mapsto \beta^\sigma = \gamma_\sigma \beta \gamma_\sigma^{-1}$ for some $\gamma_\sigma \in \mathcal{O}$ that normalizes $\mathcal{O}$ ($\beta^\sigma \in \mathcal{O}$ for every $\beta \in \mathcal{O}$). Furthermore, since the endomorphisms in $R \subset \mathcal{O}$ are defined over $\mathbb{Q}$, γ_σ belongs to the commutator of E in B, which turns out to be E itself because it is a maximal subfield of B. So $\sigma_\gamma \in R = E \cap \mathcal{O}$. In this way one finds a continuous homomorphism

$$\psi : G_{\mathbb{Q}} \longrightarrow E^\times/F^\times, \sigma \mapsto \gamma_\sigma,$$

which can be used to show the above assertions (see e.g. [**Rot08**, Lemma 2.3]).

On the other hand, if $\alpha : G_{\mathbb{Q}} \to E^\times$ is a lift of ψ (which needs not to be a homomorphism), then the map

$$c : G_{\mathbb{Q}} \times G_{\mathbb{Q}} \longrightarrow F^\times, (\sigma, \tau) \mapsto c(\sigma, \tau) = \frac{\alpha(\sigma)\alpha(\tau)}{\alpha(\sigma\tau)}$$

satisfies the cocycle condition, and hence defines an element $[c]$ in $\mathrm{H}^2(G_{\mathbb{Q}}, F^\times)$ (here $F^\times$ is regarded as a $G_{\mathbb{Q}}$-module with trivial action, and $[c]$ does not depend on the choice of the lift α). Now, we can consider the image of $[c]$ under the map

$$\xi : \mathrm{H}^2(G_{\mathbb{Q}}, F^\times) \longrightarrow \mathrm{H}^2(G_F, F^\times) \longrightarrow \mathrm{H}^2(G_F, \bar{\mathbb{Q}}^\times) = \mathrm{Br}(F),$$

where the first arrow is the restriction map and the second one is the induced by the inclusion $F^\times \hookrightarrow \bar{\mathbb{Q}}^\times$ ($\bar{\mathbb{Q}}^\times$ is viewed as a $G_{\mathbb{Q}}$-module with the natural Galois action). The importance of this 2-cocycle relies in the following theorem attributed to Chi (see [**Rib92**, Theorem 5.6]):

Theorem 6.1 (Chi). *The class of B in $\mathrm{Br}(F)$ coincides with $\xi([c])$:*

$$\xi([c]) = [B].$$

Corollary 6.2. *With the above notations, $B \simeq (\frac{-d,m}{F})$.*

Proof. Indeed, we know that $E = F(\sqrt{m})$ is a subfield of B. But now, since the character ψ is trivial on $G_K = \mathrm{Gal}\,(\bar{\mathbb{Q}}/K)$, it is also trivial on G_{KF}, where the composite field KF is just $F(\sqrt{-d})$. Then, the cohomology class $[c]$ can be regarded as an element in $\mathrm{H}^2(\mathrm{Gal}\,(F(\sqrt{-d})/F), F^\times)$, and instead of viewing $\xi([c])$ as taking values in $\bar{\mathbb{Q}}^\times$, we can regard it taking values in $F(\sqrt{-d})^\times$. That is, we can think $\xi([c]) \in \mathrm{H}^2(\mathrm{Gal}\,(F(\sqrt{-d})/F), F(\sqrt{-d})^\times) = \mathrm{Br}(F(\sqrt{-d})/F)$, the relative Brauer group. From this remark, it follows that $F(\sqrt{-d})$ is a subfield of B. Once we know this, and noting that the cocycle c factors through $\mathrm{Gal}\,(K/\mathbb{Q})$, if $\sigma \in \mathrm{Gal}\,(K/\mathbb{Q})$ denotes the nontrivial element, then $c(\sigma, \sigma) = \alpha(\sigma)^2 \in F^\times$, while $\alpha(\sigma) \in E^\times = F(\sqrt{m})^\times$. So we can assume $c(\sigma, \sigma) = m$. Appealing to Exercise 3 of §14.2 of [**Pie82**], we get $B \simeq (\frac{-d,m}{F})$. □

Now we return to the case of Shimura curves, hence to $F = \mathbb{Q}$. In this case, the problem of deciding when an abelian surface with quaternionic multiplication corresponding to a point $P \in X_B(k)$, for k a characteristic zero field, admits a model rational over k was solved by Jordan in [**Jor86**]. A necessary and sufficient condition is that k splits B, as stated in Theorem 4.2. Now we want to study this problem for abelian surfaces with real multiplication by the totally real quadratic field $\mathbb{Q}(\sqrt{m})$ corresponding to a point $Q \in X_B^{(m)}(\mathbb{Q})$, assuming that the Atkin-Lehner involution ω_m is twisting.

Recall that when $F = \mathbb{Q}$ the three Atkin-Lehner groups introduced in Chapter 2 coincide, and moreover we can choose any set of elements α_m in $\mathrm{Norm}_{B^\times}(\mathcal{O}) \cap \mathcal{O}$ whose reduced norms range over the positive divisors of $D = \mathrm{disc}(B)$ as representatives for the group W_D, so that we can write

$$W_D = \{\omega_m : m|D, m > 0\} \subseteq \mathrm{Aut}_{\mathbb{Q}}(X_B),$$

where ω_m is the involution induced by α_m.

Then, in a similar direction of that in Theorem 4.2, the following result was proved in [**BFGR06**]. Here $X_B^{(m)}(\mathbb{Q})_{nh}$ stands for the set of non-Heegner points in $X_B^{(m)}(\mathbb{Q})$.

Theorem 6.3. *There exists an abelian surface $A/\mathbb{Q}$ such that $\mathrm{End}^0_{\mathbb{Q}} \simeq \mathbb{Q}(\sqrt{m})$ and $\mathrm{End}_{\bar{\mathbb{Q}}}(A) \simeq \mathcal{O}$ if and only if there exists $Q \in X_B^{(m)}(\mathbb{Q})_{nh}$ such that $\pi_m^{-1}(Q) \subset X_B(K)$ for an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-d})$ with*

$$B \simeq \left(\frac{-d, m}{\mathbb{Q}}\right),$$

where $\pi_m : X_B \to X_B^{(m)}$ is the natural projection.

From this result and its proof, we have a criterion to decide whether the abelian surface corresponding to a point $Q \in X_B^{(m)}(\mathbb{Q})_{nh}$ admits a model rational over $\mathbb{Q}$ or not. Namely, the preimages of Q by the natural projection π_m must lie in $X_B(K)$ for an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-d})$ such that $B \simeq (\frac{-d,m}{\mathbb{Q}})$.

In the next section, we should generalize the above result to abelian surfaces over $\mathbb{Q}_\ell$, for any prime ℓ.

2. Abelian surfaces parametrized by $X_B^{(m)}(\mathbb{Q}_\ell)$

Towards a generalization of Theorem 6.3, let k be either a number field or a finite extension of $\mathbb{Q}_\ell$, for some prime ℓ. Let also $B = B_D$ be the (unique up to isomorphism) rational indefinite quaternion algebra of reduced discriminant $D = p_1 \cdots p_{2r}, r \geq 1$, $\mathcal{O} \subseteq B$ a maximal order (unique up to conjugation), and ϱ a positive anti-involution on B. We consider the abelian surfaces with quaternionic multiplication parametrized by the Shimura curve X_B defined by the quaternionic datum $(B, \mathcal{O}, \varrho)$ (of principal type). Recall that, in particular, $\varrho = \varrho_\mu : \beta \mapsto \mu^{-1}\bar{\beta}\mu$ for some $\mu \in \mathcal{O}$ with $\mu^2 + D = 0$. As in the previous section, we restrict ourselves to abelian surfaces corresponding to non-Heegner points of X_B.

Fixed a positive divisor m of D, assume that the Atkin-Lehner involution ω_m on the Shimura curve X_B is a twisting involution. In particular, $B \simeq (\frac{-D,m}{\mathbb{Q}})$, and the ring of integers $R_{\mathbb{Q}(\sqrt{m})}$ of the quadratic field $\mathbb{Q}(\sqrt{m})$ is optimally embedded in $\mathcal{O}$. Then, recall that the forgetful map $\pi_{R_{\mathbb{Q}(\sqrt{m})}} : X_B \to \mathcal{H}_{R_{\mathbb{Q}(\sqrt{m})}}$ from X_B to the Hilbert surface classifying abelian surfaces with real multiplication by $R_{\mathbb{Q}(\sqrt{m})}$ factors through the Atkin-Lehner quotient $X_B^{(m)}$.

In order to achieve our goal, we adapt the arguments of the proof of Theorem 6.3 given in [**BFGR06**]. The first main ingredient is a well-known result due to A. Weil ([**Wei56**]):

Theorem 6.4 (Weil)**.** *A polarized abelian variety $(A, \mathcal{L})/k$ admits a model rational over its field of moduli k_0 if and only if for each $\sigma \in \mathrm{Gal}\,(\bar{k}_0/k_0)$ there exists an isomorphism $\mu_\sigma : (A^\sigma, \mathcal{L}^\sigma) \to (A, \mathcal{L})$ such that $\mu_\sigma \mu_\tau^\sigma = \mu_{\sigma\tau}$ for any $\sigma, \tau \in \mathrm{Gal}\,(\bar{k}_0/k_0)$.*

Relating the field of definition of the endomorphisms of abelian surfaces A/k with QM by $\mathcal{O}$ admitting real multiplication by $R_{\mathbb{Q}(\sqrt{m})}$ over k, we now prove that all the quaternionic multiplication is defined, at most, over a quadratic field extension K/k by adapting an argument which has already been sketched in the previous section:

Lemma 6.5. *Let A/k be an abelian surface such that $\mathrm{End}^0_k(A) \supseteq \mathbb{Q}(\sqrt{m})$ and $\mathrm{End}_{\bar{k}}(A) \simeq \mathcal{O}$. Let K/k be the minimal extension over which all the endomorphisms of $A \times \bar{k}$ are defined, i.e. $\mathrm{End}_K(A) \simeq \mathcal{O}$. Then K/k is at most of degree 2, and it does not admit a real embedding.*

Proof. First we prove that K/k is of degree at most two. For this, note that the Galois group $G_k = \mathrm{Gal}\,(\bar{k}/k)$ acts on the ring of endomorphisms $\mathrm{End}_{\bar{k}}(A) \simeq \mathcal{O}$. By the Noether-Skolem Theorem, the automorphism $B \to B$, $\beta \mapsto \beta^\sigma$, induced by any $\sigma \in G_k$ is inner, hence there exists $\gamma_\sigma \in \mathcal{O}$ such that $\beta^\sigma = \gamma_\sigma \beta \gamma_\sigma^{-1}$ for every $\beta \in \mathcal{O}$.

On the other hand, let $R = \mathrm{End}_k(A) \cap \mathbb{Q}(\sqrt{m}) \subset \mathcal{O}$, which is a suborder of the ring of integers of $\mathbb{Q}(\sqrt{m})$. Since the endomorphisms in R are defined over k, it follows that for any

$\sigma \in G_k$ the element γ_σ belongs to the commutator of $\mathbb{Q}(\sqrt{m})$ in B, which is $\mathbb{Q}(\sqrt{m})$ itself because it is a maximal subfield of B. Hence for any $\sigma \in G_k$ we have $\gamma_\sigma \in \mathbb{Q}(\sqrt{m}) \cap \mathcal{O}$. As a consequence, we get a continuous homomorphism

$$\psi : G_k \longrightarrow \mathbb{Q}(\sqrt{m})^\times/\mathbb{Q}^\times, \quad \sigma \longmapsto \gamma_\sigma.$$

It is straightforward that the kernel of this homomorphism is

$$\ker(\psi) = \{\sigma \in G_k : \gamma_\sigma \in \mathbb{Q}^\times\} = \{\sigma \in G_k : \beta^\sigma = \beta \ \ \forall \beta \in \mathcal{O}\} = \mathrm{Gal}\,(\bar{k}/K).$$

Therefore, K/k is a Galois extension and $\mathrm{Gal}\,(K/k) \simeq G_k/\ker(\psi)$. But now observe that being $\mathbb{Q}(\sqrt{m})$ totally real, it contains no roots of unity $\zeta \neq \pm 1$, and then the non-trivial finite subgroups of $\mathbb{Q}(\sqrt{m})^\times/\mathbb{Q}^\times$ must be of order two. In particular, since ψ embeds $\mathrm{Gal}\,(K/k)$ in $\mathbb{Q}(\sqrt{m})^\times/\mathbb{Q}^\times$ it follows that $[K : k] \leq 2$.

The second part of the statement follows from an argument essentially due to Ribet (see Theorems 1 and 2 in [**Rib81**]). □

Remark 6.6. In the above lemma, if k is totally real then $[K : k] = 2$. In particular, this forces the inclusion $\mathbb{Q}(\sqrt{m}) \subseteq \mathrm{End}_k^0(A)$ to be an equality.

The following lemma exploits a little bit more the relation between the field extension K/k over which all endomorphisms of an abelian surface A as in the previous lemma are defined and the arithmetic of B:

Lemma 6.7. *Let A/k be an abelian surface such that* $\mathrm{End}_k^0(A) \supseteq \mathbb{Q}(\sqrt{m})$ *and* $\mathrm{End}_K^0(A) \simeq B$*, where $K = k(\sqrt{\delta})$ is a field extension of degree at most 2 not admitting a real embedding. Then $B \otimes_{\mathbb{Q}} k \simeq (\frac{\delta, m}{k})$.*

Proof. Let $\alpha : G_k \to \mathbb{Q}(\sqrt{m})^\times$ be a lift of the homomorphism ψ from the last lemma. As in the previous section, α induces a 2-cocycle

$$c : G_k \times G_k \longrightarrow \mathbb{Q}^\times, (\sigma, \tau) \mapsto c(\sigma, \tau) = \frac{\alpha(\sigma)\alpha(\tau)}{\alpha(\sigma\tau)},$$

which defines an element $[c] \in \mathrm{H}^2(G_k, \mathbb{Q}^\times)$. Now the inclusion $\mathbb{Q}^\times \hookrightarrow \bar{k}^\times$ induces in cohomology a map $\xi : \mathrm{H}^2(G_k, \mathbb{Q}^\times) \to \mathrm{H}^2(G_k, \bar{k}^\times) = \mathrm{Br}(k)$. The arguments in the proof of Theorem 6.1 given by Ribet (see [**Rib92**, Theorem 5.6]) apply here in an analogous way to ensure that the class of $B \otimes_{\mathbb{Q}} k$ in $\mathrm{Br}(k)$ coincides with $\xi([c])$.

Now, assume first that $m \in (k^\times)^2$. Then we can regard k as a field extension of $\mathbb{Q}(\sqrt{m})$, which is a splitting field of B, hence k also splits B. On the other hand, if m is a square in k then $(\frac{\delta, m}{k}) \simeq (\frac{\delta, 1}{k}) \simeq \mathrm{M}_2(k)$, so that the isomorphism $B \otimes_{\mathbb{Q}} k \simeq (\frac{\delta, m}{k})$ holds. In the same way, if δ is a square in $k^\times$ one has $(\frac{\delta, m}{k}) \simeq (\frac{1, m}{k}) \simeq \mathrm{M}_2(k)$. But in this case, $\delta \in (k^\times)^2$ corresponds to $K = k$, which implies that the cocycle c is trivial, hence $B \otimes_{\mathbb{Q}} k \simeq \mathrm{M}_2(k)$.

Therefore, suppose that neither m nor δ are squares in k, so that both $K = k(\sqrt{\delta})$ and $k(\sqrt{m})$ are quadratic extensions of k. Then, since $\mathbb{Q}(\sqrt{m})$ is a splitting field of B and $\mathbb{Q}(\sqrt{m}) \otimes_{\mathbb{Q}} k = k(\sqrt{m})$, we get that $k(\sqrt{m})$ splits $B \otimes_{\mathbb{Q}} k$ as well, hence $B \otimes_{\mathbb{Q}} k$ contains a maximal subfield isomorphic to $k(\sqrt{m})$. On the other hand, the homomorphism ψ is trivial on G_K, which implies that c factors through $\mathrm{Gal}\,(K/k) = G_k/G_K$. Arguing like at the end of the previous section, we obtain the desired isomorphism $B \otimes_{\mathbb{Q}} k \simeq (\frac{\delta, m}{k})$. □

When working with (polarized) abelian surfaces with quaternionic multiplication, the role of the polarization is quite important. For example, there are no non-trivial automorphisms in a polarized abelian surface with QM away from the Heegner locus of X_B:

Lemma 6.8. *Let $(A, \mathcal{L})/k$ be a polarized abelian surface such that* $\mathrm{End}_{\bar{k}}(A) \simeq \mathcal{O}$*. Then* $\mathrm{Aut}_{\bar{k}}(A, \mathcal{L}) = \{\pm 1\}$.

Proof. This lemma is stated in [**BFGR06**, Lemma 4.2] for abelian varieties defined over number fields, but the proof given there is also valid for the case where they are defined over any field of characteristic zero. □

Furthermore, recall that we assumed that the abelian surfaces parametrized by X_B are all principal, or in other words, that the quaternionic datum $(B, \mathcal{O}, \varrho)$ is of principal type. This is the reason for the main difference between the statement of the next theorem and [**BFGR06**, Theorem 4.5]. Once we have adapted the main ingredients for the proof in the above lemmas, the proof of the theorem goes essentially as in [**BFGR06**], but we include it for completeness.

Theorem 6.9. *There exists a principally polarized abelian surface $(A, \mathcal{L})/k$ such that $\mathrm{End}_k^0(A) \supseteq \mathbb{Q}(\sqrt{m})$ and $\mathrm{End}_{\bar{k}}(A) \simeq \mathcal{O}$ if and only if there exists $Q \in X_B^{(m)}(k)_{nh}$ such that $\pi_m^{-1}(Q) \subseteq X_B(K)$ for a quadratic field $K = k(\sqrt{\delta})$, $\delta \in R_k$, not admitting a real embedding, with*

$$B \otimes_{\mathbb{Q}} k \simeq \left(\frac{\delta, m}{k}\right).$$

When this is the case, K corresponds to the minimal field of definition of all the endomorphisms of $A \times \bar{\mathbb{Q}}$.

Proof. **Part I.** Assume that there exists a principally polarized abelian surface $(A, \mathcal{L})/k$ such that $\mathrm{End}_k^0(A) \supseteq \mathbb{Q}(\sqrt{m})$ and $\mathrm{End}_{\bar{k}}(A) \simeq \mathcal{O}$. We want to attach to A a point $Q \in X_B^{(m)}(k)_{nh}$ satisfying the conditions in the statement.

Fixing an isomorphism $\iota : \mathcal{O} \overset{\simeq}{\to} \mathrm{End}_{\bar{k}}(A)$, then $R = \iota^{-1}(\mathrm{End}_k(A) \cap \mathbb{Q}(\sqrt{m}))$ is isomorphic to a quadratic order of $\mathbb{Q}(\sqrt{m})$, and by construction R is optimally embedded in $\mathcal{O}$.

On the other hand, we know by Lemma 6.5 that $\mathrm{End}_{\bar{k}}(A) = \mathrm{End}_K(A) \simeq \mathcal{O}$ for some field extension $K = k(\sqrt{\delta})$ of degree at most two, with $\delta \in R_k$, where R_k is the ring of integers of k. In this way, the triplet $(A, \iota, \mathcal{L})$ produces a point P in $X_B(K)$. However, the triplet $(A, \iota_{|R}, \mathcal{L})$ is defined over k, so that $\pi_R(P) \in \mathcal{H}_R(k)$. Now, as it was quoted above, this forgetful map $\pi_R : X_B \to \mathcal{H}_R$ factors through the Atkin-Lehner quotient $\pi_m : X_B \to X_B^{(m)}$. Indeed, π_R is birationally equivalent to the composition of π_m and an immersion of $X_B^{(m)}$ into $\mathcal{H}_R$. Therefore, $Q = \pi_m(P) \in X_B^{(m)}(k)_{nh}$ (hence, $\pi_m^{-1}(Q) = \{P, \omega_m(P)\} \subseteq X_B(K)$).

Finally, by Lemma 6.7 we have $B \otimes_{\mathbb{Q}} k \simeq (\frac{\delta, m}{k})$.

Part II. Conversely, let $K = k(\sqrt{\delta})$ be a quadratic extension of k. Assume that $B \otimes_{\mathbb{Q}} k \simeq (\frac{\delta, m}{k})$ and let $P \in X_B(K)$ satisfy $Q = \pi_m(P) \in X_B^{(m)}(k)_{nh}$ (so that $\pi_m^{-1}(Q) = \{P, \omega_m(P)\} \subseteq X_B(K)$). Choose $\mu \in \mathcal{O} \otimes_{\mathbb{Z}} R_k$, $\omega \in \mathcal{O}$, such that $\mu^2 = \delta$, $\omega^2 = m$, $\mu\omega = -\omega\mu$ and let $R = \mathbb{Q}(\omega) \cap \mathcal{O}$. The choice of the element μ determines an embedding of K into $B \otimes_{\mathbb{Q}} k$, hence K splits $B \otimes_{\mathbb{Q}} k$, hence also B. By [**Jor81**, Theorem 2.1.3], this implies that the point $P \in X_B(K)$ can be represented by the $\bar{k}$-isomorphism class of a (principally) polarized simple abelian surface with quaternionic multiplication $(A_0, \iota_0, \mathcal{L}_0)$ *completely defined over* K and such that the Rosati involution induced by $\mathcal{L}_0$ on B is ϱ_μ. As before, by using the forgetful map $\pi_R : X_B \to \mathcal{H}_R$, the condition $\pi_m(P) \in X_B^{(m)}(k)_{nh}$ implies that $\pi_R(P) \in \mathcal{H}_R(k)$. Therefore, the field of moduli of $(A_0, \iota_{0|R}, \mathcal{L}_0)$ is k.

For any field extension $k \subseteq F \subseteq \bar{k}$, we write as usual $G_F = \mathrm{Gal}(\bar{k}/F)$. Let $\sigma \in G_k \backslash G_K$. Then there exists an isomorphism $\nu : A_0 \to A_0^\sigma$ such that $\nu^*(\mathcal{L}_0^\sigma) = \mathcal{L}_0$ and $\nu \cdot \omega^{-1} \cdot \alpha \cdot \omega = \alpha^\sigma \cdot \nu$ for all endomorphisms $\alpha \in B = \mathrm{End}_K^0(A)$. In particular, by taking $\alpha = \omega, \mu$ we get the following relations:

$$\nu \cdot \omega = \omega^\sigma \cdot \nu\,, \quad \nu \cdot \mu = -\mu^\sigma \cdot \nu\,.$$

Now, before proceeding with the proof, we need the following fact:

Claim: ν may be assumed to be defined over K.

