UNIVERSITAT DE BARCELONA

Images of Galois representations and *p*-adic models of Shimura curves

Laia Amorós Carafí

PhD-FSTC-2016-59
Faculty of Sciences, Technology and Communication

Facultat de Matemàtiques i Informàtica
Departament d'Àlgebra i Geometria

DISSERTATION

Defense held on 16/12/2016 in Luxembourg
to obtain the degree of

DOCTEUR DE L'UNIVERSITÉ DU LUXEMBOURG EN MATHÉMATIQUES

AND

DOCTORA PER LA UNIVERSITAT DE BARCELONA EN MATEMÀTIQUES

by

Laia AMORÓS CARAFÍ
Born on 1 February 1989 in Barcelona (Spain)

IMAGES OF GALOIS REPRESENTATIONS AND p-ADIC MODELS OF SHIMURA CURVES

Dissertation defense committee

Dr Gabor WIESE, dissertation supervisor
Professor, Université du Luxembourg

Dr Pilar BAYER, dissertation supervisor
Professor, Universitat de Barcelona

Dr David KOHEL, reporter
Professor, Université d'Aix Marseille

Dr Xavier GUITART, reporter
Universitat de Barcelona

Dr Martin SCHLICHENMAIER, Chairman
Professor, Université du Luxembourg

Dr Sara ARIAS DE REYNA, Vice Chairman
Universidad de Sevilla

Introduction

The Langlands program is a vast and unifying network of conjectures that connect the world of automorphic representations of reductive algebraic groups and the world of Galois representations. These conjectures associate an automorphic representation of a reductive algebraic group to every n-dimensional representation of a Galois group, and the other way around: they attach a Galois representation to any automorphic representation of a reductive algebraic group. Moreover these correspondences are done in such a way that the automorphic L-functions attached to the two objects coincide.

The theory of modular forms is a field of complex analysis whose main importance lies on its connections and applications to number theory. We will make use, on the one hand, of the arithmetic properties of modular forms to study certain Galois representations and their number theoretic meaning. On the other hand, we will use the geometric meaning of these complex analytic functions to study a natural generalisation of modular curves. A modular curve is a geometric object that parametrises isomorphism classes of elliptic curves together with some additional structure depending on some modular subgroup. The generalisation that we will be interested in are the so called Shimura curves. We will be particularly interested in their p-adic models.

In this thesis we treat two different topics, one in each side of the Langlands program. In the Galois representations' side, we are interested in Galois representations that take values in local Hecke algebras attached to modular forms over finite fields. In the automorphic forms' side, we are interested in Shimura curves: we develop some arithmetic results in definite quaternion algebras and give some results about Mumford curves covering p-adic Shimura curves.

By a theorem of Deligne, Deligne-Serre and Shimura, we know that one can attach, to any normalised eigenform $f \in S_2(N, \varepsilon; \overline{\mathbb{F}}_p)$, an odd semisimple 2-dimensional continuous Galois representation of the absolute Galois group $G_{\mathbb{Q}}$ of the field of rational numbers. And moreover, since Khare, Wintenberger and others proved Serre's modularity conjecture ([KW09a], [KW09b]), we know that the converse is also true, i.e. irreducible odd Galois representations over $\overline{\mathbb{F}}_p$ come from modular forms in a very concrete way. The properties that the coefficients of modular forms enjoy have been exploited since the time of Jacobi and Eisenstein, later on by Ramanujan, and continue to be nowadays. One can be interested in finding, for example, the congruences that may appear among them modulo some prime. Just to give an example, in [Ram16] Ramanujan defined his *tau function* $\tau(n)$, which turns out to describe the coefficients of a cusp form of weight 12 and level 1, and conjectured that $\tau(n) \equiv \sigma_{11}(n) \bmod 691$, where $\sigma_k(n)$ denotes the sum of the k-th powers of the positive divisors of n. Ramanujan also conjectured many other congruences, which were not proven until a few years later.