To prove this claim, first observe that since $\mathrm{End}_{\bar{k}}(A_0) \simeq \mathcal{O}$, Lemma 6.8 applies to ensure that $\mathrm{Aut}_K(A_0, \mathcal{L}_0) = \{\pm 1\}$. Since $(A_0, \mathcal{L}_0)$ is defined over K, it turns out that for each $\tau \in G_K$, the composition $\nu^{-1} \cdot \nu^{\tau}$ defines an element in $\mathrm{Aut}_K(A_0, \mathcal{L}_0)$. So consider the group homomorphism $\rho_\nu : G_K \to \mathrm{Aut}_K(A_0, \mathcal{L}_0) = \{\pm 1\}$ defined by $\rho_\nu(\tau) = \nu^{-1} \cdot \nu^{\tau}$.

Assume for contradiction that ν is not defined over K, that is $\rho_\nu(G_K) = \{\pm 1\}$, and let L/K be the quadratic extension such that $G_L = \ker(\rho_\nu)$. Since L is the minimal field of definition of all homomorphisms in $\mathrm{Hom}(A_0, A_0^{\sigma})$ and $\mathrm{Hom}(A_0^{\sigma}, A_0)$, we deduce that L/k is a Galois extension. Since K does not admit a real embedding, L/k can not be cyclic and hence there exists an square-free $d \in R_k$ such that $L = K(\sqrt{d})$, the diagram of extensions being

$$\begin{tikzcd}
 & L = K(\sqrt{d}) \arrow[dl, dash] \arrow[dd, dash] \arrow[dr, dash] & \\
k(\sqrt{d}) \arrow[dr, dash] & & K = k(\sqrt{\delta}) \arrow[dl, dash] \\
 & k &
\end{tikzcd}$$

Now let $V_K = H^0(A_0, \Omega^1_{A_0/K})$ denote the vector space of regular differentials on A over K. Since $B \simeq \mathrm{End}^0_K(A_0)$, the natural action of the endomorphisms on V_K induces an embedding $* : B \hookrightarrow \mathrm{End}_K(V_K) \simeq \mathrm{M}_2(K)$ and an isomorphism $B \otimes_{\mathbb{Q}} K \simeq K + K\mu + K\omega + K\mu\omega \simeq \mathrm{M}_2(K)$. By the Noether-Skolem Theorem, all the automorphisms of $\mathrm{M}_2(K)$ are inner, so that we may choose basis of V_K such that the matrix expressions of ω^* and μ^* acting on V_K are

$$M_m = \begin{pmatrix} 0 & 1 \\ m & 0 \end{pmatrix}, \quad M_\delta = \begin{pmatrix} \sqrt{\delta} & 0 \\ 0 & -\sqrt{\delta} \end{pmatrix},$$

respectively. With these notations we have $B \otimes K \simeq \mathrm{M}_2(K) = K + KM_\delta + KM_m + KM_\delta M_m$.

Let $N \in \mathrm{GL}_2(K(\sqrt{d}))$ be the matrix expression of $\nu \in \mathrm{Hom}(A_0, A_0^{\sigma})$ with respect to this basis of V_K and its Galois conjugate of V_K^{σ}. Then N satisfies

$$N^{\tau} = -N, \quad M_m \cdot N = N \cdot M_m^{\sigma} = N \cdot M_m, \quad M_\delta \cdot N = -N \cdot M_\delta^{\sigma} = N \cdot M_\delta,$$

for $\tau \in G_K \setminus G_L$. Hence, $N = \sqrt{d}\begin{pmatrix} \beta & 0 \\ 0 & \beta \end{pmatrix}$ for some $\beta \in K$, because $B \otimes_{\mathbb{Q}} K$ is central over K. Fix $\sigma \in G_{k(\sqrt{d})}$, $\sigma \notin G_K$. We have $\nu^{\sigma} \cdot \nu \in \mathrm{Aut}(A_0, \mathcal{L}_0) = \{\pm 1\}$, thus $N \cdot N^{\sigma} = \pm\mathrm{id}$ and $\beta \cdot \beta^{\sigma} = 1/d$. This implies that the normal closure F of the extension $K(\sqrt{\beta})/k$ is dihedral containing $K(\sqrt{d})$ and that the extension $F/k(\sqrt{d \cdot \delta})$ is cyclic. Let $\rho_\beta : G_K \to \{\pm 1\}$ be the surjective morphism such that $\ker(\rho_\beta) = G_{K(\sqrt{\beta})}$. Attached to the cocycle $\rho_\beta \in H^1(G_K, \{\pm 1\})$ there is a polarized abelian surface $(A_1, \mathcal{L}_1)$ defined over K together with an isomorphism $\lambda : (A_0, \mathcal{L}_0) \to (A_1, \mathcal{L}_1)$ such that $\lambda^{\tau} = \lambda \cdot \rho_\beta(\tau)$. We claim that $\phi = \lambda^{\sigma} \cdot \nu \cdot \lambda^{-1} : A_1 \to A_1^{\sigma}$ is defined over K. Indeed, for any $\tau \in G_K$,

$$\phi^{\tau} = (\lambda^{\sigma\cdot\tau\cdot\sigma^{-1}})^{\sigma} \cdot \nu^{\tau} \cdot (\lambda^{-1})^{\tau} = \rho_\beta(\sigma \cdot \tau \cdot \sigma^{-1} \cdot \tau^{-1}) \cdot \rho_\nu(\tau) \cdot \phi.$$

But recall that both ρ_β and ρ_ν take values in $\{\pm 1\}$, and $\ker(\rho_\nu) = G_{K(\sqrt{d})}$, $\ker(\rho_\beta) = G_{K(\sqrt{\beta})}$. Then, since $\sigma \cdot \tau \cdot \sigma^{-1} \cdot \tau^{-1} \in G_{K(\sqrt{\beta})}$ if and only if $\tau \in G_{K(\sqrt{d})}$, we get that $\phi^{\tau} = \phi$. Moreover, all the endomorphisms of A_1 are of the form $\lambda \cdot \varphi \cdot \lambda^{-1}$ with φ in $\mathrm{End}_K(A_0)$. These are all defined over K because

$$(\lambda \cdot \varphi \cdot \lambda^{-1})^{\tau} = \rho_\beta(\tau \cdot \tau^{-1})\lambda \cdot \varphi \cdot \lambda^{-1} = \lambda \cdot \varphi \cdot \lambda^{-1}.$$

Then the claim is proved and we therefore assume that ν is defined over K.

Now we may show that $(A_0, \mathcal{L}_0)$ admits a model over k with all its endomorphisms defined over K, and for doing so we will use Theorem 6.4. Since $(A_0, \mathcal{L}_0)$ is already defined over K, we do not need to check the condition in Theorem 6.4 for the elements in $G_K \subset G_k$. And for those in $G_k \backslash G_K$, it is enough to prove it for the element σ singled out above, since G_K has index two in G_k.

Note first that $\sigma^2 \in G_K$, so that $\nu^\sigma \cdot \nu \in \mathrm{Aut}(A_0, \mathcal{L}_0)$, hence $\nu^\sigma \cdot \nu = s \,\mathrm{id}$ with $s \in \{\pm 1\}$. Using the same basis of $H^0(A_0, \Omega^1_{A_0/K})$ and $H^0(A_0^\sigma, \Omega^1_{A_0^\sigma/K})$ as before, the matrix expression $N \in \mathrm{GL}_2(K)$ of ν satisfies $M_m \cdot N = N \cdot M_m^\sigma = N \cdot M_m, M_\delta \cdot N = -N \cdot M_\delta^\sigma = N \cdot M_\delta$. It follows that

$$N = \begin{pmatrix} \beta & 0 \\ 0 & \beta \end{pmatrix}, \quad \beta \in K.$$

Hence, $\beta \cdot \beta^\sigma = s$. Since K does not admit a real embedding, $s = 1$. Then Theorem 6.4 applies to ensure the existence of a polarized abelian surface $(A, \mathcal{L})$ defined over k and isomorphic over K to $(A_0, \mathcal{L}_0)$. Since $A \simeq A_0$ over K, we obtain that there is an isomorphism $\iota : \mathcal{O} \xrightarrow{\sim} \mathrm{End}_K(A)$.

Finally, it remains to show that $\mathrm{End}^0_k(A) \supseteq \mathbb{Q}(\sqrt{m})$. The triplets $(A, \iota, \mathcal{L})$ and $(A_0, \iota_0, \mathcal{L}_0)$ are isomorphic over K, and the fact that $[(A, \iota_{|R}, [\mathcal{L}])] \in X_B^{(m)}(k)$ implies that for every $\sigma \in G_k$ and every $\alpha \in R$ we have $\iota(\alpha)^\sigma = \iota(\alpha) \in \mathrm{End}_{\bar{k}}(A)$. Hence $\iota(R) \subseteq \mathrm{End}_k(A)$. Therefore, $\mathbb{Q}(\sqrt{m}) = R \otimes \mathbb{Q} \subseteq \mathrm{End}^0_k(A) \subseteq \mathrm{End}^0_{\bar{k}}(A) = B$. □

Remark 6.10. Suppose that $(A, \iota, [\mathcal{L}])$ is a QM-abelian surface corresponding to a point $P \in X_B(k)$, hence $\pi_m(P) \in X_B^{(m)}(k)$. Then with notations from Theorem 6.9, $K = k$ and the theorem says that $(A, \iota, [\mathcal{L}])$, as a QM-abelian surface, admits a model rational over k if and only if k splits B, since $\delta \in k^{\times 2}$ implies $(\frac{\delta, m}{k}) \simeq \mathrm{M}_2(k)$. Hence we recover Theorem 4.2 of Jordan.

Since we are especially interested in the case $k = \mathbb{Q}_\ell$ for a prime ℓ, we rewrite the theorem as a corollary in this case:

Corollary 6.11. *There exists a principally polarized abelian surface* $(A, \mathcal{L})/\mathbb{Q}_\ell$ *such that* $\mathrm{End}^0_{\mathbb{Q}_\ell}(A) \supseteq \mathbb{Q}(\sqrt{m})$ *and* $\mathrm{End}_{\bar{\mathbb{Q}}_\ell}(A) \simeq \mathcal{O}$ *if and only if there exists* $Q_\ell \in X_B^{(m)}(\mathbb{Q}_\ell)_{nh}$ *such that* $\pi_m^{-1}(Q_\ell) \subseteq X_B(K_\ell)$, *where* $K_\ell = \mathbb{Q}_\ell(\sqrt{\delta})$ *satisfies*

$$B \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \simeq \left(\frac{\delta, m}{\mathbb{Q}_\ell} \right).$$

When this is the case, K_ℓ *corresponds to the minimal field of definition of all the endomorphisms of* $A \times \bar{\mathbb{Q}}_\ell$.

Definition 6.12. *With the above notations, we will say that* the pair (B, m) satisfies condition (M) with respect to the prime ℓ *if for every non-Heegner point* $Q_\ell \in X_B^{(m)}(\mathbb{Q}_\ell)_{nh}$, *we have an isomorphism* $B \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \simeq (\frac{\delta, m}{\mathbb{Q}_\ell})$, *where* $\mathbb{Q}_\ell(\sqrt{\delta})$ *is an at most quadratic extension of* $\mathbb{Q}_\ell$ *such that* $\pi_m^{-1}(Q_\ell) \subseteq X_B(\mathbb{Q}_\ell(\sqrt{\delta}))$.

Remark 6.13. By Corollary 6.11, if (B, m) satisfies condition (M) with respect to ℓ, then every abelian surface parametrized by $X_B^{(m)}(\mathbb{Q}_\ell)_{nh}$ admits a model rational over $\mathbb{Q}_\ell$, and conversely. What is more, by the remark at the beginning of the chapter, we have actually that if (B, m) satisfies condition (M) with respect to ℓ, then every abelian surface parametrized by $X_B^{(m)}(\mathbb{Q}_\ell)$ admits a model rational over $\mathbb{Q}_\ell$.

Note the analogy with the case of abelian surfaces parametrized by $X_B(\mathbb{Q}_\ell)$: by Theorem 4.2, if $\mathbb{Q}_\ell$ splits B then every abelian surface parametrized by $X_B(\mathbb{Q}_\ell)$ admits a model rational over $\mathbb{Q}_\ell$. Fixed the prime ℓ, this is a condition which depends only on B. Now, if (B, m) satisfies condition (M) then every abelian surface parametrized by $X_B^{(m)}(\mathbb{Q}_\ell)$ admits a model rational over $\mathbb{Q}_\ell$. But observe that assuming this condition amounts to assume a condition for *every* point $Q_\ell \in X_B^{(m)}(\mathbb{Q}_\ell)$, which is difficult to check in practice.

Although this big difference, working under the hypothesis that condition (M) is satisfied by (B, m) for some particular primes, we can achieve an approach to our main theorem, as is proved in Theorem 7.19.

Since condition (M) is not easy to check, and since moreover we would like to remove it at the end, we should explore what we can say about the field of rationality of an abelian surface (A_ℓ, i_ℓ) parametrized by a point in $X_B^{(m)}(\mathbb{Q}_\ell)$, for some prime ℓ. As we show below, under some mild hypotheses we can control quite well some aspects of it.

So, consider a point $Q_\ell \in X_B^{(m)}(\mathbb{Q}_\ell)$ corresponding to an abelian surface (A_ℓ, i_ℓ) with real multiplication by the ring of integers $R_{\mathbb{Q}(\sqrt{m})}$ of $\mathbb{Q}(\sqrt{m})$ whose field of moduli is $\mathbb{Q}_\ell$. Let also $K_\ell/\mathbb{Q}_\ell$ be an at most quadratic extension such that $\pi_m^{-1}(Q_\ell) = \{P_\ell, P'_\ell\} \subseteq X_B(K_\ell)$, with $P'_\ell = \omega_m(P_\ell)$, and where π_m is the natural projection as before.

The point P_ℓ corresponds to an abelian surface (A_ℓ, ι_ℓ) with quaternionic multiplication by B (note that the underlying abelian surface is the same as for Q_ℓ), such that $\iota_{\ell | R_{\mathbb{Q}(\sqrt{m})}} = i_\ell$, and whose field of moduli is contained in K_ℓ.

Proposition 6.14. *Suppose that $2 \nmid D$. Then, with the above notations, both (A_ℓ, ι_ℓ) and (A_ℓ, i_ℓ) admit a model rational over K_ℓ.*

Proof. The hypothesis $2 \nmid D$ implies, by the results in [**JL85**] (see also [**Jor86**, Theorem 0]), that $X_B(\mathbb{Q}_\ell) = \emptyset$. Therefore, K_ℓ is quadratic over $\mathbb{Q}_\ell$.

Now, suppose first that $\ell \nmid D$. Then $B \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \simeq \mathrm{M}_2(\mathbb{Q}_\ell)$ is the split algebra, so that clearly K_ℓ splits B, and by Theorem 4.2 (A_ℓ, ι_ℓ) admits a model rational over K_ℓ, hence also (A_ℓ, i_ℓ) does.

Secondly, suppose $\ell | D$, so that $B \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ is the unique (up to isomorphism) quaternion division algebra over $\mathbb{Q}_\ell$. Choosing an element $e \in \mathbb{Z}_\ell^\times \backslash \mathbb{Z}_\ell^{\times 2}$, the only quadratic extensions of $\mathbb{Q}_\ell$ are $\mathbb{Q}_\ell(\sqrt{e}), \mathbb{Q}_\ell(\sqrt{\ell})$ and $\mathbb{Q}_\ell(\sqrt{e\ell})$, where the first one is the unique quadratic unramified extension of $\mathbb{Q}_\ell$ and the other two are ramified. In particular, K_ℓ is one of these three quadratic extensions of $\mathbb{Q}_\ell$. But note that all of them are subfields of the quaternion division $\mathbb{Q}_\ell$-algebra

$$B \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \simeq B_\ell = \mathbb{Q}_\ell(\sqrt{e}) + \mathbb{Q}_\ell(\sqrt{e})\pi,$$

where $\pi^2 = \ell$ and $\pi\beta = {}^\tau\beta\pi$ for all $\beta \in \mathbb{Q}_\ell(\sqrt{e})$, and where $\tau \in \mathrm{Gal}\,(\mathbb{Q}_\ell(\sqrt{e})/\mathbb{Q}_\ell)$ is the nontrivial automorphism (see Theorem 1.17). Hence, K_ℓ splits B in any case, and again by Theorem 4.2 (A_ℓ, ι_ℓ) admits a model rational over K_ℓ, hence also (A_ℓ, i_ℓ) does. □

Recall that stating that (A_ℓ, i_ℓ) admits a model rational over K_ℓ amounts to say that A_ℓ admits a model rational over K_ℓ such that $i_\ell : R_{\mathbb{Q}(\sqrt{m})} \hookrightarrow \mathrm{End}_{K_\ell}(A_\ell)$. Besides, saying that (A_ℓ, ι_ℓ) admits a model rational over K_ℓ means that A_ℓ has a model rational over K_ℓ such that $\iota_\ell : \mathcal{O} \hookrightarrow \mathrm{End}_{K_\ell}(A_\ell)$.

As quoted in the proof, under the hypothesis $2 \nmid D$ the field K_ℓ is quadratic over $\mathbb{Q}_\ell$. Then, observe that, although we are stating that (A_ℓ, i_ℓ) admits a model rational over K_ℓ, it may also happen that (A_ℓ, i_ℓ) admits indeed a model rational over $\mathbb{Q}_\ell$ (its field of moduli). Hence, the main point is that we can assume (A_ℓ, i_ℓ) to be defined over an at most quadratic extension $K_\ell/\mathbb{Q}_\ell$, over which (A_ℓ, ι_ℓ) is also defined. In particular, not only the endomorphisms in $\mathbb{Q}(\sqrt{m})$ via i_ℓ become defined over K_ℓ, but all of them in B via ι_ℓ.

For this reason, it is convenient to distinguish between the minimal field of definition F_ℓ of (A_ℓ, i_ℓ) and the field K_ℓ. Here, by the minimal field of definition of (A_ℓ, i_ℓ) we mean the minimal field F_ℓ over which (A_ℓ, i_ℓ) admits a rational model. Being (A_ℓ, i_ℓ) a representative for the isomorphism class of abelian surfaces with real multiplication corresponding to a point $Q_\ell \in X_B^{(m)}(\mathbb{Q}_\ell)$, we may assume that (A_ℓ, i_ℓ) is already defined over F_ℓ. Always supposing that $2 \nmid D$, we have therefore two cases:

Case i): $F_\ell = K_\ell$ is a quadratic extension of $\mathbb{Q}_\ell$, so that $F_\ell = K_\ell$ is either $\mathbb{Q}_\ell(\sqrt{e}), \mathbb{Q}_\ell(\sqrt{\ell})$ or $\mathbb{Q}_\ell(\sqrt{e\ell})$, following the notations from the proposition.

Case ii): $F_\ell = \mathbb{Q}_\ell$. In this case (A_ℓ, i_ℓ) admits a model rational over $\mathbb{Q}_\ell$, so we will assume it is defined over $\mathbb{Q}_\ell$.

In the next chapter, we will use these notations. Summing up, an abelian surface (A_ℓ, i_ℓ) corresponding to a point $Q_\ell \in X_B^{(m)}(\mathbb{Q}_\ell)$ can always be chosen to be defined either over $\mathbb{Q}_\ell$ or over the quadratic field K_ℓ over which the quaternionic multiplication is defined, provided that 2 does not divide D.

Chapter 7
Main result

The final goal of this chapter is to give a proof of our main result stated at the end of Chapter 5. As usual, B denotes an indefinite rational quaternion division algebra, and we consider the Shimura curve X_B parametrizing abelian surfaces with quaternionic multiplication by a fixed datum $(B, \mathcal{O}, \varrho)$. We assume moreover that $2 \nmid D = \operatorname{disc}(B)$, so that the comments and notations after Proposition 6.14 apply. By the result of Milne quoted in Proposition 2.9, and for ease of notation, we consider abelian surfaces with QM as pairs $(A, \iota : \mathcal{O} \hookrightarrow \operatorname{End}(A))$, so that we drop the weak polarization off.

Throughout the chapter, let $p \geq 5$ be a prime factor of D. Let also $m > 0$ be a proper divisor of D such that $p \nmid m$, and assume that the Atkin-Lehner involution ω_m is twisting. Then consider (a model over $\mathbb{Q}$ of) the Atkin-Lehner quotient $X_B^{(m)}$. The points on $X_B^{(m)}$ parametrize isomorphism classes of certain abelian surfaces with real multiplication by the ring of integers R_E of $E = \mathbb{Q}(\sqrt{m})$, as was shown in Proposition 2.33.

On the other hand, adapting the ideas of Skorobogatov we will consider a suitable étale subcovering $Y_{B,p}^{(m)} \to X_B^{(m)}$ of the Galois covering $X_{B,p}^{(m)} \to X_B^{(m)}$ constructed in Chapter 5, which becomes an $X_B^{(m)}$-torsor under $\mathbb{F}_{p^2}^{\times 12}$. Then, following the work of Rotger in [**Rot08**] we relate the characters arising by specialization of this torsor to (suitable *extensions* of) certain Galois representations attached to the abelian surfaces parametrized by $X_B^{(m)}$. The relations we find are analogous to the relations appearing in the work of Skorobogatov and allow us to prove our main result.

1. Galois representations

Let (A_ℓ, i_ℓ) be an abelian surface with real multiplication by the ring of integers R_E of $E = \mathbb{Q}(\sqrt{m})$ corresponding to a point $Q_\ell \in X_B^{(m)}(\mathbb{Q}_\ell)$, for some prime ℓ. In particular, we have $\mathcal{O} \hookrightarrow \operatorname{End}_{\bar{\mathbb{Q}}_\ell}(A_\ell)$. If K_ℓ is the quadratic extension of $\mathbb{Q}_\ell$ such that $\pi_m^{-1}(Q_\ell) \subseteq X_B(K_\ell)$, by Proposition 6.14 both (A_ℓ, i_ℓ) and the abelian surface with quaternionic multiplication corresponding to any of the preimages of Q_ℓ admit a model rational over K_ℓ. Following the notations of the previous chapter, let also F_ℓ be the minimal field of definition of (A_ℓ, i_ℓ) in $K_\ell/\mathbb{Q}_\ell$, so that either i) $F_\ell = K_\ell$, or ii) $F_\ell = \mathbb{Q}_\ell$.

Now, for the fixed prime p, consider the p-adic Tate module $V_p(A_\ell) = T_p(A_\ell) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ of A_ℓ (see Chapter 1). Being A_ℓ defined over F_ℓ, the Galois group $\operatorname{Gal}(\bar{\mathbb{Q}}_\ell/F_\ell)$ acts continuously on $V_p(A_\ell)$ via the natural action on $A_\ell(\bar{\mathbb{Q}}_\ell)$, giving rise to the classical p-adic representation of A_ℓ, namely

$$r_{A_\ell,p} : \operatorname{Gal}(\bar{\mathbb{Q}}_\ell/F_\ell) \longrightarrow \operatorname{Aut}(V_p(A_\ell)) \simeq \operatorname{GL}_4(\mathbb{Q}_p),$$

where the isomorphism depends on the choice of a $\mathbb{Q}_p$-basis of $V_p(A_\ell)$.

On the other hand, $\operatorname{End}^0_{\bar{\mathbb{Q}}_\ell}(A_\ell)$ acts on $V_p(A_\ell)$ by endomorphisms, so that $V_p(A_\ell)$ admits a module structure over $E_p = E \otimes_{\mathbb{Q}} \mathbb{Q}_p$. Since $E \hookrightarrow \operatorname{End}^0_{F_\ell}(A_\ell)$, the endomorphisms on E are defined over F_ℓ, and therefore the action of E commutes with the Galois action, which means that the action of $\mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/F_\ell)$ on $V_p(A_\ell)$ is E_p-linear. This implies that the above representation takes values in $\mathrm{Aut}_{E_p}(V_p(A_\ell))$, i.e.

$$r_{A_\ell,p}:\mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/F_\ell)\longrightarrow \mathrm{Aut}_{E_p}(V_p(A_\ell))\subseteq \mathrm{Aut}(V_p(A_\ell))\simeq \mathrm{GL}_4(\mathbb{Q}_p),$$

where $\mathrm{Aut}_{E_p}(V_p(A_\ell))=\{f\in\mathrm{Aut}(V_p(A_\ell)) : f \text{ commutes with the action of } E_p\}$.

Now let $\mathfrak{p}$ be a prime of E over p, and consider the $\mathfrak{p}$-adic Tate module $V_\mathfrak{p}(A_\ell):=V_p(A_\ell)\otimes_{E_p}E_\mathfrak{p}$. Since $\mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/F_\ell)$ acts E_p-linearly on $V_p(A_\ell)$, it also acts $E_\mathfrak{p}$-linearly on $V_\mathfrak{p}(A_\ell)$. Hence, we obtain a $\mathfrak{p}$-adic representation

$$r_{A_\ell,\mathfrak{p}}:\mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/F_\ell)\longrightarrow \mathrm{Aut}_{E_\mathfrak{p}}(V_\mathfrak{p}(A_\ell))\subseteq \mathrm{Aut}(V_\mathfrak{p}(A_\ell))\simeq \mathrm{GL}_2(E_\mathfrak{p}).$$

We can consider as well the Galois representation on the "integral" Tate modules $T_p(A_\ell)$ and $T_\mathfrak{p}(A_\ell):=T_p(A_\ell)\otimes_{\mathbb{Z}_p}R_{E_\mathfrak{p}}$, which are a free $\mathbb{Z}_p$-module of rank 4 and a free $R_{E_\mathfrak{p}}$-module of rank 2, respectively. These representations will be denoted also by $r_{A_\ell,p}$ and $r_{A_\ell,\mathfrak{p}}$, but it should be clear from the context which representation we are considering in each case. These integral versions of the above representations take values on $\mathrm{GL}_4(\mathbb{Z}_p)$ and $\mathrm{GL}_2(R_{E_\mathfrak{p}})$, respectively.

The above isomorphism $\mathrm{Aut}(V_\mathfrak{p}(A_\ell))\simeq\mathrm{GL}_2(E_\mathfrak{p})$ holds because of the general fact that, if E has degree d over $\mathbb{Q}$, then the dimension of $V_\mathfrak{p}(A_\ell)$ over $E_\mathfrak{p}$ equals $2\dim(A_\ell)/d$. In fact, observe that this dimension does not depend neither on the prime $\mathfrak{p}$ nor on p. This dimension equals also the rank of $V_p(A_\ell)$ as an E_p-module (which is 2 in our case).

Let us assume for a moment that we are in the general case in which $E/\mathbb{Q}$ is an arbitrary degree d extension, and $\mathfrak{p}$ is any prime of E above p. Write $E_\mathfrak{p}$ for the completion of E at $\mathfrak{p}$, which is a field extension of $\mathbb{Q}_p$. Then, the natural inclusions $E\hookrightarrow E_\mathfrak{p}$ induce homomorphisms $E\otimes_\mathbb{Q}\mathbb{Q}_p\to E_\mathfrak{p}$ via $a\otimes b\mapsto ab$, and hence a canonical homomorphism

$$E_p=E\otimes_\mathbb{Q}\mathbb{Q}_p\longrightarrow\prod_{\mathfrak{p}|p}E_\mathfrak{p},$$

where the product is over all the primes above p. Note first that the tensor product is taken in the sense of vector spaces, i.e. the $\mathbb{Q}$-vector space E is lifted to a $\mathbb{Q}_p$-vector space $E_p=E\otimes_\mathbb{Q}\mathbb{Q}_p$. The latter, however, is not a field in general, but rather a $\mathbb{Q}_p$-algebra with the multiplication $(a\otimes b)(a'\otimes b')=aa'\otimes bb'$, and the above homomorphism is then a homomorphism of $\mathbb{Q}_p$-algebras.

It turns out that, being $E/\mathbb{Q}$ a separable extension, this homomorphism induces an isomorphism $E_p=E\otimes_\mathbb{Q}\mathbb{Q}_p\simeq\prod_{\mathfrak{p}|p}E_\mathfrak{p}$ ([**Neu99**, p. 164]). As a consequence, we also have

$$[E:\mathbb{Q}]=\sum_{\mathfrak{p}|p}[E_\mathfrak{p}:\mathbb{Q}_p],\ \mathrm{N}_{E/\mathbb{Q}}(\alpha)=\prod_{\mathfrak{p}|p}\mathrm{N}_{E_\mathfrak{p}/\mathbb{Q}_p}(\alpha),\ \mathrm{Tr}_{E/\mathbb{Q}}(\alpha)=\sum_{\mathfrak{p}|p}\mathrm{Tr}_{E_\mathfrak{p}/\mathbb{Q}_p}(\alpha).$$

Indeed, consider the endomorphism 'multiplication by α' on both sides of the above isomorphism. The characteristic polynomial of α on the $\mathbb{Q}_p$-vector space $E_p=E\otimes_\mathbb{Q}\mathbb{Q}_p$ is the same as that on the $\mathbb{Q}$-vector space E, and therefore

$$\mathrm{charpol}_{E/\mathbb{Q}}(\alpha)=\prod_{\mathfrak{p}|p}\mathrm{charpol}_{E_\mathfrak{p}/\mathbb{Q}_p}(\alpha).$$

Moreover, the decomposition $E_p\simeq\prod_{\mathfrak{p}|p}E_\mathfrak{p}$ gives rise to a decomposition $V_p(A_\ell)\simeq\prod_{\mathfrak{p}|p}V_\mathfrak{p}(A_\ell)$ of the p-adic Tate module of A_ℓ (see [**Rib76**, p. 768]).

Back to our case, $E=\mathbb{Q}(\sqrt{m})$ is quadratic over $\mathbb{Q}$ and p is inert in E, so that $\mathfrak{p}=pR_E$ is the unique prime of E over p. Then, we immediately see that $V_p(A_\ell)\simeq V_\mathfrak{p}(A_\ell)$ (where the isomorphism is as $\mathbb{Q}_p$-vector spaces), and the representations $r_{A_\ell,p}$ and $r_{A_\ell,\mathfrak{p}}$ differ by an isomorphism between the two vector spaces. This observation is crucial for proving the next result:

Lemma 7.1. $\det(r_{A_\ell,\mathfrak{p}})$ *coincides with the restriction of the cyclotomic character* χ_p *to* $\mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/F_\ell)$.

Recall that for a field k and a prime p, the cyclotomic character $\chi_p : \mathrm{Gal}\,(\bar{k}/k) \to \mathbb{Z}_p^\times$ arises from the Galois action on $\varprojlim_n \mu_{p^n}(\bar{k}) \simeq \mathbb{Z}_p$, where $\mu_{p^n}(\bar{k}) \simeq \mathbb{Z}/p^n\mathbb{Z}$ is the group of roots of unity of order p^n, for $n \geq 1$. More precisely, for each integer n define $\zeta_n = e^{2\pi i/p^n}$, which is a primitive p^n-th root of unity. Then, for each $\sigma \in \mathrm{Gal}\,(\bar{k}/k)$ we have that $\sigma(\zeta_n) = \zeta_n^{a_{n,\sigma}}$ for some $a_{n,\sigma} \in (\mathbb{Z}/p^n\mathbb{Z})^\times$. For a fixed σ, if we let n vary then $(a_{n,\sigma})_n$ gives an element in $\mathbb{Z}_p^\times$, which by definition is $\chi_p(\sigma)$.

Proof of Lemma 7.1. By the above observation, it suffices to show that $\det(r_{A_\ell,p}) = \chi_p$. Ribet proved in [**Rib76**, §4] that if A is an abelian variety over a number field K such that $\mathrm{End}_K(A) \otimes \mathbb{Q}$ is a totally real number field of degree equal to $\dim(A)$ and that all the endomorphisms of A are defined over K, then $\det(r_{A,p}) = \chi_p$, where now $\chi_p : \mathrm{Gal}\,(\bar{K}/K) \to \mathbb{Z}_p^\times$.

However, this result comes back to the work of W. Casselman in [**Cas71**], in which a more general context is considered. According to [**Cas71**, §5], if A is an abelian variety over a field k (not necessarily a number field), together with a k-polarization λ, and E is a totally real number field of degree equal to $\dim(A)$ such that

(a) there exists a ring monomorphism $\eta : E \hookrightarrow \mathrm{End}_k^0(A)$, and
(b) $E_p^\lambda(\eta(a)x, y) = E_p^\lambda(x, \eta(a)y)$ for all $x, y \in V_p(A)$ and all $a \in E_p := E \otimes_{\mathbb{Q}} \mathbb{Q}_p$, where $E_p^\lambda : V_p(A) \times V_p(A) \to V_p(1)$ is the Weil pairing associated to λ,

then $\det(r_{A,p}) = \chi_p : \mathrm{Gal}\,(\bar{k}/k) \to \mathbb{Z}_p^\times$.

In our case, $E = \mathbb{Q}(\sqrt{m})$ is a degree 2 totally real number field embedded in the endomorphism algebra $\mathrm{End}_{F_\ell}^0(A_\ell)$ of the polarized abelian surface A_ℓ defined over F_ℓ, so that condition (a) holds. As for condition (b), it follows from the fact that the Rosati involution attached to a F_ℓ-polarization of A_ℓ is the identity on E, as is shown in [**ST61**, p. 41]. Therefore, Casselman's work implies that $\det(r_{A_\ell,p}) = \chi_p$, where we regard the cyclotomic character as $\chi_p : \mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/F_\ell) \to \mathbb{Z}_p^\times$. Hence, the lemma is proved. □

As we have said before, the prime p is inert in E. Therefore, the residue field of $\mathfrak{p} = pR_E$ is isomorphic to $\mathbb{F}_{p^2}$. As a consequence, by reducing the representation $r_{A_\ell,\mathfrak{p}}$ mod $\mathfrak{p}$ we obtain a representation

$$\varrho_{A_\ell,\mathfrak{p}} : \mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/F_\ell) \longrightarrow \mathrm{GL}_2(\mathbb{F}_{p^2}),$$

which is the Galois representation arising from the Galois action on the $\mathfrak{p}$-torsion subgroup $A_\ell[\mathfrak{p}] = \{x \in A_\ell : \beta \cdot x = 0\ \forall \beta \in \mathfrak{p}\} = T_\mathfrak{p}(A_\ell)/\mathfrak{p} \cdot T_\mathfrak{p}(A_\ell)$ of A_ℓ.

Now, by Theorem 1.17, the local quaternion algebra B_p can be written as $B_p = E_\mathfrak{p} + E_\mathfrak{p}\pi$, 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, with this description $\mathcal{O}_p = R_{E,\mathfrak{p}} + R_{E,\mathfrak{p}}\pi$. Recall also the two-sided ideal $I(p) = \{\beta \in \mathcal{O} : p | \mathrm{n}(\beta)\}$ of $\mathcal{O}$, which locally at p is $I(p)_p = \mathfrak{p}R_{E,\mathfrak{p}} + R_{E,\mathfrak{p}}\pi$, whereas $I(p)_q = \mathcal{O}_q$ at the rational primes $q \neq p$. Then the canonical torsion subgroup of A_ℓ at the prime p is $C_p = \ker(I(p) : A_\ell \to A_\ell) = \bigcap_{\beta \in I(p)} \ker(\beta : A_\ell \to A_\ell)$, which now we regard as a subgroup of $A_\ell[\mathfrak{p}]$.

The action of B on $A_\ell(\bar{F}_\ell)$ makes $V_\mathfrak{p}(A_\ell)$ into a B_p-module, which must be free because B_p is simple. In fact, we have $V_\mathfrak{p}(A_\ell) \simeq B_p$, since $\dim_{\mathbb{Q}_p}(B_p) = \dim_{\mathbb{Q}_p}(V_\mathfrak{p}(A_\ell)) = 4$. In the same way, $T_\mathfrak{p}(A_\ell)$ is naturally a module over $\mathcal{O}_p$. In fact, choosing an isomorphism $V_\mathfrak{p}(A_\ell) \simeq B_p$ we can identify $T_\mathfrak{p}(A_\ell)$ as a left ideal of $\mathcal{O}_p$. Since $\mathcal{O}_p$ is maximal, it follows from [**Vig80**, p. 34] that it is a principal ideal, so we may write $T_\mathfrak{p}(A_\ell) = \mathcal{O}_p \cdot x$ for some $x \in A_\ell[\mathfrak{p}]$. But now note that

$$A[\mathfrak{p}] = T_\mathfrak{p}(A_\ell)/\mathfrak{p} \cdot T_\mathfrak{p}(A_\ell) \simeq \mathcal{O}_p/\mathfrak{p}\mathcal{O}_p,$$

and also

$$C_p = \mathcal{O}_p/I(p)_\mathfrak{p} \simeq R_{E,\mathfrak{p}}/\mathfrak{p}R_{E,\mathfrak{p}} \simeq \mathbb{F}_{p^2}.$$

Therefore, as a R_E-module, $\mathrm{Aut}_{R_E}(C) \simeq \mathbb{F}_{p^2}^\times$.

Finally, since $I(p)$ is the unique two-sided $\mathcal{O}$-ideal of reduced norm p, the action of $\mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/F_\ell)$ leaves $I(p)$ invariant. Since $R_E \subseteq \mathrm{End}_{F_\ell}(A_\ell)$, $\mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/F_\ell)$ acts R_E-linearly on C, and therefore it induces a Galois representation

$$\alpha_{A_\ell,\mathfrak{p}} : \mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/F_\ell) \longrightarrow \mathrm{Aut}_{R_E}(C) \simeq \mathbb{F}_{p^2}^\times.$$

As in the case of the canonical isogeny character introduced by Jordan, and appearing also in the work of Skorobogatov, both representations $\varrho_{A_\ell,\mathfrak{p}}$ and $\alpha_{A_\ell,\mathfrak{p}}$ play an important role in the following sections.

2. Galois characters induced by the $X_B^{(m)}$-torsor $Y_{B,p}^{(m)}$

As in the previous section, consider an abelian surface (A_ℓ, i_ℓ) with real multiplication by the ring of integers R_E of $E = \mathbb{Q}(\sqrt{m})$ corresponding to a point $Q_\ell \in X_B^{(m)}(\mathbb{Q}_\ell)$. However, now we focus our attention on the $\mathbb{Q}_\ell$-rational point Q_ℓ on the Atkin-Lehner quotient $X_B^{(m)}$. To this point, by means of a suitable $X_B^{(m)}$-torsor, we attach a Galois character which is closely related to the Galois representation $\alpha_{A_\ell,\mathfrak{p}}$. For the abelian surface (A_ℓ, i_ℓ), the fields F_ℓ and K_ℓ have the same meaning as in the previous section.

Recall from Chapter 5 that we have constructed a cyclic étale covering $Z_{B,p}^{(m)} \to X_B^{(m)}$ attached to the prime p. More precisely, we have a commutative diagram

$$\begin{tikzcd}
Z_{B,p} \arrow[dr, "\text{ét}"] \arrow[dd] & \\
& X_B \arrow[dd] \\
Z_{B,p}^{(m)} \arrow[dr, "\text{ét}"] & \\
& X_B^{(m)},
\end{tikzcd}$$

where the diagonal arrows are (unconditionally) étale, and the vertical arrows are the natural projection maps $\pi_m : X_B \to X_B^{(m)}$ and $\hat{\pi}_m : Z_{B,p} \to Z_{B,p}^{(m)}$ associated to the Atkin-Lehner involution ω_m and its lifted $\hat{\omega}_m$, respectively. Indeed, recall that $Z_{B,p} \to X_B$ is the maximal étale subcovering of the cyclic Galois covering $X_{B,p} \to X_B$ introduced by Jordan. The latter has automorphism group isomorphic to $\mathbb{Z}/\frac{p^2-1}{2}\mathbb{Z}$, while the former is the quotient of $X_{B,p} \to X_B$ by a subgroup of $\mathbb{Z}/6\mathbb{Z}$.

On the bottom we have an analogous picture. The cyclic covering $Z_{B,p}^{(m)} \to X_B^{(m)}$ is the quotient of the Galois covering $X_{B,p}^{(m)} \to X_B^{(m)}$ attached to p by a subgroup of $\mathbb{Z}/6\mathbb{Z}$, and it is its maximal étale subcovering. Since the automorphism group of the covering $X_{B,p}^{(m)} \to X_B^{(m)}$ is also isomorphic to the cyclic group $\mathbb{Z}/\frac{p^2-1}{2}\mathbb{Z}$ we can use again the idea of Skorobogatov. Assume from now on that $p \geq 5$, so that 6 divides $(p^2-1)/2$. Then, we define

$$f_p : Y_{B,p}^{(m)} \to X_B^{(m)}$$

to be the quotient of $X_{B,p}^{(m)} \to X_B^{(m)}$ by $\mathbb{Z}/6\mathbb{Z}$. Then, by construction $f_p : Y_{B,p}^{(m)} \to X_B^{(m)}$ is a subcovering of $Z_{B,p}^{(m)} \to X_B^{(m)}$, hence it is étale. Moreover, this leads directly to:

Lemma 7.2. *$f_p : Y_{B,p}^{(m)} \to X_B^{(m)}$ is an $X_B^{(m)}$-torsor under the constant group scheme $\mathbb{F}_{p^2}^{\times 12} \simeq \mathbb{Z}/\frac{p^2-1}{12}\mathbb{Z}$.*

Now let k be a field of characteristic zero. As explained in Chapter 3, by specialization the torsor $f_p : Y_{B,p}^{(m)} \to X_B^{(m)}$ associates to each point $Q \in X_B^{(m)}(k)$ a continuous character

$\phi_Q \in \mathrm{Hom}(\mathrm{Gal}\,(\bar{k}/k), \mathbb{F}_{p^2}^{\times 12})$ by which the Galois group acts on the fibre of $Y_{B,p}^{(m)} \to X_B^{(m)}$ at Q. In particular, for the $\mathbb{Q}_\ell$-rational point $Q_\ell \in X_B^{(m)}(\mathbb{Q}_\ell)$ we obtain a Galois character

$$\phi_\ell := \phi_{Q_\ell} : \mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell) \longrightarrow \mathbb{F}_{p^2}^{\times 12}.$$

From the definitions and the moduli interpretation of the covering $X_{B,p}^{(m)} \to X_B^{(m)}$, it follows that this Galois character is closely related to the Galois representation $\alpha_{A_\ell,\mathfrak{p}}$. More precisely:

Lemma 7.3. *With the above notations, if (A_ℓ, i_ℓ) is an abelian surface corresponding to the point Q_ℓ, then $\phi_{\ell|\,\mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/F_\ell)} = \alpha_{A_\ell,\mathfrak{p}}^{12}$.*

This relation allows us to deduce some properties of the character ϕ_ℓ by studying the representation $\alpha_{A_\ell,\mathfrak{p}}$. For example:

Proposition 7.4. *With notations as before and for $\ell \neq p$,*

(a) *if $F_\ell = K_\ell$, then $\alpha_{A_\ell,\mathfrak{p}}^{12}$ is unramified;*
(b) *if $F_\ell = \mathbb{Q}_\ell$, then $\alpha_{A_\ell,\mathfrak{p}}^{24}$ is unramified.*

PROOF. This result is similar to Proposition 2.2 in [**Sko05**], which is proved by the methods explained in [**Jor86**, §3]. In our case, both statements (a) and (b) can also be deduced from these methods:

(a) Assume $F_\ell = K_\ell$, and let $\mathfrak{l}$ be the prime in F_ℓ above ℓ, which corresponds to the unique extension to F_ℓ of the ℓ-adic valuation in $\mathbb{Q}_\ell$. Write $\alpha_{A_\ell,\mathfrak{p}} : \mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/F_\ell) \to \mathbb{F}_{p^2}^\times$. We want to prove that $\alpha_{A_\ell,\mathfrak{p}}^{12}(I_\mathfrak{l}) = \{1\}$, where $I_\mathfrak{l} \subseteq \mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/F_\ell)$ is the inertia subgroup.

Consider first the integral Galois representation

$$r_{A_\ell,p} : \mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/F_\ell) \longrightarrow \mathrm{Aut}(T_p(A)) \simeq \mathrm{GL}_4(\mathbb{Z}_p),$$

arising from the Galois action on the Tate-module, and assume that we know $r_{A_\ell,p}^{12}(I_\mathfrak{l}) = \{1\}$. Since the endomorphisms of A_ℓ in E are defined over F_ℓ, the induced representation $r_{A_\ell,\mathfrak{p}} : \mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/F_\ell) \to \mathrm{GL}_2(R_{E_\mathfrak{p}})$ can be regarded as a subrepresentation of $r_{A_\ell,p}$. It follows that also $r_{A_\ell,\mathfrak{p}}^{12}(I_\mathfrak{l}) = \{1\}$. This means that $I_\mathfrak{l}^{12}$ acts trivially on $A[\mathfrak{p}]$, so that it also acts trivially on $C \subseteq A[\mathfrak{p}]$ as well. Hence, $\alpha_{A_\ell,\mathfrak{p}}^{12}(I_\mathfrak{l}) = \{1\}$.

That is, in order to prove the statement it is enough to show that $r_{A_\ell,p}^{12}(I_\mathfrak{l}) = \{1\}$ holds. But under our hypotheses, this follows from the study of abelian surfaces admitting quaternionic multiplication over local fields found in [**Jor86**, §3].

(b) Now suppose $F_\ell = \mathbb{Q}_\ell$, which corresponds to case ii) above. The goal now is to prove that $\alpha_{A_\ell,\mathfrak{p}}^{24}(I_\ell) = \{1\}$, where $I_\ell \subseteq \mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$ is the inertia subgroup.

Now we cannot appeal directly to [**Jor86**, §3], because our abelian surface A_ℓ is defined over $\mathbb{Q}_\ell$ but $B \not\subseteq \mathrm{End}_{\mathbb{Q}_\ell}^0(A_\ell)$, we can only ensure that $B \hookrightarrow \mathrm{End}_{K_\ell}^0(A_\ell)$, with K_ℓ quadratic over $\mathbb{Q}_\ell$.

In view of this, define $\mathfrak{l}$ to be the prime of K_ℓ above ℓ, which corresponds to the unique extension to K_ℓ of the ℓ-adic valuation in $\mathbb{Q}_\ell$. If $I_\mathfrak{l} \subseteq \mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/K_\ell)$ is the corresponding inertia subgroup, since $B \hookrightarrow \mathrm{End}_{K_\ell}^0(A_\ell)$, considering A_ℓ as being defined over K_ℓ, the results from [**Jor86**, §3] apply to deduce as in the previous case that $\alpha_{A_\ell,\mathfrak{p}|\,\mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/K_\ell)}^{12}(I_\mathfrak{l}) = \{1\}$. Since $[K_\ell : \mathbb{Q}_\ell] = 2$, we have $[I_\ell : I_\mathfrak{l}] \leq 2$, and this leads to $\alpha_{A_\ell,\mathfrak{p}}^{24}(I_\ell) = \{1\}$, so the lemma is proved.

□

By using Lemma 7.3, the above proposition can be translated directly in terms of the Galois character ϕ_ℓ:

Corollary 7.5. *For each $\ell \neq p$, ϕ_ℓ^2 is unramified.*

Proof. We split the proof in two cases, in order to apply the previous lemma.

(a) Suppose $F_\ell = K_\ell$, a quadratic extension of $\mathbb{Q}_\ell$. Then the restriction
$$\phi_{\ell|\,\mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/F_\ell)} : \mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/F_\ell) \to \mathbb{F}_{p^2}^{\times 12}$$
equals $\alpha^{12}_{A_\ell,\mathfrak{p}} : \mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/F_\ell) \to \mathbb{F}_{p^2}^{\times 12}$, which is unramified by the first part of the previous lemma. Since $[F_\ell : \mathbb{Q}_\ell] = 2$, it follows that $\phi_\ell^2 : \mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell) \to \mathbb{F}_{p^2}^{\times 24}$ is unramified.

(b) Now assume $F_\ell = \mathbb{Q}_\ell$. Then we have an equality of characters $\phi_\ell = \alpha^{12}_{A_\ell,\mathfrak{p}} : \mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell) \to \mathbb{F}_{p^2}^{\times 12}$, without restricting ϕ_ℓ. Therefore, $\phi_\ell^2 = \alpha^{24}_{A_\ell,\mathfrak{p}}$, which is unramified by the second part of the lemma.

□

3. When the field of definition is $\mathbb{Q}_\ell$

Now we make a closer analysis when the abelian surface (A_ℓ, i_ℓ) corresponding to the point $Q_\ell \in X_B^{(m)}(\mathbb{Q}_\ell)$ admits a model rational over $\mathbb{Q}_\ell$, so throughout this section we assume this condition holds[1]. With the previous notations, this means $F_\ell = \mathbb{Q}_\ell$. Then we have an equality of characters $\phi_\ell = \alpha^{12}_{A_\ell,\mathfrak{p}}$, without restricting ϕ_ℓ to an index 2 subgroup.

Also the representations $r_{A_\ell,\mathfrak{p}}$ and $\varrho_{A_\ell,\mathfrak{p}}$ have source $\mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$ and, in this situation, we can relate $\alpha_{A_\ell,\mathfrak{p}}$ to $\varrho_{A_\ell,\mathfrak{p}}$ as we now explain. First of all, consider the action of $\mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$ on the ring of endomorphisms $\mathcal{O} \subseteq \mathrm{End}_{\bar{\mathbb{Q}}_\ell}(A_\ell)$ of $A_\ell \times \bar{\mathbb{Q}}_\ell$. By the Noether-Skolem Theorem, for any $\sigma \in \mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$ the automorphism $B \to B$, $\beta \mapsto \beta^\sigma$, is inner. That is, there exists $\gamma_\sigma \in \mathcal{O}$ such that $\beta^\sigma = \gamma_\sigma \beta \gamma_\sigma^{-1}$ for all $\beta \in B$. Since $\beta^\sigma \in \mathcal{O}$ for all $\beta \in \mathcal{O}$, we have $\gamma_\sigma \in \mathrm{Norm}_B(\mathcal{O})$. Moreover, since the endomorphisms of $R_E \subset E$ are defined over $\mathbb{Q}_\ell$, γ_σ lies in the commutator of E in B, which is E itself because it is a maximal subfield of B. Therefore, $\gamma_\sigma \in E \cap \mathcal{O}$, and we obtain a character
$$\psi : \mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell) \to E^\times/\mathbb{Q}^\times,\ \sigma \mapsto \gamma_\sigma.$$

Indeed, as all the endomorphisms of A_ℓ lying in B are defined over K_ℓ, we can think ψ having source $\mathrm{Gal}\,(K_\ell/\mathbb{Q}_\ell)$. Hence, ψ is a quadratic character.

Lemma 7.6. *There exists an $\mathbb{F}_{p^2}$-basis of $A_\ell[\mathfrak{p}]$ with respect to which*
$$\begin{array}{cccc} \varrho_{A_\ell,\mathfrak{p}} : & \mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell) & \longrightarrow & \mathrm{GL}_2(\mathbb{F}_{p^2}) \\ & \sigma & \longmapsto & \begin{pmatrix} \psi(\sigma)\alpha_{A_\ell,\mathfrak{p}}(\sigma)^p & 0 \\ \beta_\sigma & \alpha_{A_\ell,\mathfrak{p}}(\sigma) \end{pmatrix} \end{array}$$
for some $\beta_\sigma \in \mathbb{F}_{p^2}$.

Proof. The proof of [**Rot08**, Lemma 3.1] can be rewritten without trouble for this case. □

According to Lemma 2.1 in [**Rot08**], we can choose a finite extension $L_\ell/\mathbb{Q}_\ell$ such that ℓ ramifies completely in L_ℓ and the closed fibre of the Néron model of $A_\ell \times L_\ell$ over the ring of integers of L_ℓ is an abelian surface $\tilde{A}_\ell$ over $\mathbb{F}_\ell$. That is, we can fix a finite extension of $\mathbb{Q}_\ell$ over which A_ℓ acquires good reduction having residue field $\mathbb{F}_\ell$. Choose also an element $\sigma_\ell \in \mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/L_\ell)$ inducing the Frobenius automorphism $\mathrm{Fr}_\ell \in \mathrm{Gal}\,(\bar{\mathbb{F}}_\ell/\mathbb{F}_\ell)$ under reduction.

Then we consider the characteristic polynomial of $r_{A_\ell,\mathfrak{p}}(\sigma_\ell)$, which is a quadratic polynomial $\Phi_\ell(T) := \Phi_{\sigma_\ell}(T) \in R_{E_\mathfrak{p}}[T]$. By Lemma 7.1, we have $\det(r_{A_\ell,\mathfrak{p}}(\sigma_\ell)) = \ell$, but using the above lemma we can give an expression for the reduction of $\Phi_\ell(T)$ modulo $\mathfrak{p}$:

[1] More generally, if we assume that the pair (B, m) satisfies condition (M) with respect to the prime ℓ, then the hypothesis holds for any choice of $Q_\ell \in X_B^{(m)}(\mathbb{Q}_\ell)$.

Proposition 7.7. *If $\ell \neq p$, the characteristic polynomial Φ_ℓ of $r_{A_\ell,\mathfrak{p}}(\sigma_\ell)$ satisfies the congruence*

$$\Phi_\ell(T) \equiv T^2 - (\alpha_{A_{\ell,\mathfrak{p}}}(\sigma_\ell) + \ell\alpha_{A_{\ell,\mathfrak{p}}}(\sigma_\ell^{-1}))T + \ell \in \mathbb{F}_{p^2}[T].$$

Proof. From Lemma 7.6, the characteristic polynomial $\Phi_\ell(T) \in R_{E_\mathfrak{p}}[T]$ satisfies the congruence

$$\Phi_\ell(T) \mod \mathfrak{p} \equiv T^2 - (\alpha_{A_\ell,\mathfrak{p}}(\sigma_\ell) + \psi(\sigma_\ell)\alpha_{A_\ell,\mathfrak{p}}(\sigma_\ell)^p)T + \psi(\sigma_\ell)N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\alpha_{A_\ell,\mathfrak{p}}(\sigma_\ell)).$$

Since $\ell \neq p$ and $\det(r_{A_\ell,\mathfrak{p}}(\sigma_\ell)) = \ell$, we can write

$$\psi(\sigma_\ell)\alpha_{A_\ell,\mathfrak{p}}(\sigma_\ell)^p\alpha_{A_\ell,\mathfrak{p}}(\sigma_\ell) = \ell \in \mathbb{F}_{p^2},$$

and therefore

$$\alpha_{A_\ell,\mathfrak{p}}(\sigma_\ell) + \psi(\sigma_\ell)\alpha_{A_\ell,\mathfrak{p}}(\sigma_\ell)^p \equiv \alpha_{A_\ell,\mathfrak{p}}(\sigma_\ell) + \ell\alpha_{A_\ell,\mathfrak{p}}(\sigma_\ell^{-1}) \mod \mathfrak{p}.$$

Summing up, we obtain the claimed congruence. □

4. Global considerations

Before proving a first approach to our main result announced at the end of Chapter 5, we make some considerations for the case of "global" rational points on $X_B^{(m)}$. For this section, we do not need to assume that ω_m is a twisting involution. So, just for this section, note that ω_m is allowed to be *any* Atkin-Lehner involution on our Shimura curve X_B.

Let $Q \in X_B^{(m)}(\mathbb{Q})$, and let $K/\mathbb{Q}$ be an imaginary quadratic extension over which its preimages by π_m lie. That is, $\pi_m^{-1}(Q) = \{P, \omega_m(P)\} \subseteq X_B(K)$. We also let (A,ι) an abelian surface with quaternionic multiplication by B representing either P or $\omega_m(P)$.

Understanding the field K is of great importance, and this fact appears reflected on the definition of the set of algebras $\mathcal{B}_{p,m}(q)$ introduced before the statement of Theorem 5.10. The aim of this section is to prove the following:

Proposition 7.8. *If there exists a prime $p|D$, $p \nmid m$, $p \equiv 3 \mod 4$, then K is unramified away from D.*

First recall the following criterion describing when ω_m is fixed point free, which is a direct consequence of Ogg's formula for the number of fixed points of an Atkin-Lehner involution on X_B:

Lemma 7.9. *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.*

Proof. By the criterion of Hasse, we know that $\mathbb{Q}(\sqrt{-m})$ embeds in B if and only if every prime $p|D$ does not split in $\mathbb{Q}(\sqrt{-m})$. Equivalently, $\mathbb{Q}(\sqrt{-m})$ does not embed in B if and only if $(\frac{-m}{p}) = 1$ for some prime $p|D$. By the formula for the number of fixed points of an Atkin-Lehner involution due to Ogg ([**Ogg83**]), this last condition is equivalent to ω_m having no fixed points. □

Now, we use descent to prove the following:

Lemma 7.10. *If $\mathbb{Q}(\sqrt{-m})$ does not embed in B, then K is unramified away from D.*

Proof. By the above lemma, ω_m is fixed point free. Therefore, $\pi_m : X_B \to X_B^{(m)}$ is unramified, so it is an $X_B^{(m)}$-torsor under the constant group scheme $\mathbb{Z}/2\mathbb{Z}$. By the work of Morita on integral models of X_B (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.

As it is well-known, the $\mathbb{Q}$-rational points of $X_B^{(m)}$ can be recovered from the $\mathbb{Q}$-rational points on the twisted torsors of $\pi_m : X_B \to X_B^{(m)}$. More precisely,

$$X_B^{(m)}(\mathbb{Q}) = \bigcup_{\tau \in H^1(\mathbb{Q},\{\pm 1\})} {}^{\tau}X_B(\mathbb{Q}),$$

where ${}^{\tau}X_B(\mathbb{Q})$ stands for ${}^{\tau}\pi_m({}^{\tau}X_B(\mathbb{Q}))$. Here the cohomology classes $\tau \in H^1(\mathbb{Q},\{\pm 1\})$ must be regarded as Galois quadratic characters $\tau : \mathrm{Gal}\,(\bar{\mathbb{Q}}/\mathbb{Q}) \to \{\pm 1\}$, hence they are in correspondence with quadratic extensions. Since X_B has no real points, we can restrict 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 ${}^{\tau_L}X_B(\mathbb{Q}) = \emptyset$, 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 $X_B^{(m)}(\mathbb{Q})$.

In particular, since $P \in X_B(K)$ and $\pi_m(P) = Q \in X_B^{(m)}(\mathbb{Q})$, the class $\zeta(Q) \in \mathrm{H}^1(\mathbb{Q},\{\pm 1\})$ of the $\mathbb{Q}$-torsor given by the fibre $X_{B,Q} \to Q$ is the quadratic character τ_K corresponding to the quadratic extension $K/\mathbb{Q}$. Hence, the point Q comes from a $\mathbb{Q}$-rational point on the twisted curve ${}^{\tau_K}X_B$. By the above discussion, K must be unramified away from D. □

Finally we show how to use these lemmas to prove the proposition:

Proof of Proposition 7.8. By the second lemma, it suffices to show that $\mathbb{Q}(\sqrt{-m})$ does not embed in B. The hypotheses directly imply that the prime p is inert in $\mathbb{Q}(\sqrt{m})$. That is, $(\frac{m}{p}) = -1$. Therefore,

$$(\frac{-m}{p}) = (\frac{-1}{p})(\frac{m}{p}) = 1,$$

which implies that $\mathbb{Q}(\sqrt{-m})$ does not embed in B, and the statement follows. □

Indeed, Proposition 7.8 is the case $F = \mathbb{Q}$ of [**Rot08**, Proposition 1.3], which states an answer to the question of how does K depend on the pair $(\mathcal{O}, R_{\mathbb{Q}(\sqrt{m})})$.

Moreover, Proposition 7.8 together with the material in [**Rot08**] allows us to prove the non-existence of rational points on Atkin-Lehner quotients of Shimura curves in some particular cases (see Theorem 7.13 below). We need a previous lemma and a definition.

First, the lemma goes in the same direction as some comments at the end of Chapter 6 for the local case:

Lemma 7.11. *With the above notations, the hypothesis* $2 \nmid D$ *implies that the abelian surface* (A, ι) *admits a model rational over* K*.*

Proof. See [**Jor86**, p. 93]. □

And second, let us define a finite set of primes for a given prime q:

Definition 7.12. *For a given prime* q*, we define* $P_0(q)$ *to be the set of prime factors of the non-zero integers in the set* $\cup_{s,a}\{q, a^2 - sq\}$*, where the union is over* $s = 0, 1, 2, 3, 4$ *and the integers* a *such that* $|a| \leq 2\sqrt{q}$*.*

This is obviously a finite set of prime ideals, rather small for small values of q. We have for instance $P_0(2) = \{2, 3, 5, 7\}$ and $P_0(3) = \{2, 3, 5, 11\}$.

Theorem 7.13. *Let* p, m *be two different primes,* $m \equiv p \equiv 3 \bmod 4$*,* $(\frac{m}{p}) = -1$*,* $p \neq 3, 7, 11, 19, 23, 43, 67, 163$*. If there exists an odd prime* q *such that* $p \notin P_0(q)$*,* $(\frac{q}{p}) = 1$ *and* $(\frac{q}{m}) = -1$*, then* $X_{pm}^{(m)}(\mathbb{Q}) = \emptyset$*, where* X_{pm} *is the Shimura curve associated to the quaternion algebra* $B(pm)$ *of reduced discriminant* pm*.*

Proof. The fact that $p \neq 3, 7, 11, 19, 23, 43, 67, 163$ implies by [**BFGR06**, Proposition 5.1] that there exist no CM-points in $X_{pm}^{(m)}(\mathbb{Q})$.

So, suppose 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 Proposition 7.8, K is unramified at the primes not dividing pm. Hence the only possibilities are $\mathbb{Q}(\sqrt{-p})$, $\mathbb{Q}(\sqrt{-m})$, $\mathbb{Q}(\sqrt{-pm})$.

The last option is excluded because it 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 $\mathbb{Q}_p$. 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 $B \simeq (\frac{-p,m}{\mathbb{Q}})$ (easy computation of Hilbert symbols). Therefore, by the above lemma and [**BFGR06**, Theorem 4.5] the point Q corresponds, in the terminology of [**Rot08**], to a *modular triplet* $(\mathcal{O}_{pm}, R_{\mathbb{Q}(\sqrt{m})}, \mathbb{Q}(\sqrt{-p}))$. By applying [**Rot08**, Theorem 1.4], we deduce $(\frac{-q}{m}) = -1$, but our assumptions imply

$$(\frac{-q}{m}) = (\frac{-1}{m})(\frac{q}{m}) = 1,$$

and thus we get a contradiction. Therefore, $X_{pm}^{(m)}(\mathbb{Q}) = \emptyset$. □

This result is significant progress with respect to [**RSY05**, Theorem 5.1] and [**RSY05**, Corollary 5.2]. Fixed a prime q, Theorem 7.13 says that $X_{pm}^{(m)}(\mathbb{Q}) = \emptyset$ whenever m and p are different primes such that $p \notin P_0(q)$, $p \neq 3$, 7, 11, 19, 23, 43, 67, 163, $m \equiv p \equiv 3 \bmod 4$, $(\frac{m}{p}) = -1$, $(\frac{q}{p}) = 1$ and $(\frac{q}{m}) = -1$. By Čebotarev Density Theorem, there exist infinitely many such m and p.

Moreover, [**RSY05**, Theorem 3.1] gives a criterion for $X_{pm}^{(m)}(\mathbb{A}_{\mathbb{Q}})$ being non-empty. Whenever this holds, the Atkin-Lehner quotient $X_{pm}^{(m)}$ is then a counterexample to the Hasse principle over $\mathbb{Q}$.

Example 7.14. For instance, if we take $q = 3$ then $P_0(3) = \{2, 3, 5, 11\}$, and for $q = 5$ we have $P_0(5) = \{2, 3, 5, 7, 11, 19\}$. Then, computing pairs of primes (p, m) satisfying the hypotheses of the theorem (for $q = 3$ or 5) we find, for example, that

$$X_{31\cdot 3}^{(3)}(\mathbb{Q}) = X_{71\cdot 7}^{(7)}(\mathbb{Q}) = X_{31\cdot 23}^{(23)}(\mathbb{Q}) = X_{47\cdot 19}^{(19)}(\mathbb{Q}) = \emptyset.$$

Remark 7.15. Note that Theorem 7.13 does not require the Atkin-Lehner involution ω_m to be twisting. Indeed, if $B(pm)$ denotes the rational quaternion algebra of reduced discriminant pm, with p and m as in Theorem 7.13, 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 (see Lemma 2.21).

As a consequence, Theorem 7.13 (obtained by "global" methods) does not go in the same direction as our Main Theorem (see Theorem 7.31 below), which deals with quotients of Shimura curves by *twisting* Atkin-Lehner involutions. So, the above examples will not be covered by Theorem 7.31.

5. A first approach to the main theorem

Recall that asking for the pair (B, m) to satisfy condition (M) with respect to a prime ℓ is equivalent to assume that every abelian surface (A_ℓ, i_ℓ) parametrized by a point in $X_B^{(m)}(\mathbb{Q}_\ell)_{nh}$ admits a model rational over $\mathbb{Q}_\ell$ (see Corollary 6.11). Indeed, when this condition holds *every* abelian surface parametrized by a point in $X_B^{(m)}(\mathbb{Q}_\ell)$ admits a model rational over $\mathbb{Q}_\ell$. Assuming this condition for two *well-chosen* primes, we are already able to prove a first approach to our main theorem.

As in [**Rot08**], and motivated from [**Sko05**], we need to define a finite set of *exceptional primes* with respect to a fixed prime q, which contains the set $P_0(q)$ defined above:

Definition 7.16. *For a rational prime q, let $P(q)$ be the set of prime factors of the non-zero integers in the set $\cup_{s,a}\{q, a^2 - sq, a^4 - 4a^2q + q^2\}$, where the union is over $s = 0, 1, 2, 3, 4$ and the integers a such that $|a| \leq 2\sqrt{q}$.*

In Theorem 7.19 below, we will perform descent on the torsor $f_p : Y_{B,p}^{(m)} \to X_B^{(m)}$. Following the notations of the previous sections, if ℓ is any rational prime, for a point $Q_\ell \in X_B^{(m)}(\mathbb{Q}_\ell)$ we denote by $\phi_\ell : \mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell) \to \mathbb{F}_{p^2}^{\times 12}$ the Galois character obtained by specialization of f_p at Q_ℓ. Then, recall that $X_B^{(m)}(\mathbb{Q})$ is a subset of the descent set relative to f_p, which is

$$X_B^{(m)}(\mathbb{A}_\mathbb{Q})^{f_p} = \left\{ \{Q_\ell\}_\ell \in X_B^{(m)}(\mathbb{A}_\mathbb{Q}) \;\middle|\; \begin{array}{l} \text{there exists a global character} \\ \phi : \mathrm{Gal}\,(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_{p^2}^{\times 12} \text{ such} \\ \text{that } \phi_{|\,\mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)} = \phi_\ell \text{ for all } \ell \end{array} \right\}.$$

For the next definition, if q is a prime let us denote by $\mathbb{Q}_{q^2}$ the unique unramified quadratic extension of $\mathbb{Q}_q$. For any $e \in \mathbb{Z}_q^\times \setminus \mathbb{Z}_q^{\times 2}$, $\mathbb{Q}_{q^2} = \mathbb{Q}_q(\sqrt{e})$.

Definition 7.17. *Let $p \geq 5$ be a prime and $m > 1$ a squarefree positive integer not divisible by p. Denote by $\mathcal{Q}(pm)$ the set of rational indefinite quaternion algebras whose reduced discriminant is divisible by pm. For a prime q, we define the following subsets of $\mathcal{Q}(pm)$:*

$$\mathcal{B}_{p,m}(q) = \left\{ B \in \mathcal{Q}(pm) \;\middle|\; \begin{array}{l} \mathbb{Q}(\sqrt{-q}) \textit{ does not split } B \textit{ and } q \textit{ is not inert in any} \\ \textit{imaginary quadratic field } K \textit{ such that } K \textit{ is} \\ \textit{unramified away from } \mathrm{disc}(B) \end{array} \right\},$$

$$\mathcal{B}_{p,m}^{\mathrm{Br}}(q) = \left\{ B \in \mathcal{Q}(pm) \;\middle|\; \begin{array}{l} \mathbb{Q}(\sqrt{-q}) \textit{ does not split } B \textit{ and for every} \\ \textit{sequence } \{Q_\ell\}_\ell \in X_B^{(m)}(\mathbb{A}_\mathbb{Q})^{f_p} \textit{ one has} \\ \pi_m^{-1}(Q_q) \nsubseteq X_B(\mathbb{Q}_{q^2}) \end{array} \right\}.$$

Remark 7.18. In the theorem below, as well as later in our main result in Theorem 7.31 we need to restrict to these families of rational quaternion algebras, so let us make some remarks about these restrictions.

First suppose that $B \in \mathcal{Q}(pm)$ and let q be a prime such that $\mathbb{Q}(\sqrt{-q})$ does not split B, a condition which is easy to check. In order to check whether B is in $\mathcal{B}_{p,m}(q)$ or not, note that we only need to ask q to be inert in a finite number of quadratic imaginary fields $K/\mathbb{Q}$, and we explicitly know all the possible fields K in terms of $D = \mathrm{disc}(B)$.

As for the technical condition defining $\mathcal{B}_{p,m}^{\mathrm{Br}}(q)$, we think that it is a hardly avoidable hypothesis in our result. At least, it seems that it is really needed in order to prove the statement below by means of analogue methods to that in [**Sko05**].

Finally, our first approach to the main result of this thesis is the following (compare with Theorem 5.10 stated at the end of Chapter 5 and proved below in Section 6.6 of this chapter, where condition (M) is removed at the cost of imposing that $p \equiv 3 \pmod 4$):

Theorem 7.19. *Let B be an indefinite rational quaternion algebra of discriminant D, with $2 \nmid D$. Let ω_m be a twisting Atkin-Lehner involution on X_B, with $m \neq D$. Let $p \geq 5$ be a prime factor of D such that $p \nmid m$, and suppose that (B, m) satisfies condition (M) with respect to p and to another prime q. Then*

(1) *If $B \in \mathcal{B}_{p,m}(q)$ and $p \notin P(q)$, then $X_B^{(m)}(\mathbb{Q}) = \emptyset$.*
(2) *If $B \in \mathcal{B}_{p,m}^{\mathrm{Br}}(q)$ and $p \notin P(q)$, then $X_B^{(m)}(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}} = \emptyset$.*

Proof. For the proof of both statements we will consider the $X_B^{(m)}$-torsor $f_p : Y_{B,p}^{(m)} \to X_B^{(m)}$ under $\mathbb{F}_{p^2}^{\times 12}$ attached to the prime p. If ℓ is a prime, recall that a point $Q_\ell \in X_B^{(m)}(\mathbb{Q}_\ell)$ defines a character $\phi_\ell = \phi_{Q_\ell} : \mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell) \to \mathbb{F}_{p^2}^{\times 12}$.

We may assume that $X_B^{(m)}(\mathbb{A}_\mathbb{Q}) \neq \emptyset$, since otherwise there is nothing to prove. Hence, by [**RSY05**, Theorem 3.1] this implies that $D = pm$.

(1) Suppose that there exists $Q \in X_B^{(m)}(\mathbb{Q})$. Then, by the moduli interpretation of the Atkin-Lehner quotient $X_B^{(m)}$, we can choose an abelian surface (A, i) with real multiplication by the ring of integers R_E of $E = \mathbb{Q}(\sqrt{m})$ whose field of moduli is $\mathbb{Q}$, and such that $B \subseteq \mathrm{End}^0_{\mathbb{Q}}(A)$, corresponding to the point Q. The preimages of Q under π_m^{-1} are rational over some quadratic extension of $\mathbb{Q}$, say K. That is, $\pi_m^{-1}(Q) = \{P, \omega_m(P)\} \subseteq X_B(K)$. After Shimura, K must be imaginary. By means of the diagonal embedding $X_B^{(m)}(\mathbb{Q}) \hookrightarrow X_B^{(m)}(\mathbb{A}_{\mathbb{Q}})$, the point Q defines a sequence of local points $\{Q_\ell\}_\ell \in X_B^{(m)}(\mathbb{A}_{\mathbb{Q}})$. For each one of these points, say $Q_\ell \in X_B^{(m)}(\mathbb{Q}_\ell)$, 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).

Now, because of the commutativity of the diagram 7, the global character $\phi : \mathrm{Gal}\,(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_{p^2}^{\times 12}$ obtained by specialization of the torsor f_p at Q restricts to each of the local characters ϕ_ℓ attached to each point Q_ℓ on $\mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$. Therefore, by Corollary 7.5 we have that ϕ^2 is unramified away from p.

By our assumptions, the abelian surface (A_q, i_q) representing Q_q admits a model rational over $\mathbb{Q}_q$, so we may assume it is defined over $\mathbb{Q}_q$. By Lemma 7.3, $\phi_q^2 = \alpha_{A_q,\mathfrak{p}}^{24}$, which is unramified because $q \neq p$. We claim first that $\alpha_{A_q,\mathfrak{p}}^{24}(\sigma_q) = q^{12}$. For each prime ℓ, consider the local Artin reciprocity map

$$w_\ell : \mathbb{Z}_\ell^\times \overset{\simeq}{\twoheadrightarrow} I_\ell^{ab},$$

and let

$$w : \prod_\ell \mathbb{Z}_\ell^\times \overset{\prod w_\ell}{\twoheadrightarrow} \mathrm{Gal}\,(\mathbb{Q}^{ab}/\mathbb{Q})$$

be the global Artin map. Observe that the image by w of the idèle

$$\beta = (\frac{1}{q}, \ldots, \frac{1}{q}, 1, \frac{1}{q}, \ldots) \in \prod_\ell \mathbb{Z}_\ell^\times,$$

where the 1 is in the q^{th} position, is an element $\tilde{\sigma}_q \in \mathrm{Gal}\,(\mathbb{Q}^{ab}/\mathbb{Q})$ which reduces to the Frobenius automorphism $\mathrm{Fr}_q \in \mathrm{Gal}\,(\bar{\mathbb{F}}_q/\mathbb{F}_q)$. Therefore, $\sigma_q \circ \tilde{\sigma}_q^{-1} \in I_q$, and since ϕ restricted to $\mathrm{Gal}\,(\bar{\mathbb{Q}}_q/\mathbb{Q}_q)$ coincides with ϕ_q, whose square is unramified, we have $\phi^2(\sigma_q) = \phi^2(\tilde{\sigma}_q)$.

In order to show our claim, note that we have

$$\phi^2(\sigma_q) = \phi_q^2(\sigma_q) = \alpha_{A_q,\mathfrak{p}}^{24}(\sigma_q),$$

because $\phi_{|\,\mathrm{Gal}\,(\bar{\mathbb{Q}}_q/\mathbb{Q}_q)} = \phi_q$, and

$$\phi^2(\tilde{\sigma}_q) = \phi^2(w(\beta)) = \phi^2(w_p(\frac{1}{q})) = \alpha_{A_p,\mathfrak{p}}^{24}(w_p(\frac{1}{q})),$$

since ϕ^2 is unramified away from p. So we should prove that $\alpha_{A_p,\mathfrak{p}}^{24}(w_p(\frac{1}{q})) = q^{12}$. Now let $\bar{\chi}_p : \mathrm{Gal}\,(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathbb{F}_p^\times$ the reduction of the cyclotomic character (restricted to $\mathrm{Gal}\,(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$) mod p. By [**Ser72**, Prop. 3] we have $\bar{\chi}_{p|I_p^{ab}}(w_p(x)) = \frac{1}{x} \bmod p$ for all $x \in \mathbb{Z}_p^\times$. Since $\det(\varrho_{A_p,\mathfrak{p}}) = \bar{\chi}_p$ by Lemma 7.1, writing $\tilde{x} \in \mathbb{F}_p^\times$ for the reduction modulo p of an element $x \in \mathbb{Z}_p^\times$,

$$\begin{aligned} \frac{1}{\tilde{x}} &= \bar{\chi}_p(w_p(x)) = \det \varrho_{A_p,\mathfrak{p}}(w_p(x)) = \\ &= \psi(w_p(x)) N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\alpha_{A_p,\mathfrak{p}}(w_p(x))) = \pm\alpha_{A_p,\mathfrak{p}}^2(w_p(x)), \end{aligned}$$

where we have used that $\alpha_{A_p,\mathfrak{p}} \circ w_p : \mathbb{Z}_p^\times \to \mathbb{F}_{p^2}^\times$ takes values in $\mathbb{F}_p^\times$ because it is a continuous homomorphism. Since $\mathbb{Z}_p^\times$ is an extension of $\mathbb{F}_p^\times$ by a pro-p-group, the homomorphism $\alpha_{A_p,\mathfrak{p}} \circ w_p : \mathbb{Z}_p^\times \to \mathbb{F}_p^\times \subseteq \mathbb{F}_{p^2}^\times$ must be trivial on the pro-p-part. Hence, it factors through a homomorphism $\mathbb{F}_p^\times \to \mathbb{F}_p^\times \subseteq \mathbb{F}_{p^2}^\times$. Therefore, for

$x \in \mathbb{Z}_p^\times$ we can write

$$\alpha_{A_p,\mathfrak{p}}(w_p(x)) = (\tilde{x})^{-c}$$

for some integer c determined modulo $p-1$. Combining the two last expressions,

$$\tilde{x}^{-2c} = \pm\tilde{x}^{-1},$$

so that $2c \equiv 1$ or $\frac{p+1}{2} \bmod p-1$. Since $p-1$ is even, we deduce $p \equiv 3 \bmod 4$, and $c \equiv \frac{p+1}{4}$ or $\frac{3p-1}{4} \bmod p-1$.

As a consequence,

$$\alpha^{24}_{A_p,\mathfrak{p}}(w_p(x)) \equiv x^{-\frac{24(p+1)}{4}} \text{ or } x^{-\frac{24(3p-1)}{4}} \mod p,$$

but note that $\frac{24(p+1)}{4} \equiv \frac{24(3p-1)}{4} \equiv 12 \bmod p-1$, so that particularizing for $x = \frac{1}{q}$ we finally obtain

$$\alpha^{24}_{A_p,\mathfrak{p}}(w_p(\frac{1}{q})) = q^{12} \in \mathbb{F}_p^\times.$$

Summing up,

$$\alpha^{24}_{A_q,\mathfrak{p}}(\sigma_q) = \phi^2(\sigma_q) = \phi^2(\tilde{\sigma}_q) = \alpha^{24}_{A_p,\mathfrak{p}}(\omega_p(\frac{1}{q})) = q^{12} \tag{13}$$

as we claimed.

While proving the above claim, we have proved in passing that $p \equiv 3 \bmod 4$. By Proposition 7.8, this implies that K is unramified away from D. Then, since $B \in \mathcal{B}_{p,m}(q)$, the prime q is not inert in K. Hence, $qR_K = \mathfrak{q}^2$ or $qR_K = \mathfrak{q}^\tau\mathfrak{q}$, for $\tau \in \mathrm{Gal}\,(K/\mathbb{Q})$ the nontrivial automorphism. In any case, let $\mathfrak{q}$ be a prime of R_K above q. We can regard the point P as a point in $X_B(K_\mathfrak{q})$, where $\mathfrak{q}$ is the completion of K at $\mathfrak{q}$, so that, in our previous notation, 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 the finite field $\mathbb{F}_q$ of q elements.

On the other hand, the action of σ_q on the Tate modules $T_p(A_q)$ and $T_p(\tilde{A}_q)$ is the same, where $\tilde{A}_q$ is the abelian surface over $\mathbb{F}_q$ constructed as in Section 3 of this chapter. Moreover, since the residue field of $K_q/\mathbb{Q}_q$ is $\mathbb{F}_q$, the quaternion algebra $B \subseteq \mathrm{End}^0_{K_q}(A_q)$ is embedded in $\mathrm{End}^0_{\mathbb{F}_q}(\tilde{A}_q)$ by reducing the endomorphisms modulo q. By Lemma 7.7, the characteristic polynomial of $r_{A_q,\mathfrak{p}}(\sigma_q)$ reduced modulo $\mathfrak{p}$ is

$$T^2 - (\alpha_{A_{q,\mathfrak{p}}}(\sigma_q) + q\alpha_{A_{q,\mathfrak{p}}}(\sigma_q^{-1}))T + q$$

so that by [**Jor86**, Theorem 2.1] $\alpha_{A_{q,\mathfrak{p}}}(\sigma_q) + q\alpha_{A_{q,\mathfrak{p}}}(\sigma_q^{-1})$ is the reduction modulo p of an integer a_q of absolute value at most $2\sqrt{q}$. Then, using (13) we can write

$$a_q \equiv \sqrt{q}(\zeta + \zeta^{-1}) \mod \bar{\mathfrak{p}},$$

where $\zeta = \frac{\alpha_{A_q,\mathfrak{p}}(\sigma_q)}{\sqrt{q}}$ 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 $P(q)$ the above congruence must be an equality. Moreover, since a_q is an integer the only possibility is $a_q = 0$.

Now we will show that $a_q = 0$ leads to a contradiction with the assumption that the algebra B is in $\mathcal{B}_{p,m}(q)$. As we have said above, since the extension $K_q/\mathbb{Q}_q$ has residue field $\mathbb{F}_q$, the quaternion algebra $B \subseteq \mathrm{End}^0_{K_q}(A_q)$ embeds in $\mathrm{End}^0_{\mathbb{F}_q}(\tilde{A}_q)$ by reducing the endomorphisms of A_q modulo q. Then, 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 $\mathrm{End}^0_{\mathbb{F}_q}(\tilde{A}_q) \simeq \mathrm{M}_2(\mathbb{Q}(\sqrt{-q}))$, which implies that B is split by $\mathbb{Q}(\sqrt{-q})$, and this contradicts the fact that $B \in \mathcal{B}_{p,m}(q)$.

(2) The second statement of the theorem essentially strengthens the first one under the assumption that B belongs to $\mathcal{B}^{\mathrm{Br}}_{p,m}(q)$ instead of $\mathcal{B}_{p,m}(q)$.

Now we should prove that there does not exist a family of points $Q_\ell \in X_B^{(m)}(\mathbb{Q}_\ell)$, one for each finite prime ℓ of $\mathbb{Q}$, such that the local characters $\phi_\ell = \phi_{Q_\ell}$ attached to them come from a single global character $\phi : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_{p^2}^{\times 12}$. In other words, we want to show that under our assumptions $X_B^{(m)}(\mathbb{A}_\mathbb{Q})^{f_p}$ must be empty. Then, by applying the main theorem of descent theory of Colliot-Thélène and Sansuc (see Theorem 3.32 and the comments after its statement), this implies actually that $X_B^{(m)}(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}} = \emptyset$ as we want.

So, suppose in order to find a contradiction that $X_B^{(m)}(\mathbb{A}_\mathbb{Q})^{f_p} \neq \emptyset$. Then, we can choose a family of points $\{Q_\ell\}_\ell$, $Q_\ell \in X_B^{(m)}(\mathbb{Q}_\ell)$ for each prime ℓ, such that there exists a global character ϕ restricting to each local character ϕ_ℓ on $\mathrm{Gal}(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$. Using the moduli interpretation of $X_B^{(m)}$, write (A_ℓ, i_ℓ) for an abelian surface with real multiplication by $R_{\mathbb{Q}(\sqrt{m})}$ corresponding to each point Q_ℓ.

Now the rest of the proof is exactly as in the first part, since the hypothesis $B \in \mathcal{B}^{\mathrm{Br}}_{p,m}(q)$ implies that, for every possible choice of $\{Q_\ell\}_\ell \in X_B^{(m)}(\mathbb{A}_\mathbb{Q})$, the preimages of the point $Q_q \in X_B^{(m)}(\mathbb{Q}_q)$ are rational over a quadratic extension K_q of $\mathbb{Q}_q$ with residue field $\mathbb{F}_q$. Therefore, all the arguments apply verbatim to get the same contradiction.

□

As we quoted at the end of Chapter 5, there is an explicit criterion given in [**RSY05**, Theorem 3.1] for deciding whether $X_B^{(m)}(\mathbb{A}_\mathbb{Q})$ is empty or not. When $X_B^{(m)}(\mathbb{A}_\mathbb{Q}) \neq \emptyset$, statement (1) of the above theorem gives sufficient conditions for $X_B^{(m)}$ to be a counterexample to the Hasse principle over $\mathbb{Q}$, and under the conditions of statement (2), not only $X_B^{(m)}$ is a counterexample to the Hasse principle over $\mathbb{Q}$, but moreover it is accounted for by the Brauer-Manin obstruction.

Remark 7.20. From the proof of the above theorem, it is clear that the family of quaternion algebras $\mathcal{B}_{p,m}(q)$ could be defined to be bigger, by asking the prime q not to be inert only in those imaginary quadratic fields K, unramified away from D, such that $X_B(K) \neq \emptyset$. This should define a family $\mathcal{B}^0_{p,m}(q) \supseteq \mathcal{B}_{p,m}(q)$, and we can replace $\mathcal{B}_{p,m}(q)$ by $\mathcal{B}^0_{p,m}(q)$ in the theorem. However, in practice is easier to work with $\mathcal{B}_{p,m}(q)$ instead of with $\mathcal{B}^0_{p,m}(q)$.

6. Extended Galois representations and main theorem

The aim of this section is to remove condition (M) from Theorem 7.19, in order to finally give a proof of our main result in Theorem 7.31. Given an abelian surface (A_ℓ, i_ℓ) representing a $\mathbb{Q}_\ell$-rational point $Q_\ell \in X_B^{(m)}(\mathbb{Q}_\ell)$ of our quotient of X_B by a twisting Atkin-Lehner involution, for some prime ℓ, the basic idea is to extend the Galois representations introduced in Section 1 of this chapter in an appropriate way.

More precisely, under the assumptions made from the beginning of this chapter, we should assume that the abelian surface (A_ℓ, i_ℓ) is defined either over $\mathbb{Q}_\ell$ or over K_ℓ, where K_ℓ is the quadratic extension of $\mathbb{Q}_\ell$ over which the preimages of Q_ℓ under π_m on X_B are rational. If we do not know whether (A_ℓ, i_ℓ) admits a model rational over $\mathbb{Q}_\ell$ or not, *a priori* we can only define the Galois representations $r_{A_\ell,\mathfrak{p}}$, $\varrho_{A_\ell,\mathfrak{p}}$ and $\alpha_{A_\ell,\mathfrak{p}}$ as representations of the Galois group $G_{K_\ell} = \mathrm{Gal}(\bar{\mathbb{Q}}_\ell/K_\ell)$, but not of the whole Galois group $G_{\mathbb{Q}_\ell} = \mathrm{Gal}(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$.

Independently on whether (A_ℓ, i_ℓ) admits a model rational over $\mathbb{Q}_\ell$ or not, we will define suitable *extensions* of these representations to the whole $G_{\mathbb{Q}_\ell}$. These extensions satisfy some properties analogous to the ones exposed in Sections 1, 2 and 3 of this chapter, and allow us to give a proof of our main theorem which goes along the same lines as the proof of Theorem 7.19.

6.1. Field of moduli and field of definition. With notations as usual, fix the prime ℓ, let $Q_\ell \in X_B^{(m)}(\mathbb{Q}_\ell)$ be a $\mathbb{Q}_\ell$-rational point on the Atkin-Lehner quotient and choose any abelian surface $(A_\ell, i_\ell : R_E \hookrightarrow \mathrm{End}(A))$ representing Q_ℓ.

In order to extend the Galois representations $r_{A_\ell,\mathfrak{p}}$, $\varrho_{A_\ell,\mathfrak{p}}$ and $\alpha_{A_\ell,\mathfrak{p}}$ of G_{K_ℓ} to representations of the whole $G_{\mathbb{Q}_\ell}$, we exploit the fact that the field of moduli of (A_ℓ, i_ℓ) is $\mathbb{Q}_\ell$. This implies, by definition, that there exist isomorphisms $f_\sigma : {}^\sigma A_\ell \to A_\ell$, one for each $\sigma \in G_{\mathbb{Q}_\ell} = \mathrm{Gal}(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$, such that the diagram

$$\begin{tikzcd} {}^\sigma A_\ell \arrow[r, "f_\sigma"] \arrow[d, "{}^\sigma i_\ell(\alpha)"'] & A_\ell \arrow[d, "i_\ell(\alpha)"] \\ {}^\sigma A_\ell \arrow[r, "f_\sigma"] & A_\ell, \end{tikzcd} \tag{14}$$

commutes for any $\alpha \in R_E$.

By the assumption $2 \nmid D$, combining the work of Jordan-Livné [**JL85**] and Jordan [**Jor86**], we know that the preimages $\pi_m^{-1}(Q_\ell) = \{P_\ell, P'_\ell\} \subseteq X_B(K_\ell)$ are rational over a quadratic extension $K_\ell/\mathbb{Q}_\ell$ (and they are not rational over $\mathbb{Q}_\ell$), and an abelian surface (A_ℓ, ι_ℓ) representing any of the points P_ℓ, P'_ℓ admits a model rational over K_ℓ (see Proposition 6.14). Hence, we can assume that (A_ℓ, i_ℓ) is defined over K_ℓ. Then, fix some element $s \in G_{\mathbb{Q}_\ell}$ inducing the nontrivial automorphism in $\mathrm{Gal}(K_\ell/\mathbb{Q}_\ell) = G_{\mathbb{Q}_\ell}/G_{K_\ell}$ and write

$$G_{\mathbb{Q}_\ell} = G_{K_\ell} \cup s \cdot G_{K_\ell}.$$

If $\sigma \in G_{K_\ell}$, then we can choose $f_\sigma = \mathrm{id}$, since (A_ℓ, i_ℓ) is defined over K_ℓ. And if $\sigma \notin G_{K_\ell}$, then we can choose $f_\sigma = f_s$. That is, the choice of the family $\{f_\sigma\}_{\sigma \in G_{\mathbb{Q}_\ell}}$ reduces to the choice of f_s. So fix once and for all the isomorphism f_s.

In general, the isomorphisms $\{f_\sigma\}$ can be related one to each other by considering the 2-cocycle

$$\begin{array}{rccc} c: & G_{\mathbb{Q}_\ell} \times G_{\mathbb{Q}_\ell} & \longrightarrow & \mathrm{Aut}(A_\ell, i_\ell : E \hookrightarrow \mathrm{End}^0(A)) \simeq \{\pm 1\} \\ & (\sigma, \tau) & \mapsto & f_\sigma \cdot {}^\sigma f_\tau \cdot f_{\sigma\tau}^{-1} \end{array}$$

where the isomorphism on the right follows from [**BFGR06**, Lemma 4.2]. By Weil's criterion, the abelian surface (A_ℓ, i_ℓ) admits a model rational over $\mathbb{Q}_\ell$ if and only if $f_\sigma \cdot {}^\sigma f_\tau = f_{\sigma\tau}$ for all $\sigma, \tau \in G_{\mathbb{Q}_\ell}$, that is, if and only if the cocycle c is trivial.

In our case, writing down the expression of the cocycle c, the above discussion leads to the following

Proposition 7.21. *With the above notations, the abelian surface (A_ℓ, i_ℓ) admits a model rational over $\mathbb{Q}_\ell$ if and only if $f_s \cdot {}^s f_s = id$.*

6.2. "Extending" Galois representations. Now assume that $M = T_\mathfrak{p}(A_\ell)$, $A_\ell[\mathfrak{p}]$, or C_p, where $\mathfrak{p}$ is the unique prime of $E = \mathbb{Q}(\sqrt{m})$ above p. Since (A_ℓ, i_ℓ) is defined over K_ℓ, the Galois action of $\mathrm{Gal}(\bar{\mathbb{Q}}_\ell/K_\ell)$ on M gives rise to the Galois representation $r_{A_\ell,\mathfrak{p}}$, $\varrho_{A_\ell,\mathfrak{p}}$ or $\alpha_{A_\ell,\mathfrak{p}}$, respectively, as in the previous sections. If moreover (A_ℓ, i_ℓ) admits a model rational over $\mathbb{Q}_\ell$, each one of these representations is defined on the whole absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$. As we do not want to assume that (A_ℓ, i_ℓ) admits a model rational over $\mathbb{Q}_\ell$, we need to lift these Galois representations to $\mathrm{Gal}(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$ in some sense.

If we denote the action of $\sigma \in G_{K_\ell}$ on M by $x \mapsto {}^\sigma x$, then for $\sigma \in G_{\mathbb{Q}_\ell}$ we can consider the map[2]

$$x \in M \mapsto \sigma \cdot x := f_\sigma({}^\sigma x).$$

[2] Although there are only two possibilities for f_σ, namely id or f_s, depending on whether $\sigma \in G_{K_\ell}$ or not, the action of σ on $x \in M$ depends on σ, and it is for this reason that we keep the notation f_σ.

If (A_ℓ, i_ℓ) admits a model rational over $\mathbb{Q}_\ell$, this is nothing but the usual Galois action. However, if (A_ℓ, i_ℓ) does not admit a model rational over $\mathbb{Q}_\ell$ then this does not define a $G_{\mathbb{Q}_\ell}$-action, since for $\sigma, \tau \in G_{\mathbb{Q}_\ell} \setminus G_{K_\ell}$ one has

$$\sigma\tau \cdot x := f_{\sigma\tau}({}^{\sigma\tau}x) = -f_\sigma f_\tau({}^{\sigma\tau}x) = -f_\sigma({}^{\sigma}(f_\tau({}^{\tau}x))) = -\sigma \cdot (\tau \cdot x). \tag{15}$$

In any case, we can consider the map (which is not a homomorphism, in general)

$$\begin{array}{ccc} G_{\mathbb{Q}_\ell} & \longrightarrow & \mathrm{Aut}(M) \\ \sigma & \longmapsto & (x \mapsto f_\sigma({}^{\sigma}x)). \end{array}$$

Let us denote by $\tilde{r}_{A_\ell,\mathfrak{p}}$, $\tilde{\varrho}_{A_\ell,\mathfrak{p}}$ and $\tilde{\alpha}_{A_\ell,\mathfrak{p}}$ the maps obtained in this way when replacing M by $T_{\mathfrak{p}}(A_\ell)$, $A_\ell[\mathfrak{p}]$ and C_p, respectively. That is, we get maps

$$\begin{array}{rcl} \tilde{r}_{A_\ell,\mathfrak{p}} : G_{\mathbb{Q}_\ell} & \longrightarrow & \mathrm{Aut}_{R_{E_{\mathfrak{p}}}}(T_{\mathfrak{p}}(A_\ell)) \simeq \mathrm{GL}_2(R_{E_{\mathfrak{p}}}), \\ \tilde{\varrho}_{A_\ell,\mathfrak{p}} : G_{\mathbb{Q}_\ell} & \longrightarrow & \mathrm{Aut}_{\mathbb{F}_{p^2}}(A_\ell[\mathfrak{p}]) \simeq \mathrm{GL}_2(\mathbb{F}_{p^2}), \\ \tilde{\alpha}_{A_\ell,\mathfrak{p}} : G_{\mathbb{Q}_\ell} & \longrightarrow & \mathrm{Aut}_{R_E}(C_p) \simeq \mathbb{F}_{p^2}^{\times}. \end{array}$$

Note that the R_E-linearity follows immediately from the commutative diagram (14). Although these maps are not homomorphisms in general, when restricting to G_{K_ℓ} we have equalities

$$\tilde{r}_{A_\ell,\mathfrak{p}|G_{K_\ell}} = r_{A_\ell,\mathfrak{p}}, \quad \tilde{\varrho}_{A_\ell,\mathfrak{p}|G_{K_\ell}} = \varrho_{A_\ell,\mathfrak{p}}, \quad \tilde{\alpha}_{A_\ell,\mathfrak{p}|G_{K_\ell}} = \alpha_{A_\ell,\mathfrak{p}}.$$

In particular, *the restrictions* to G_{K_ℓ} of these maps *are morphisms*. In order to have a feel about the obstruction for $\tilde{r}_{A_\ell,\mathfrak{p}}$, $\tilde{\varrho}_{A_\ell,\mathfrak{p}}$ and $\tilde{\alpha}_{A_\ell,\mathfrak{p}}$ to be morphisms, assume for a while that (A_ℓ, i_ℓ) does not admit a model rational over $\mathbb{Q}_\ell$, and take $\sigma \in G_{\mathbb{Q}_\ell} \setminus G_{K_\ell}$. Then, let us compute for example $\tilde{\alpha}_{A_\ell,\mathfrak{p}}(\sigma)^2$: if $x \in C_p$,

$$\tilde{\alpha}_{A_\ell,\mathfrak{p}}(\sigma)^2 = x \mapsto f_\sigma({}^{\sigma}(f_\sigma({}^{\sigma}x))) = x \mapsto f_s({}^{s}f_s({}^{\sigma^2}x))) = x \mapsto -({}^{\sigma^2}x) = -\tilde{\alpha}_{A_\ell,\mathfrak{p}|G_{K_\ell}}(\sigma^2), \tag{16}$$

where we have used that $f_\sigma = f_s$, $f_s \cdot {}^{s}f_s = -1$, and we have stressed the fact that $\sigma^2 \in G_{K_\ell}$. Analogous equalities hold for $\tilde{r}_{A_\ell,\mathfrak{p}}$ and $\tilde{\varrho}_{A_\ell,\mathfrak{p}}$. In the following, care must be taken because of this phenomenon.

On the other hand, the observation in (15) tells us that the reductions modulo ± 1 of these maps are morphisms, so we do get Galois representations

$$\begin{array}{rcl} \bar{r}_{A_\ell,\mathfrak{p}} = \tilde{r}_{A_{\ell,\mathfrak{p}}} \mod \pm 1 : G_{\mathbb{Q}_\ell} & \longrightarrow & \mathrm{Aut}_{R_{E_{\mathfrak{p}}}}(T_{\mathfrak{p}}(A_\ell))/\{\pm 1\} \simeq \mathrm{GL}_2(R_{E_{\mathfrak{p}}})/\{\pm 1\}, \\ \bar{\varrho}_{A_\ell,\mathfrak{p}} = \tilde{\varrho}_{A_\ell,\mathfrak{p}} \mod \pm 1 : G_{\mathbb{Q}_\ell} & \longrightarrow & \mathrm{Aut}_{\mathbb{F}_{p^2}}(A_\ell[\mathfrak{p}])/\{\pm 1\} \simeq \mathrm{GL}_2(\mathbb{F}_{p^2})/\{\pm 1\}, \\ \bar{\alpha}_{A_\ell,\mathfrak{p}} = \tilde{\alpha}_{A_\ell,\mathfrak{p}} \mod \pm 1 : G_{\mathbb{Q}_\ell} & \longrightarrow & \mathrm{Aut}_{R_E}(C_p)/\{\pm 1\} \simeq \mathbb{F}_{p^2}^{\times}/\{\pm 1\}. \end{array}$$

So, at the end, we have extended our representations to $G_{\mathbb{Q}_\ell}$, taking into account that the target must be mod out by $\{\pm 1\}$.

6.3. Some properties of the extended representations. Once we have defined our extended representations, the next step is to prove some properties for them analogous to the ones shown in the previous sections. In order to study them, it will be useful to look also at the maps $\tilde{r}_{A_\ell,\mathfrak{p}}$, $\tilde{\varrho}_{A_\ell,\mathfrak{p}}$ and $\tilde{\alpha}_{A_\ell,\mathfrak{p}}$, which can be regarded as lifts of $\bar{r}_{A_\ell,\mathfrak{p}}$, $\bar{\varrho}_{A_\ell,\mathfrak{p}}$ and $\bar{\alpha}_{A_\ell,\mathfrak{p}}$, respectively.

We start by relating $\bar{r}_{A_\ell,\mathfrak{p}}$ to the p-cyclotomic character $\chi_p : G_{\mathbb{Q}_\ell} \to \mathbb{Z}_p^{\times}$. We have seen in Lemma 7.1 that $\det(r_{A_\ell,\mathfrak{p}}) = \chi_{p|G_{K_\ell}}$. This directly implies that $\det(\tilde{r}_{A_\ell,\mathfrak{p}|G_{K_\ell}}) = \chi_{p|G_{K_\ell}}$.

Now observe that being $\bar{r}_{A_\ell,\mathfrak{p}}$ a 2-dimensional representation, for $\sigma \in G_{\mathbb{Q}_\ell}$ we can compute $\det(\bar{r}_{A_\ell,\mathfrak{p}}(\sigma))$ just as $\det(\tilde{r}_{A_\ell,\mathfrak{p}}(\sigma))$ (although $\tilde{r}_{A_\ell,\mathfrak{p}}$ is not a representation). Then, with this observation in mind, we have an equality

$$\det(\bar{r}_{A_\ell,\mathfrak{p}}(\sigma)) = \chi_p(\sigma) \quad \text{for all } \sigma \in G_{K_\ell}.$$

Obviously, if (A_ℓ, i_ℓ) admits a model rational over $\mathbb{Q}_\ell$, this equality holds for all $\sigma \in G_{\mathbb{Q}_\ell}$ (indeed, in this case $\tilde{r}_{A_\ell,\mathfrak{p}} = r_{A_\ell,\mathfrak{p}}$ and the equality has already been proved in Lemma 7.1). So assume that (A_ℓ, i_ℓ) does not admit a model rational over $\mathbb{Q}_\ell$ and take $\sigma \in G_{\mathbb{Q}_\ell} \setminus G_{K_\ell}$. By the analogous version of (16) for $\tilde{r}_{A_\ell,\mathfrak{p}}$, we have

$$\tilde{r}_{A_\ell,\mathfrak{p}}(\sigma)^2 = -\tilde{r}_{A_\ell,\mathfrak{p}|G_{K_\ell}}(\sigma^2).$$

Therefore,

$$\det(\bar{r}_{A_\ell,\mathfrak{p}}(\sigma))^2 = \det(\tilde{r}_{A_\ell,\mathfrak{p}}(\sigma)^2) = \det(-\tilde{r}_{A_\ell,\mathfrak{p}|G_{K_\ell}}(\sigma^2)) = \chi_p(\sigma^2) = \chi_p(\sigma)^2,$$

which implies that $\det(\bar{r}_{A_\ell,\mathfrak{p}}(\sigma)) = \pm\chi_p(\sigma)$.

Remark 7.22. Note that the same equality holds therefore for $\det(\bar{\varrho}_{A_\ell,\mathfrak{p}})$ and $\bar{\chi}_p$.

Now, before relating $\bar{\varrho}_{A_\ell,\mathfrak{p}}$ to $\bar{\alpha}_{A_\ell,\mathfrak{p}}$, let us look at the local behavior of $\bar{\alpha}_{A_\ell,\mathfrak{p}}$, provided $\ell \neq p$. That is, we want to study the image of the inertia subgroup $I_\ell \subseteq G_{\mathbb{Q}_\ell}$.

Assume first that (A_ℓ, i_ℓ) admits a model rational over $\mathbb{Q}_\ell$. In this case, we have seen in Proposition 7.4 that if $\ell \neq p$ then $\alpha^{24}_{A_\ell,\mathfrak{p}}$ is unramified, where now note that $\alpha_{A_\ell,\mathfrak{p}} : G_{\mathbb{Q}_\ell} \to \mathbb{F}^\times_{p^2}$. That is, $\alpha_{A_\ell,\mathfrak{p}}(I_\ell)^{24} = \{1\}$, where $I_\ell \subseteq G_{\mathbb{Q}_\ell}$ is the inertia subgroup. Since in this case $\tilde{\alpha}_{A_\ell,\mathfrak{p}} = \alpha_{A_\ell,\mathfrak{p}}$ and $\bar{\alpha}_{A_\ell,\mathfrak{p}}$ is its reduction modulo ±1, we conclude that $\bar{\alpha}_{A_\ell,\mathfrak{p}}(I_\ell)^{12} = \{1\} \subseteq \mathbb{F}^\times_{p^2}/\{\pm1\}$.

Now assume that (A_ℓ, i_ℓ) does not admit a model rational over $\mathbb{Q}_\ell$, so that $\alpha_{A_\ell,\mathfrak{p}}$ is only defined on G_{K_ℓ}. Also by Proposition 7.4 we know that $\alpha_{A_\ell,\mathfrak{p}}(I_v)^{12} = \{1\}$, where $I_v \subseteq G_{K_\ell}$ is the corresponding inertia subgroup to the unique place v of K_ℓ above ℓ. Now observe that $[I_\ell : I_v] \leq 2$, because $[K_\ell : \mathbb{Q}_\ell] = 2$. As a consequence, if $\tau \in I_\ell$ then $\tau^2 \in I_v$ and $\alpha_{A_\ell,\mathfrak{p}}(\tau^2)^{12} = 1$. Using (16), we deduce that for any $\tau \in I_\ell$

$$\tilde{\alpha}_{A_\ell,\mathfrak{p}}(\tau)^{24} = (\tilde{\alpha}_{A_\ell,\mathfrak{p}}(\tau)^2)^{12} = (-\tilde{\alpha}_{A_\ell,\mathfrak{p}|G_{K_\ell}}(\tau^2))^{12} = \alpha_{A_\ell,\mathfrak{p}}(\tau^2)^{12} = 1.$$

And, as before, since $\bar{\alpha}_{A_\ell,\mathfrak{p}}$ is the reduction modulo ±1 of $\tilde{\alpha}_{A_\ell,\mathfrak{p}}$, we conclude that $\bar{\alpha}_{A_\ell,\mathfrak{p}}(I_\ell)^{12} = \{1\} \subseteq \mathbb{F}^\times_{p^2}/\{\pm1\}$.

Therefore, we have proved:

Proposition 7.23. *If $\ell \neq p$, then $\bar{\alpha}^{12}_{A_\ell,\mathfrak{p}}$ is unramified, i.e. $\bar{\alpha}_{A_\ell,\mathfrak{p}}(I_\ell)^{12} = \{1\}$. Indeed, $\tilde{\alpha}_{A_\ell,\mathfrak{p}}(I_\ell)^{24} = \{1\}$.*

Finally, we want to relate the representations $\bar{\varrho}_{A_\ell,\mathfrak{p}}$ and $\bar{\alpha}_{A_\ell,\mathfrak{p}}$ as in Lemma 7.6. For doing so, it is useful to work with their lifts $\tilde{\varrho}_{A_\ell,\mathfrak{p}}$ and $\tilde{\alpha}_{A_\ell,\mathfrak{p}}$. First of all, the relation between $\bar{\varrho}_{A_\ell,\mathfrak{p}|G_{K_\ell}}$ and $\bar{\alpha}_{A_\ell,\mathfrak{p}|G_{K_\ell}}$ is not difficult to see following a similar reasoning as in [**Rot08**, Lemma 3.1]:

Lemma 7.24. *There exists an $\mathbb{F}_{p^2}$-basis of $A_\ell[\mathfrak{p}]$ with respect to which*

$$\begin{array}{rccc} \bar{\varrho}_{A_\ell,\mathfrak{p}|G_{K_\ell}}: & G_{K_\ell} & \longrightarrow & \mathrm{GL}_2(\mathbb{F}_{p^2})/\{\pm1\} \\ & \sigma & \longmapsto & \begin{pmatrix} \tilde{\alpha}_{A_\ell,\mathfrak{p}|G_{K_\ell}}(\sigma)^p & 0 \\ * & \tilde{\alpha}_{A_\ell,\mathfrak{p}|G_{K_\ell}}(\sigma) \end{pmatrix} \bmod \pm 1. \end{array}$$

Proof. Write $\mathcal{O}_p = R_\mathfrak{p} + R_\mathfrak{p}\cdot\pi$, and let $x \in A_\ell[\mathfrak{p}]$ be such that $A[\mathfrak{p}] = \mathcal{O}_p/\mathfrak{p}\mathcal{O}_p\cdot x = R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}\cdot x + R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}\cdot\pi(x)$. We shall compute $\tilde{\varrho}_{A_\ell,\mathfrak{p}|G_{K_\ell}} = \varrho_{A_\ell,\mathfrak{p}}$ with respect to the $\mathbb{F}_{p^2}$-basis $\{x, \pi(x)\}$ of $A_\ell[\mathfrak{p}]$ and try to read $\tilde{\alpha}_{A_\ell,\mathfrak{p}|G_{K_\ell}}$ from its expression.

Take an element $\sigma \in G_{K_\ell}$. Then the automorphism $\tilde{r}_{A_\ell,\mathfrak{p}|G_{K_\ell}}(\sigma) = r_{A_\ell,\mathfrak{p}}(\sigma)$ is the one induced by the usual Galois action of σ on $T_\mathfrak{p}(A_\ell)$, and $\tilde{\varrho}_{A_\ell,\mathfrak{p}|G_{K_\ell}}(\sigma) = \varrho_{A_\ell,\mathfrak{p}}(\sigma)$ is its reduction modulo $\mathfrak{p}$. On the one hand, let us write ${}^\sigma x = u_\sigma\cdot x + v_\sigma\cdot\pi(x)$ for some $u_\sigma, v_\sigma \in R_{E_\mathfrak{p}}$, which are uniquely determined modulo $\mathfrak{p}$. And on the other hand, since the endomorphisms of A coming from B are defined over K_ℓ, we have ${}^\sigma\pi = \pi$. Therefore,

$${}^\sigma(\pi(x)) = {}^\sigma\pi({}^\sigma x) = \pi(u_\sigma\cdot x + v_\sigma\cdot\pi(x)) = {}^\tau u_\sigma \pi(x) + {}^\tau v_\sigma\pi^2(x) = {}^\tau u_\sigma\pi(x),$$

since $\pi^2 = p$ and $p\cdot x = 0$, and where $\tau \in \mathrm{Gal}\,(E_\mathfrak{p}/\mathbb{Q}_p)$ is the non-trivial automorphism.

Switching u_σ by ${}^\tau u_\sigma$ and reducing mod $\mathfrak{p}$, it follows that $\tilde{\varrho}_{A_\ell,\mathfrak{p}}(\sigma) = \varrho_{A_\ell,\mathfrak{p}}(\sigma) = \begin{pmatrix} u^p_\sigma & 0 \\ v_\sigma & u_\sigma \end{pmatrix}$, and we recover $\tilde{\alpha}_{A_\ell,\mathfrak{p}|G_{K_\ell}} = \alpha_{A_\ell,\mathfrak{p}}$ as $\tilde{\alpha}_{A_\ell,\mathfrak{p}|G_{K_\ell}}(\sigma) = u_\sigma$. Hence the lemma follows. □

However, we would like to prove a similar relation without restricting to G_{K_ℓ}. The key point is to adapt the character ψ introduced in [**Rot08**, p. 6], and already considered in Section 1 of Chapter 6, by extending the natural G_{K_ℓ}-action on the endomorphisms of A_ℓ/K_ℓ coming from B to a $G_{\mathbb{Q}_\ell}$-action using the isomorphism f_s.

Regarding the elements in the quaternion algebra B as endomorphisms of the abelian surface A_ℓ/K_ℓ, it is clear that the Galois group G_{K_ℓ} acts naturally on B: for any $\sigma \in G_{K_\ell}$, $\beta \mapsto {}^\sigma\beta$ defines an automorphism $B \to B$. But if $\sigma \in G_{\mathbb{Q}_\ell} \setminus G_{K_\ell}$, then ${}^\sigma A_\ell$ must not be equal to A and this does not work. Instead, we define an action of $G_{\mathbb{Q}_\ell}$ on B by using the chosen isomorphisms f_σ. That is, for any $\sigma \in G_{\mathbb{Q}_\ell}$ we can consider the automorphism

$$B \longrightarrow B, \quad \beta \longmapsto f_\sigma {}^\sigma\beta f_\sigma^{-1}.$$

Observe that if (A_ℓ, i_ℓ) admits a model rational over $\mathbb{Q}_\ell$, then all the f_σ's can be chosen to be the identity and this is nothing but the usual Galois action.

By the Noether-Skolem Theorem, each one of these automorphisms is inner, so that there exists $\omega_\sigma \in \mathcal{O}$ such that $f_\sigma {}^\sigma\beta f_\sigma^{-1} = \omega_\sigma \beta \omega_\sigma^{-1}$.

As before, everything reduces to the role played by f_s. Indeed, recall that for an arbitrary $\sigma \in G_{\mathbb{Q}_\ell}$, the isomorphism f_σ has been chosen to be either the identity or f_s, depending on whether $\sigma \in G_{K_\ell}$ or not, respectively. Also, if $\tau \in G_{K_\ell}$, note that since (A_ℓ, ι_ℓ) is defined over K_ℓ (in particular, all the endomorphisms coming from B are defined over K_ℓ) we have ${}^\tau\beta = \beta$, so that for any $\sigma \in G_{\mathbb{Q}_\ell}$, ${}^\sigma\beta$ equals either β or ${}^s\beta$, depending on whether $\sigma \in G_{K_\ell}$ or not, respectively. Summing up,

$$f_\sigma {}^\sigma\beta f_\sigma^{-1} = \begin{cases} \beta & \text{if } \sigma \in G_{K_\ell} \\ f_s {}^s\beta f_s^{-1} = \omega_s \beta \omega_s^{-1} & \text{if } \sigma \notin G_{K_\ell}. \end{cases}$$

Now, the commutativity of (14) implies that $\beta = \omega_s \beta \omega_s^{-1}$ for every $\beta \in E$ (equivalently, the same happens replacing s by σ, for any $\sigma \in G_{\mathbb{Q}_\ell}$). Therefore, ω_s belongs to the commutator of E in B, which is E itself because it is a maximal subfield of B. Hence, $\omega_s \in R_E = \mathcal{O} \cap E$.

In this way, there is a continuous homomorphism

$$\psi : G_{\mathbb{Q}_\ell} \longrightarrow E^\times/\mathbb{Q}^\times, \quad \sigma \longmapsto \omega_\sigma,$$

which indeed factors as

$$\psi : G_{\mathbb{Q}_\ell} \twoheadrightarrow \mathrm{Gal}\,(K_\ell/\mathbb{Q}_\ell) \longrightarrow E^\times/\mathbb{Q}^\times,$$

and therefore corresponds to the quadratic character attached to $K_\ell/\mathbb{Q}_\ell$. From now on, we shall assume then that $\psi : G_{\mathbb{Q}_\ell} \to \{\pm 1\}$.

Once the character ψ is introduced, the above lemma generalizes to a relation between $\tilde{\varrho}_{A_\ell,\mathfrak{p}}$ and $\tilde{\alpha}_{A_\ell,\mathfrak{p}}$ as we now prove.

Lemma 7.25. *There exists an $\mathbb{F}_{p^2}$-basis of $A_\ell[\mathfrak{p}]$ with respect to which*

$$\begin{array}{cccc} \tilde{\varrho}_{A_\ell,\mathfrak{p}} : & G_{\mathbb{Q}_\ell} & \longrightarrow & \mathrm{GL}_2(\mathbb{F}_{p^2})/\{\pm 1\} \\ & \sigma & \longmapsto & \begin{pmatrix} \psi(\sigma)\tilde{\alpha}_{A_\ell,\mathfrak{p}}(\sigma)^p & 0 \\ * & \tilde{\alpha}_{A_\ell,\mathfrak{p}}(\sigma) \end{pmatrix} \bmod \pm 1. \end{array}$$

Proof. With the same notations as in the proof of the previous lemma, we shall compute $\tilde{\varrho}_{A_\ell,\mathfrak{p}}$ with respect to the $\mathbb{F}_{p^2}$-basis $\{x, \pi(x)\}$ of $A_\ell[\mathfrak{p}]$ and try to read $\tilde{\alpha}_{A_\ell,\mathfrak{p}}$ from its expression.

Since the character ψ is trivial on G_{K_ℓ}, the statement for $\sigma \in G_{K_\ell}$ is exactly the previous lemma. So we have to deal with the case $\sigma \in G_{\mathbb{Q}_\ell} \setminus G_{K_\ell}$. As before, we now write

$$\tilde{r}_{A_\ell,\mathfrak{p}}(\sigma)(x) = f_\sigma({}^\sigma x) = u_\sigma \cdot x + v_\sigma \cdot \pi(x),$$

where $u_\sigma, v_\sigma \in R_{E_\mathfrak{p}}$ are uniquely determined modulo $\mathfrak{p}$. In order to compute $\tilde{r}_{A_\ell,\mathfrak{p}}(\sigma)(\pi(x))$, following the above discussion we have that

$$f_\sigma {}^\sigma\pi f_\sigma^{-1} = \omega_s \pi \omega_s^{-1} = \pi^\tau \omega_s \omega_s^{-1} = -\pi,$$

where again $\tau \in \mathrm{Gal}\,(E_{\mathfrak{p}}/\mathbb{Q}_p)$ denotes the non-trivial automorphism.

Therefore,

$$f_\sigma({}^{\sigma}(\pi(x))) = -\pi(f_\sigma({}^{\sigma}x)) = -\pi(u_\sigma \cdot x + v_\sigma \cdot \pi(x)) = -{}^{\tau}u_\sigma \cdot \pi(x).$$

Switching u_σ and $-{}^{\tau}u_\sigma$ for ease of notation and reducing modulo $\mathfrak{p}$, we finally obtain that

$$\tilde{\varrho}_{A_\ell,\mathfrak{p}}(\sigma) = \begin{pmatrix} -u_\sigma^p & 0 \\ v_\sigma & u_\sigma \end{pmatrix} = \begin{pmatrix} \psi(\sigma)u_\sigma^p & 0 \\ v_\sigma & u_\sigma \end{pmatrix}.$$

Reducing modulo ± 1, we deduce that $\bar{\alpha}_{A_\ell,\mathfrak{p}}(\sigma) = u_\sigma \mod \pm 1$, so the lemma follows. □

Using this expression for $\bar{\varrho}_{A_\ell,\mathfrak{p}}$ in terms of $\tilde{\alpha}_{A_\ell,\mathfrak{p}}$, we can obtain an expression for the characteristic polynomial of a Frobenius element under $\bar{r}_{A_\ell,\mathfrak{p}}$ modulo $\mathfrak{p}$. Let $\sigma_\ell \in G_{\mathbb{Q}_\ell}$ 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 7.26. *If $\ell \neq p$, then the characteristic polynomial $\Phi_\ell(T) \in R_E[T]$ of $\bar{r}_{A_\ell,\mathfrak{p}}(\sigma_\ell)$ satisfies the congruence*

$$\Phi_\ell(T) \equiv T^2 - (\tilde{\alpha}_{A_\ell,\mathfrak{p}}(\sigma_\ell) \pm \ell\tilde{\alpha}_{A_\ell,\mathfrak{p}}(\sigma_\ell)^{-1})T \pm \ell \mod \mathfrak{p}.$$

Proof. From the previous lemma, it is clear that $\Phi_\ell(T)$ satisfies the congruence

$$\Phi_\ell(T) \bmod \mathfrak{p} \equiv T^2 - (\tilde{\alpha}_{A_\ell,\mathfrak{p}}(\sigma_\ell) + \psi(\sigma_\ell)\tilde{\alpha}_{A_\ell,\mathfrak{p}}(\sigma_\ell)^p)T + \psi(\sigma_\ell)N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\tilde{\alpha}_{A_\ell,\mathfrak{p}}(\sigma_\ell)).$$

Since $\ell \neq p$ and $\det(\bar{\varrho}_{A_\ell,\mathfrak{p}}(\sigma_\ell)) = \pm\ell$, we can write

$$\psi(\sigma_\ell)\tilde{\alpha}_{A_\ell,\mathfrak{p}}(\sigma_\ell)^p\tilde{\alpha}_{A_\ell,\mathfrak{p}}(\sigma_\ell) = \pm\ell \in \mathbb{F}_{p^2}^\times,$$

and therefore

$$\tilde{\alpha}_{A_\ell,\mathfrak{p}}(\sigma_\ell) + \psi(\sigma_\ell)\tilde{\alpha}_{A_\ell,\mathfrak{p}}(\sigma_\ell)^p \equiv \tilde{\alpha}_{A_\ell,\mathfrak{p}}(\sigma_\ell) \pm \ell\tilde{\alpha}_{A_\ell,\mathfrak{p}}(\sigma_\ell)^{-1} \mod \mathfrak{p},$$

so the statement is proved. □

Remark 7.27. If $\sigma_\ell \in G_{K_\ell}$, the proof of Lemma 7.24 implies a stronger fact: in this case, the characteristic polynomial of $r_{A_\ell,\mathfrak{p}}(\sigma_\ell) = \tilde{r}_{A_\ell,\mathfrak{p}}(\sigma_\ell)$ reduced modulo $\mathfrak{p}$ is congruent to $T^2 - (\tilde{\alpha}_{A_\ell,\mathfrak{p}}(\sigma_\ell) + \ell\tilde{\alpha}_{A_\ell,\mathfrak{p}}(\sigma_\ell)^{-1})T + \ell \in \mathbb{F}_{p^2}[T]$.

Remark 7.28. We have proved in Lemma 7.25 that

$$\bar{\varrho}_{A_\ell,\mathfrak{p}}(\sigma) = \begin{pmatrix} \psi(\sigma)\tilde{\alpha}_{A_\ell,\mathfrak{p}}(\sigma)^p & 0 \\ * & \tilde{\alpha}_{A_\ell,\mathfrak{p}}(\sigma) \end{pmatrix} \mod \pm 1,$$

for any $\sigma \in G_{\mathbb{Q}_\ell}$. We also have mentioned that $\det(\bar{\varrho}_{A_\ell,\mathfrak{p}}(\sigma))$ can be computed as $\det(\tilde{\varrho}_{A_\ell,\mathfrak{p}}(\sigma))$. Equivalently, as the determinant of the matrix on the right hand side of the above equality.

On the other hand, observe that $\bar{\alpha}_{A_\ell,\mathfrak{p}} : \mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell) \to \mathbb{F}_{p^2}^\times/\{\pm 1\} \simeq \mathbb{Z}/\frac{p^2-1}{2}\mathbb{Z}$ takes values in an abelian group, hence it factors through a homomorphism $\bar{\alpha}_{A_\ell,\mathfrak{p}} : \mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)^{ab} \to \mathbb{F}_{p^2}^\times/\{\pm 1\}$. However, we cannot say the same for $\tilde{\alpha}_{A_\ell,\mathfrak{p}}$, as it is not a homomorphism.

But note that $\det(\bar{\varrho}_{A_\ell,\mathfrak{p}}) : \mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell) \to \mathbb{F}_{p^2}^\times$ is a homomorphism, and then by the same reasoning it factors through a homomorphism $\det(\bar{\varrho}_{A_\ell,\mathfrak{p}}) : \mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)^{ab} \to \mathbb{F}_{p^2}^\times$. Using the above relation given by Lemma 7.25, this shows that

$$\sigma \mapsto \psi(\sigma)\tilde{\alpha}_{A_\ell,\mathfrak{p}}(\sigma)^p\tilde{\alpha}_{A_\ell,\mathfrak{p}}(\sigma)$$

depends only on the coset of $\sigma \in \mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$ in the abelianization $\mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)^{ab}$. Indeed, since ψ is a quadratic character,

$$\sigma \mapsto \tilde{\alpha}_{A_\ell,\mathfrak{p}}(\sigma)^p\tilde{\alpha}_{A_\ell,\mathfrak{p}}(\sigma)$$

depends only on the coset of $\sigma \in \mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$ in the abelianization $\mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)^{ab}$.

6.4. $\bar{\alpha}_{A_p,\mathfrak{p}}$ on the inertia subgroup $I_p \subseteq \mathrm{Gal}\,(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$. We have already seen that, for a prime $\ell \neq p$, the character $\bar{\alpha}_{A_\ell,\mathfrak{p}}^{12}$ is unramified. Now we want to make a closer analysis of the case $\ell = p$. First, recall that the local Artin reciprocity map gives us an isomorphism $w_p : \mathbb{Z}_p^\times \overset{\simeq}{\to} I_p^{ab} \subseteq G_{\mathbb{Q}_p}^{ab} = \mathrm{Gal}\,(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)^{ab}$. Also, the character $\bar{\alpha}_{A_p,\mathfrak{p}}$ factors through $\bar{\alpha}_{A_p,\mathfrak{p}} : G_{\mathbb{Q}_p}^{ab} \to \mathbb{F}_{p^2}^\times/\{\pm 1\}$. Therefore, we can consider the composition

$$\bar{\alpha}_{A_p,\mathfrak{p}} \circ w_p : \mathbb{Z}_p^\times \underset{\simeq}{\xrightarrow{w_p}} I_p^{ab} \subseteq G_{\mathbb{Q}_p}^{ab} \xrightarrow{\bar{\alpha}_{A_p,\mathfrak{p}}} \mathbb{F}_{p^2}^\times/\{\pm 1\},$$

which is a continuous homomorphism.

Observe that $\mathbb{F}_{p^2}^\times/\{\pm 1\}$ is isomorphic to the cyclic group $C_{(p^2-1)/2} \simeq \mathbb{Z}/\frac{p^2-1}{2}\mathbb{Z}$ of $\frac{p^2-1}{2}$ elements, which has exactly one (cyclic) subgroup of order d for each positive divisor d of $\frac{p^2-1}{2}$. Among them, $\mathbb{F}_p^\times/\{\pm 1\} \subseteq \mathbb{F}_{p^2}^\times/\{\pm 1\}$ is identified with the cyclic subgroup of order $(p-1)/2$. Note also that $\mathbb{Z}_p^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$.

Therefore, the image $\bar{\alpha}_{A_p,\mathfrak{p}}(w_p(\mathbb{Z}_p^\times))$ of $\mathbb{Z}_p^\times$ under $\bar{\alpha}_{A_p,\mathfrak{p}} \circ w_p$ must be contained in a cyclic subgroup $C_d \subseteq \mathbb{F}_{p^2}^\times/\{\pm 1\}$, for some $d|(p^2-1)/2$, which arises as a quotient of $\mathbb{Z}_p^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$ by a closed subgroup. Such quotients are of the form $C_{d'} \times \mathbb{Z}/p^n\mathbb{Z}$, for some integer $n \geq 1$ and some cyclic subgroup $C_{d'}$ of order d' dividing $p-1$. Clearly, the factor $\mathbb{Z}/p^n\mathbb{Z}$ cannot arise, so that the image of $\mathbb{Z}_p^\times$ must be contained in a cyclic subgroup $C_d \subseteq \mathbb{F}_{p^2}^\times/\{\pm 1\}$, with $d|(p-1)$. In any case, $\bar{\alpha}_{A_p,\mathfrak{p}}(w_p(\mathbb{Z}_p^\times)) \subseteq C_{p-1} \subseteq \mathbb{F}_{p^2}^\times/\{\pm 1\}$, and $C_{(p-1)/2} \simeq \mathbb{F}_p^\times/\{\pm 1\} \subseteq C_{p-1}$ with index 2. Hence, for any $x \in \mathbb{Z}_p^\times$, $\bar{\alpha}_{A_p,\mathfrak{p}}(w_p(x))^2 = \bar{\alpha}_{A_p,\mathfrak{p}}(w_p(x^2)) \in \mathbb{F}_p^\times/\{\pm 1\}$.

If we take any representative $\tau \in I_p$ of $w_p(x) \in I_p^{ab}$, this implies that $\bar{\alpha}_{A_p,\mathfrak{p}}(\tau^2) \in \mathbb{F}_p^\times/\{\pm 1\}$. As a consequence, $\tilde{\alpha}_{A_p,\mathfrak{p}}(\tau^2) \in \mathbb{F}_p^\times$ for any $\tau \in I_p \subseteq G_{\mathbb{Q}_p}$.

Combining this with the above remark, if $\tau \in I_p$ is a representative for $w_p(x)$, then

$$(\tilde{\alpha}_{A_p,\mathfrak{p}}(\tau^2))^2 = N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\tilde{\alpha}_{A_p,\mathfrak{p}}(\tau^2)) = \tilde{\alpha}_{A_p,\mathfrak{p}}(\tau^2)^p \tilde{\alpha}_{A_p,\mathfrak{p}}(\tau^2)$$

depends only on $w_p(x) \in I_p^{ab}$.

6.5. Galois representations and local characters. As we have seen in our first approach to the main theorem of this work, one of the key points has been the equality $\phi_{\ell|G_{K_\ell}} = \alpha_{A_\ell,\mathfrak{p}}^{12}$ relating the Galois representation $\alpha_{A_\ell,\mathfrak{p}} : \mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/K_\ell) \to \mathbb{F}_{p^2}^\times$, arising from the Galois action on the canonical torsion subgroup C_p of A_ℓ at p, and the local character $\phi_\ell : G_{\mathbb{Q}_\ell} \to \mathbb{F}_{p^2}^{\times 12}$ obtained by specialization of the torsor f_p at $Q_\ell \in X_B^{(m)}(\mathbb{Q}_\ell)$. Now, since $\tilde{\alpha}_{A_\ell,\mathfrak{p}|G_{K_\ell}} = \alpha_{A_\ell,\mathfrak{p}}$, we have an equality

$$(\tilde{\alpha}_{A_\ell,\mathfrak{p}|G_{K_\ell}})^{12} = \phi_{\ell|G_{K_\ell}}.$$

Furthermore, let $\sigma \in G_{\mathbb{Q}_\ell} \setminus G_{K_\ell}$. By applying (16),

$$\tilde{\alpha}_{A_\ell,\mathfrak{p}}(\sigma)^{24} = (\tilde{\alpha}_{A_\ell,\mathfrak{p}}(\sigma)^2)^{12} = (-\tilde{\alpha}_{A_\ell,\mathfrak{p}}(\sigma^2))^{12} = \tilde{\alpha}_{A_\ell,\mathfrak{p}|G_{K_\ell}}(\sigma^2)^{12} = \phi_{\ell|G_{K_\ell}}(\sigma^2) = \phi_\ell(\sigma)^2,$$

which implies that $\tilde{\alpha}_{A_\ell,\mathfrak{p}}(\sigma)^{12} = \pm\phi_\ell(\sigma)$.

These facts imply the following

Proposition 7.29. *For any $\sigma \in \mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$, $\tilde{\alpha}_{A_\ell,\mathfrak{p}}(\sigma)^{24} = \phi_\ell(\sigma)^2$. In terms of $\bar{\alpha}_{A_\ell,\mathfrak{p}}$, we have*

$$\bar{\alpha}_{A_\ell,\mathfrak{p}}(\sigma)^{12} = \phi_\ell(\sigma) \mod \pm 1, \quad \forall \sigma \in \mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell).$$

Corollary 7.30. *For $\ell \neq p$, the local character ϕ_ℓ^2 is unramified.*

Proof. This follows immediately from Proposition 7.29 and Proposition 7.23. □

6.6. Proof of the main theorem. Finally, we can prove the main theorem of this thesis, which was stated in Theorem 5.10. The notations regarding the families of quaternion algebras $\mathcal{B}_{p,m}(q)$ and $\mathcal{B}^{\mathrm{Br}}_{p,m}(q)$, as well as the set of exceptional primes $P(q)$, are as before Theorem 7.19.

The big difference with respect to Theorem 7.19 is that we can remove condition (M) from the statement. Indeed, instead of assuming this condition, which cannot be checked in practice, we only need to assume a congruence condition on the prime p, which is definitely a better hypothesis. Note also that the proof goes along the same lines as the proof of Theorem 7.19, but using our extended Galois representations instead of the *usual* ones.

Theorem 7.31 (Main Theorem)**.** *Let B be an indefinite rational quaternion algebra of discriminant D, with $2 \nmid D$. Let ω_m be a twisting Atkin-Lehner involution on X_B, with $m \neq D$. Let $p \geq 5$ be a prime factor of D, $p \equiv 3 \mod 4$, such that $p \nmid m$. Let also q be a prime. Then,*

(1) *If $B \in \mathcal{B}_{p,m}(q)$ and $p \notin P(q)$, then $X_B^{(m)}(\mathbb{Q}) = \emptyset$.*
(2) *If $B \in \mathcal{B}^{\mathrm{Br}}_{p,m}(q)$ and $p \notin P(q)$, then $X_B^{(m)}(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} = \emptyset$.*

Proof. For the proof of both statements we will consider the $X_B^{(m)}$-torsor $f_p : Y_{B,p}^{(m)} \to X_B^{(m)}$ under $\mathbb{F}_{p^2}^{\times 12}$ attached to the prime p. If ℓ is a prime, recall that a point $Q_\ell \in X_B^{(m)}(\mathbb{Q}_\ell)$ defines a character $\phi_\ell = \phi_{Q_\ell} : \mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell) \to \mathbb{F}_{p^2}^{\times 12}$.

We may assume that $X_B^{(m)}(\mathbb{A}_{\mathbb{Q}}) \neq \emptyset$, since otherwise there is nothing to prove. Hence, by [**RSY05**, Theorem 3.1] this implies that $D = pm$.

(1) Suppose that there exists $Q \in X_B^{(m)}(\mathbb{Q})$. Then, by the moduli interpretation of the Atkin-Lehner quotient $X_B^{(m)}$, we can choose an abelian surface (A, i) with real multiplication by the ring of integers R_E of $E = \mathbb{Q}(\sqrt{m})$ whose field of moduli is $\mathbb{Q}$, and such that $B \subseteq \mathrm{End}^0_{\mathbb{Q}}(A)$, corresponding to the point Q. The preimages of Q under π_m^{-1} are rational over some quadratic extension of $\mathbb{Q}$, say K. That is, $\pi_m^{-1}(Q) = \{P, \omega_m(P)\} \subseteq X_B(K)$. After Shimura, K must be imaginary. By means of the diagonal embedding $X_B^{(m)}(\mathbb{Q}) \hookrightarrow X_B^{(m)}(\mathbb{A}_{\mathbb{Q}})$, the point Q defines a sequence of local points $\{Q_\ell\}_\ell \in X_B^{(m)}(\mathbb{A}_{\mathbb{Q}})$. For each one of these points, say $Q_\ell \in X_B^{(m)}(\mathbb{Q}_\ell)$, 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).

Now, because of the commutativity of the diagram 7, the global character $\phi : \mathrm{Gal}\,(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_{p^2}^{\times 12}$ obtained by specialization of the torsor f_p at Q restricts to each of the local characters ϕ_ℓ attached to each point Q_ℓ on $\mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$. Therefore, by Corollary 7.30 we have that ϕ^2 is unramified away from p.

Let us consider the abelian surface (A_q, i_q) representing the point $Q_q \in X_B^{(m)}(\mathbb{Q}_q)$, and consider the representation $\bar{\alpha}_{A_q,\mathfrak{p}} : G_{\mathbb{Q}_q} \to \mathbb{F}_{p^2}^{\times}/\{\pm 1\}$, as well as the map $\tilde{\alpha}_{A_q,\mathfrak{p}} : G_{\mathbb{Q}_q} \to \mathbb{F}_{p^2}^{\times}$. Recall also that we have a local character $\phi_q : G_{\mathbb{Q}_q} \to \mathbb{F}_{p^2}^{\times 12}$ attached to Q_q by specialization of the torsor f_p, satisfying $\phi_q^2 = \tilde{\alpha}_{A_q,\mathfrak{p}}^{24}$ and $\phi_q \mod \pm 1 = \bar{\alpha}_{A_q,\mathfrak{p}}^{12}$.

As before, choose $\sigma_q \in G_{\mathbb{Q}_q}$ a Frobenius element, i.e. inducing $\mathrm{Fr}_q \in \mathrm{Gal}\,(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ under reduction. We first claim that $\tilde{\alpha}_{A_q,\mathfrak{p}}(\sigma_q)^{24} = q^{12} \in \mathbb{F}_p^{\times}$.

For each prime ℓ, consider the local Artin reciprocity map

$$w_\ell : \mathbb{Z}_\ell^{\times} \overset{\simeq}{\to} I_\ell^{ab},$$

and let

$$w : \prod_\ell \mathbb{Z}_\ell^{\times} \overset{\prod w_\ell}{\twoheadrightarrow} \mathrm{Gal}\,(\mathbb{Q}^{ab}/\mathbb{Q})$$

be the global Artin map. Observe that the image by w of the idèle

$$\beta = (\frac{1}{q}, \dots, \frac{1}{q}, 1, \frac{1}{q}, \dots) \in \prod_{\ell} \mathbb{Z}_\ell^\times,$$

where the 1 is in the q^{th} position, is an element $\tilde{\sigma}_q \in \mathrm{Gal}\,(\mathbb{Q}^{ab}/\mathbb{Q})$ which reduces to the Frobenius automorphism $\mathrm{Fr}_q \in \mathrm{Gal}\,(\bar{\mathbb{F}}_q/\mathbb{F}_q)$. Therefore, $\sigma_q \circ \tilde{\sigma}_q^{-1} \in I_q$, and since ϕ restricted to $\mathrm{Gal}\,(\bar{\mathbb{Q}}_q/\mathbb{Q}_q)$ coincides with ϕ_q, whose square is unramified, we have $\phi(\sigma_q)^2 = \phi(\tilde{\sigma}_q)^2$.

In order to show our claim, first note that we have

$$\phi(\sigma_q)^2 = \phi_q(\sigma_q)^2 = \tilde{\alpha}_{A_q,\mathfrak{p}}(\sigma_q)^{24},$$

because $\phi_{|\,\mathrm{Gal}\,(\bar{\mathbb{Q}}_q/\mathbb{Q}_q)} = \phi_q$. Besides, since ϕ^2 is unramified away from p,

$$\phi(\tilde{\sigma}_q)^2 = \phi(w(\beta))^2 = \phi(w_p(\frac{1}{q}))^2,$$

which implies that $\phi(\tilde{\sigma}_q) \mod \pm 1 = \phi(w_p(\frac{1}{q})) \mod \pm 1$. Therefore,

$$\begin{aligned}\phi(\tilde{\sigma}_q) \bmod \pm 1 &= \phi(w_p(\frac{1}{q})) \bmod \pm 1 = \bar{\alpha}_{A_p,\mathfrak{p}}(w_p(\frac{1}{q}))^{12} = \\ &= \bar{\alpha}_{A_p,\mathfrak{p}}(\tau_{1/q})^{12} = \tilde{\alpha}_{A_p,\mathfrak{p}}(\tau_{1/q})^{12} \bmod \pm 1,\end{aligned}$$

where we choose any representative $\tau_{1/q} \in I_p$ of $w_p(\frac{1}{q}) \in I_p^{ab}$ (this makes sense since $\bar{\alpha}_{A_p,\mathfrak{p}}$ factors through $G_{\mathbb{Q}_p}^{ab} \to \mathbb{F}_{p^2}^\times/\{\pm 1\}$). In particular, this shows that

$$\phi(\tilde{\sigma}_q) = \pm\tilde{\alpha}_{A_p,\mathfrak{p}}(\tau_{1/q})^{12}, \quad \text{hence} \quad \phi(\tilde{\sigma}_q)^2 = \tilde{\alpha}_{A_p,\mathfrak{p}}(\tau_{1/q})^{24}.$$

So, for proving our claim, we must show that $\tilde{\alpha}_{A_p,\mathfrak{p}}(\tau_{1/q})^{24} = q^{12}$. For this, let $\bar{\chi}_p : \mathrm{Gal}\,(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \to F_p^\times$ be the reduction of the cyclotomic character mod p. By [**Ser72**, Prop. 3], we have $\bar{\chi}_{p|I_p^{ab}}(w_p(x)) = \frac{1}{x} \bmod p$ for all $x \in \mathbb{Z}_p^\times$. For $x \in \mathbb{Z}_p^\times$, let $\tau_x \in I_p$ be any representative of $w_p(x) \in I_p^{ab}$. Then, if $\tilde{x} \in \mathbb{F}_p^\times$ denotes the reduction modulo p of $x \in \mathbb{Z}_p^\times$,

$$\begin{aligned}\frac{1}{\tilde{x}^2} &= \bar{\chi}_p(w_p(x^2)) = \pm\det(\bar{\varrho}_{A_p,\mathfrak{p}}(w_p(x^2))) = \pm\det(\bar{\varrho}_{A_p,\mathfrak{p}}(\tau_x^2)) = \\ &= \pm\psi(\tau_x^2)N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\tilde{\alpha}_{A_p,\mathfrak{p}}(\tau_x^2)) = \pm\tilde{\alpha}_{A_p,\mathfrak{p}}(\tau_x^2)^2 = \pm\tilde{\alpha}_{A_p,\mathfrak{p}}(\tau_x)^4,\end{aligned}$$

where we have used that $\bar{\varrho}_{A_p,\mathfrak{p}}$ factors through $\bar{\varrho}_{A_p,\mathfrak{p}} : G_{\mathbb{Q}_p}^{ab} \to \mathbb{F}_{p^2}^\times$ and that $\tilde{\alpha}_{A_p,\mathfrak{p}}(\tau^2) \in \mathbb{F}_p^\times$ for every $\tau \in I_p$ (see Section 6.4 above).

In particular, for $x = 1/q$ we get

$$\tilde{\alpha}_{A_p,\mathfrak{p}}(\tau_{1/q})^{24} = q^{12} \in \mathbb{F}_p^\times, \tag{17}$$

as we claimed.

Now, since $p \equiv 3 \bmod 4$ by hypothesis, Proposition 7.8 implies that K is unramified away from D. Then, since $B \in \mathcal{B}_{p,m}(q)$, the prime q is not inert in K. Hence, $qR_K = \mathfrak{q}^2$ or $qR_K = \mathfrak{q}^g\mathfrak{q}$, for $g \in \mathrm{Gal}\,(K/\mathbb{Q})$ the nontrivial automorphism. In any case, let $\mathfrak{q}$ be a prime of R_K above q. We can regard the point P as a point in $X_B(K_\mathfrak{q})$, where $\mathfrak{q}$ is the completion of K at $\mathfrak{q}$, so that, in our previous notation, 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 the finite field $\mathbb{F}_q$ of q elements.

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 $B \subseteq \mathrm{End}_{K_q}^0(A_q)$ is embedded in $\mathrm{End}_{\mathbb{F}_q}^0(\tilde{A}_q)$, since the residue field of $K_q/\mathbb{Q}_q$ is $\mathbb{F}_q$. Also for this reason, $\sigma_q \in \mathrm{Gal}\,(\bar{\mathbb{Q}}_q/K_q) \subseteq$

Gal $(\bar{\mathbb{Q}}_q/\mathbb{Q}_q)$, hence by Corollary 7.26, the characteristic polynomial of $r_{A_q,\mathfrak{p}}(\sigma_q)$ reduced modulo $\mathfrak{p}$ is congruent to

$$T^2 - (\tilde{\alpha}_{A_q,\mathfrak{p}}(\sigma_q) + \ell\tilde{\alpha}_{A_q,\mathfrak{p}}(\sigma_q)^{-1})T + q \in \mathbb{F}_{p^2}[T],$$

so that, by [**Jor86**, Theorem 2.1], $\tilde{\alpha}_{A_q,\mathfrak{p}}(\sigma_q)+q\tilde{\alpha}_{A_q,\mathfrak{p}}(\sigma_q^{-1})$ is the reduction modulo p of an integer a_q of absolute value at most $2\sqrt{q}$. Then, using (17) we can write

$$a_q \equiv \sqrt{q}(\zeta + \zeta^{-1}) \mod \bar{\mathfrak{p}},$$

where $\zeta = \frac{\tilde{\alpha}_{A_q,\mathfrak{p}}(\sigma_q)}{\sqrt{q}}$ 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 $|a_q| \le 2\sqrt{q}$, from the definition of $P(q)$ the above congruence must be an equality. Moreover, since a_q is an integer the only possibility is $a_q = 0$.

Now we will show that $a_q = 0$ leads to a contradiction with the assumption that the algebra B is in $\mathcal{B}_{p,m}(q)$. As we have said above, since the extension $K_q/\mathbb{Q}_q$ has residue field $\mathbb{F}_q$, the quaternion algebra $B \subseteq \mathrm{End}^0_{K_q}(A_q)$ embeds in $\mathrm{End}^0_{\mathbb{F}_q}(\tilde{A}_q)$ by reducing the endomorphisms of A_q modulo q. Then, 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 $\mathrm{End}^0_{\mathbb{F}_q}(\tilde{A}_q) \simeq \mathrm{M}_2(\mathbb{Q}(\sqrt{-q}))$, which implies that B is split by $\mathbb{Q}(\sqrt{-q})$, and this contradicts the fact that $B \in \mathcal{B}_{p,m}(q)$.

(2) The second statement of the theorem essentially strengthens the first one under the assumption that B belongs to $\mathcal{B}^{\mathrm{Br}}_{p,m}(q)$ instead of $\mathcal{B}_{p,m}(q)$.

Now we should prove that there does not exist a family of points $Q_\ell \in X_B^{(m)}(\mathbb{Q}_\ell)$, one for each finite prime ℓ of $\mathbb{Q}$, such that the local characters $\phi_\ell = \phi_{Q_\ell}$ attached to them come from a single global character $\phi : \mathrm{Gal}\,(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_{p^2}^{\times 12}$. In other words, we want to show that under our assumptions $X_B^{(m)}(\mathbb{A}_\mathbb{Q})^{f_p}$ must be empty. Then, by applying the main theorem of descent theory of Colliot-Thélène and Sansuc (see Theorem 3.32 and the comments after its statement), this implies actually that $X_B^{(m)}(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}} = \emptyset$ as we want.

So, suppose in order to find a contradiction that $X_B^{(m)}(\mathbb{A}_\mathbb{Q})^{f_p} \neq \emptyset$. Then, we can choose a family of points $\{Q_\ell\}_\ell$, $Q_\ell \in X_B^{(m)}(\mathbb{Q}_\ell)$ for each prime ℓ, such that there exists a global character ϕ restricting to each local character ϕ_ℓ on $\mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$. Using the moduli interpretation of $X_B^{(m)}$, write (A_ℓ, i_ℓ) for an abelian surface with real multiplication by $R_{\mathbb{Q}(\sqrt{m})}$ corresponding to each point Q_ℓ.

Now the rest of the proof is exactly as in the first part, since the hypothesis $B \in \mathcal{B}^{\mathrm{Br}}_{p,m}(q)$ implies that, for every possible choice of $\{Q_\ell\}_\ell \in X_B^{(m)}(\mathbb{A}_\mathbb{Q})$, the preimages of the point $Q_q \in X_B^{(m)}(\mathbb{Q}_q)$ are rational over a quadratic extension K_q of $\mathbb{Q}_q$ with residue field $\mathbb{F}_q$. Therefore, all the arguments apply verbatim to get the same contradiction.

□

Remark 7.32. As in Theorem 7.19, in the first statement of the theorem we can replace $\mathcal{B}_{p,m}(q)$ by $\mathcal{B}^0_{p,m}(q)$.

As explained after Theorem 7.19, [**RSY05**, Theorem 3.1] gives a criterion for deciding whether $X_B^{(m)}(\mathbb{A}_\mathbb{Q})$ is empty or not. When $X_B^{(m)}(\mathbb{A}_\mathbb{Q}) \neq \emptyset$, now statement (1) of the above theorem also gives sufficient conditions for $X_B^{(m)}$ to be a counterexample to the Hasse principle over $\mathbb{Q}$, and under the conditions of statement (2), not only $X_B^{(m)}$ is a counterexample to the Hasse principle over $\mathbb{Q}$, but moreover it is accounted for by the Brauer-Manin obstruction.

Nevertheless, note the big difference between the hypotheses in Theorem 7.19 and in Theorem 7.31. While in the former condition (M) made the hypotheses computationally inaccessible, now in the Main Theorem all the hypotheses (as for statement (1), at least) are easy to check and then we can compute lots of examples. In the following examples, we denote by X_D the Shimura curve associated to the rational quaternion algebra of reduced discriminant D.

Example 7.33. For the prime $q = 3$, one computes $P(3) = \{2, 3, 5, 11, 23\}$. Then, take $p = 19 \equiv 3 \bmod 4$, $m = 13$ and B the quaternion algebra of reduced discriminant $D = pm = 19 \cdot 13$. The Atkin-Lehner involution $\omega_m = \omega_{13}$ is checked to be twisting on $X_{19\cdot 13}$, and $B \in \mathcal{B}_{p,m}(q)$. Therefore,

$$X_{19\cdot 13}^{(13)}(\mathbb{Q}) = \emptyset.$$

Also for $q = 3$, $p = 19$, one checks for example that $m = 37$ still works, so that $X_{19\cdot 37}^{(37)}(\mathbb{Q}) = \emptyset$ as well.

Example 7.34. Now consider $q = 11$, for which

$$P(11) = \{2, 3, 5, 7, 11, 13, 17, 19, 29, 43, 59, 97, 109, 167\}.$$

If we take $p = 23 \equiv 3 \bmod 4$, $m = 5$ and B the quaternion algebra of reduced discriminant $D = pm = 23 \cdot 5$, the Atkin-Lehner involution $\omega_m = \omega_5$ is checked to be twisting on $X_{23\cdot 5}$, and $B \in \mathcal{B}_{p,m}(q)$. Therefore,

$$X_{23\cdot 5}^{(5)}(\mathbb{Q}) = \emptyset.$$

If we take $m = 37$ instead of 5, the same holds and then we also have $X_{23\cdot 37}^{(37)}(\mathbb{Q}) = \emptyset$.

Conclusions and future work

In this thesis we have combined some descent techniques from the work of Skorobogatov in [**Sko05**] together with the study of certain Galois representations attached to abelian surfaces parametrized by the quotient of a Shimura curve by a twisting Atkin-Lehner involution, after the ideas from [**Rot08**]. As a consequence, a geometric interpretation of the results in [**Rot08**] has been obtained in terms of the Hasse principle over $\mathbb{Q}$ for Atkin-Lehner quotients of Shimura curves and the Brauer-Manin obstruction.

Therefore, this interpretation follows a parallel road to the one from Jordan's work in [**Jor86**] to Skorobogatov's in [**Sko05**], since the results about non-existence of abelian surfaces with real multiplication derived from Rotger's work in [**Rot08**] are in some sense analogous to the results of Jordan. Thus, we have closed a square linking these three articles.

It is worthwhile to mention here that one of the main achievements in this work has been the role played by the extended Galois representations introduced at the end of Chapter 7. These representations allow us to prove our result about non-existence of rational points on an Atkin-Lehner quotient $X_B^{(m)}$ without any assumption about the field of definition of the abelian surfaces parametrized by it. As we have stressed along the last chapters, this has been maybe the most difficult part to solve.

From here, some interesting future work can be pointed out. First of all, the second statement in Theorem 7.31 is not as satisfactory as we would like. As well as the hypotheses regarding statement (1) are computationally very easy to check, it is not so easy to verify whether a rational quaternion algebra B belongs to $\mathcal{B}_{p,m}^{\mathrm{Br}}(q)$ or not. It seems to us that this technical condition is hardly avoidable. At least, comparing our result with Theorem 5.3 of Skorobogatov, we believe that a condition of this kind is really needed for proving our main result with the techniques we have used. However, we would like to work out this family of quaternion algebras and make it more explicit in order to get a clearer statement.

Secondly, it seems from the work in [**Rot08**] that we should expect a natural generalization of our work to higher-dimensional Shimura varieties. Indeed, the étale coverings constructed in Chapter 5 can also be defined for Atkin-Lehner quotients of Shimura varieties, so this is another path to explore. Surely, an important question for investigating this problem will be the question of when an abelian variety (of even dimension) parametrized by a higher-dimensional Shimura variety admits a model rational over its field of moduli. That is, it would be nice to try to obtain a result generalizing Theorem 4.2 of Jordan to the higher-dimensional case.

Also, note that the étale covering of an Atkin-Lehner quotient $X_B^{(m)}$ of a Shimura curve X_B constructed in Chapter 5 also works for the full Atkin-Lehner involution ω_D, where D is the reduced discriminant of B. The case of the full Atkin-Lehner involution rarely appears studied in the literature, so it would be great if these coverings could be used to get some results about non-existence of rational points on the Atkin-Lehner quotient $X_B^{(D)}$. Besides, it is also a good idea to try to use the descent methods applied in [**RSY05**] to the double covering $X_B \to X_B^{(m)}$ given by the natural projection, provided ω_m is fixed point free, but applied to our étale coverings $Z_{B,p}^{(m)} \to X_B^{(m)}$ instead.

A more ambitious goal, which is placed in a more algebro-geometric side, is to try to shed some light on Conjecture 3.15 for the case of Shimura curves and their Atkin-Lehner quotients, being the results in [**Sko05**] together with this work a starting point.

References

[AB04] M. Alsina and P. Bayer, *Quaternion orders, quadratic forms and Shimura curves*, CRM Monograph Series, vol. 22, Amer. Math. Soc., Providence, RI, 2004.

[Als00] M. Alsina, *Dominios fundamentales modulares*, Rev. R. Acad. Cienc. Exact. Fis. Nat. **94** (2000), no. 3, 309–322.

[BB66] W. L. Baily and A. Borel, *Compactification of arithmetic quotients of bounded symmetric domains*, Ann. of Math. **84** (1966), 443–507.

[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** (2006), no. 3, 383–408.

[BHC62] A. Borel and Harish-Chandra, *Arithmetic subgroups of algebraic groups*, Ann. of Math. **75** (1962), 485–535.

[BL92] C. Birkenhake and H. Lange, *Complex Abelian Varieties*, Gundl. math. Wiss., vol. 302, Springer, 1992.

[Cas71] W. Casselman, *On Abelian Varieties with Many Endomorphisms and a Conjecture of Shimura's*, Invent. Math. **12** (1971), 225–236.

[CT86] J.-L. Colliot-Thélène, *Surfaces cubiques diagonales*, Séminaire de Théorie des Nombres de Paris 1984-1985, Progress in Math., vol. 63, Birkhäuser, 1986, pp. 51–66.

[Del71] P. Deligne, *Travaux de Shimura*, Séminaire Bourbaki, 23ème année (1970/71), Exp. No. 389, Lecture Notes in Math., vol. 244, Springer, 1971, pp. 123–165.

[Del77] ———, *Cohomologie étale*, Lect. Notes Math., vol. 569, Springer-Verlag, 1977, Séminaire de Géométrie Algébrique du Bois-Marie SGA $4\frac{1}{2}$, avec la collaboration de J. F. Boutot, A. Grothendieck, L. Illusie et J. L. Verdier.

[Dem09] C. Demarche, *Obstruction de descente et obstruction de Brauer-Manin étale*, Algebra and Number Theory **3** (2009), no. 2, 237–254.

[Gro68] A. Grothendieck, *Le Groupe de Brauer III. Àlgebres d'Azumaya et interprétations diverses*, Dix Exposés sur la Cohomologie des Schémas (Amsterdam), North-Holland, 1968, pp. 88–188.

[GS06] P. Gille and T. Szamuely, *Central Simple Algebras and Galois Cohomology*, Cambridge University Press, 2006.

[Har77] R. Hartshorne, *Algebraic Geometry*, GTM, vol. 52, Springer, 1977.

[JL85] B. Jordan and R. Livné, *Local diophantine properties of Shimura curves*, Math. Ann. **270** (1985), 235–248.

[Jor81] B. W. Jordan, *On the Diophantine Arithmetic of Shimura curves*, PhD Thesis, Harvard University, 1981.

[Jor86] ———, *Points on Shimura curves rational over number fields*, J. Reine Angew. Math. **371** (1986), 92–114.

[Kat92] S. Katok, *Fuchsian Groups*, Chicago Lectures in Mathematics, The University of Chicago Press, 1992.

[Mas77] W. S. Massey, *Algebraic Topology: An Introduction*, GTM, vol. 56, Springer, 1977.

[Maz78] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.

[Mil79] J. S. Milne, *Points on Shimura varieties mod p*, Proc. Symp. Pure Math. **33** (1979), 165–184.

[Mil80] ———, *Étale cohomology*, PMS, vol. 33, Princeton University Press, 1980.

[Mil08] ———, *Abelian varieties (v2.00)*, 2008, Available at www.jmilne.org/math/.

[Mol10] S. Molina, *Equations of hyperelliptic Shimura curves*, 2010, submitted.

[Mor81] Y. Morita, *Reduction modulo $\mathfrak{P}$ of shimura curves*, Hokkaido Math. J. **10** (1981), 209–238.

[Mum70] D. Mumford, *Abelian Varieties*, Oxford University Press, 1970.

[Neu99] J. Neukirch, *Algebraic Number Theory*, Gundl. math. Wiss., vol. 322, Springer, 1999.

[Ogg83] A. P. Ogg, *Real points on Shimura curves*, Arithmetic and geometry, Progress in Math., vol. 35, Birkäuser, 1983, pp. 277–307.

[Pie82] R. S. Pierce, *Associative Algebras*, GTM, vol. 88, Springer-Verlag, 1982.

[Poo] B. Poonen, *Rational points on varieties*, Course notes 2003/2008, available at http://math.mit.edu/˜poonen/.

[Poo06] ———, *Heuristics for the Brauer-Manin obstruction for curves*, Experimental Math. **15** (2006), no. 4, 415–420.

[Poo10] ———, *Insufficiency of of the Brauer-Manin obstruction applied to étale covers*, Ann. of Math. **171** (2010), no. 3, 2157–2169.

[PV04] B. Poonen and F. Voloch, *Random Diophantine equations*, Arithmetic of higher-dimensional algebriac varieties (Palo Alto, CA, 2002), 2004, pp. 175–184.

[Pyl02] E. Pyle, *Abelian varieties over $\mathbb{Q}$ with large endomorphism algebras and their simple components over $\bar{\mathbb{Q}}$*, Modular curves and abelian varieties (J. Cremona, J.-C. Lario, J. Quer, and K. Ribet, eds.), Progress in Math., vol. 224, Birkhäuser, 2002, pp. 189–239.

[Rib76] K. A. Ribet, *Galois action on division points of abelian varieties with real multiplications*, Amer. J. Math. **98** (1976), no. 3, 751–804.

[Rib81] ———, *Endomorphism algebras of abelian varieties attached to newforms of weight 2*, Progress in Math. **12** (1981), 263–276.

[Rib92] ———, *Abelian varieties over $\mathbb{Q}$ and modular forms*, Algebra and Topology 1992 (Taejŏn), 53-79, Korea Adv. Inst. Sci. Tech., Taejŏn (1992), Reprinted on *Modular curves and abelian varieties*, 241-261, Progress in Math. 224, Birkhäuser, 2002.

[Rot03] V. Rotger, *Quaternions, polarizations and class numbers*, J. Reine Angew. Math. **561** (2003).

[Rot04a] ———, *The field of moduli of quaternionic multiplication on abelian varieties*, International J. Math. M. Sc. **52** (2004), 2795–2808.

[Rot04b] ———, *Modular Shimura varieties and forgetful maps*, Trans. Amer. Math. Soc. **356** (2004), 1535–1550.

[Rot08] ———, *Which quaternion algebras act on a modular abelian variety?*, Math. Res. Letters **15** (2008), 251–263.

[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** (2005), no. 2, 463–476.

[Ser72] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.

[Ser73] ———, *A course in arithmetic*, GTM, vol. 7, Springer-Verlag, 1973.

[Shi63] G. Shimura, *On analytic families of polarized abelian varieties and automorphic functions*, Ann. of Math. **78** (1963), 149–192.

[Shi67] ———, *Construction of class fields and zeta functions of algebraic curves*, Ann. of Math. **85** (1967), 58–159.

[Shi72] ———, *On the field of rationality for an abelian variety*, Nagoya Math. J. **45** (1972), 161–178.

[Shi75] ———, *On the real points of an arithmetic quotient of a bounded symmetric domain*, Math. Ann. **215** (1975), 259–331.

[Sij10] J. Sijsling, *Equations for arithmetic pointed tori*, PhD Thesis, 2010.

[Sil92] A. Silverberg, *Fields of definition for homomorphisms of abelian varieties*, J. Pure Appl. Algebra **77** (1992), 253–262.

[Sko99] A. Skorobogatov, *Beyond the Manin obstruction*, Invent. Math. **135** (1999), no. 2, 399–424.

[Sko01] ———, *Torsors and Rational Points*, Cambridge Tracts in Mathematics, vol. 144, Cambridge University Press, 2001.

[Sko05] ———, *Shimura coverings of Shimura curves and the Manin obstruction*, Math. Res. Lett. **12** (2005), no. 5-6, 779–788.

[Sko09] ———, *Descent obstruction is equivalent to étale Brauer-Manin obstruction*, Math. Ann. **344** (2009), 501–510.

[SS03] S. Siksek and A. Skorobogatov, *On a shimura curve that is a counterexample to the Hasse principle*, Bull. London Math. **35** (2003), 409–414.

[ST61] G. Shimura and Y. Taniyama, *Complex Multiplication of Abelian Varieties and its Application to Number Theory*, Math. Soc. Japan, Tokio, 1961.

[ST68] J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math. **88** (1968), 492–517.

[SY04] A. Skorobogatov and A. Yafaev, *Descent on certain Shimura curves*, Israel J. Math. **140** (2004), 319–332.

[Sza09] T. Szamuely, *Galois Groups and Fundamental Groups*, Cambridge Studies in Advanced Mathematics, vol. 117, Cambridge University Press, 2009.

[Vig80] M.-F. Vignéras, *Arithmétique des algèbres de quaternions*, Lect. Notes Math., vol. 800, Springer, 1980.

[Wei56] A. Weil, *The field of definition of a variety*, Amer. J. Math. **78** (1956), 509–524.