It is well-known that local mod p Hecke algebras govern mod p congruences of normalised Hecke eigenforms. One of the aims of this thesis is to study the Galois representations with values in these Hecke algebras in order to have a better understanding of these congruences. To be more specific, suppose that we have two different normalised Hecke eigenforms $f, g \in \mathrm{S}_k(N;\mathbb{C})$ of weight k, level N and trivial character (just for the simplicity of exposition), and denote by $\mathbb{T}_{\mathbb{Z}} \subseteq \mathrm{End}_{\mathbb{C}}(\mathrm{S}_k(N;\mathbb{C}))$ the subring generated by the Hecke operators T_n with $(n, Np) = 1$ (which is a $\mathbb{Z}$-module). Consider the residual Hecke algebra $\mathbb{T}_{\mathbb{F}_p} := \mathbb{T}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{F}_p$. Then the failure of the mod p Hecke algebra $\mathbb{T}_{\mathbb{F}_p}$ of being semisimple can be a consequence of three phenomena ([MW11]): congruences between $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-conjugacy classes of newforms, ramification at p of the coefficient fields of newforms and the p-index of the local coefficient ring in the ring of integers of the local coefficient field being greater than 1. The consequences of the first phenomenon will be extensively studied in chapter 3 of this thesis.

Let $f(z) = \sum_{n=0}^{\infty} a_n(f)q^n \in \mathrm{S}_k(N;\mathbb{C})$ be a normalised Hecke eigenform, whose coefficients lie in some ring of integers $\mathcal{O}$ of a number field. Let $\overline{\rho}_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ denote the attached mod p Galois representation, which is semisimple and uniquely determined by the coefficients of f mod p, for primes $\ell \nmid Np$, and let $\mathbb{F}_q$ be the finite field generated by the $a_\ell(f)$ mod $\mathfrak{P}$, where $\mathfrak{P}$ denotes a prime above p in $\mathcal{O}$. Let $\overline{\mathbb{T}} \subseteq \mathbb{T}_{\mathbb{F}_q}$ denote the subalgebra generated by the operators T_ℓ with $\ell \nmid Np$. Consider the ring homomorphism

$$\begin{array}{rccl} \overline{\lambda}_f : & \overline{\mathbb{T}} & \to & \mathbb{F}_q \\ & T_n & \mapsto & a_n(f) \bmod p \end{array}$$

and let $\mathfrak{m}_f := \ker(\overline{\lambda}_f)$, which is a maximal ideal of $\overline{\mathbb{T}}$. We denote by $\overline{\mathbb{T}}_{\mathfrak{m}_f}$ the localisation of $\overline{\mathbb{T}}$ at $\mathfrak{m}_f$. Then $\overline{\mathbb{T}}_{\mathfrak{m}_f}$ is a commutative local finite-dimensional $\mathbb{F}_q$-algebra and, if moreover we assume that the residual Galois representation $\overline{\rho}_f$ is absolutely irreducible then, by Theorem 3 in [Car94], we have a continuous Galois representation

$$\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{T}}_{\mathfrak{m}_f})$$

such that $\overline{\rho}_f = \pi \circ \rho_f$, where π extends the natural projection $\pi : \overline{\mathbb{T}}_{\mathfrak{m}_f} \to \mathbb{F}_q$. In this setting, one is naturally interested in knowing the image of ρ_f. In chapters 2 and 3 we will see how to compute this image from the knowledge of the image of $\overline{\rho}_f$ and some additional conditions.

Another important application of these mod p Hecke algebras is that they can give us information on some abelian extensions of number fields. The Galois representations that we investigate correspond to abelian extensions of very big non-solvable number fields that standard methods do not allow to treat computationally. In chapter 4 we will see that the methods on group extensions that we develop in the previous chapters allow us to make these extensions (partially) accessible.

On the other side of the Langlands program one is led to consider Shimura curves, a natural generalisation of the classical modular curves. These algebraic curves and their arithmetic power were studied by Shimura in the 60s, leaning on previous works of Fricke, Klein and Poincaré. In the second part of this manuscript we will be dealing with Shimura curves and their uniformisations.

Just like modular curves, Shimura curves admit complex and p-adic uniformisations. Although the complex uniformisation of Shimura curves is more difficult to approach computationally due to their lack of cusps, several recent works have sorted out this difficulty and made such computations more amenable (see, for example, [AB04], [BT07], [BT08], [Nua15], [Voi06] and [VW11]). The

theory of p-adic uniformisation of Shimura curves has its basis in the fundamental theorems of Čerednik in [Cer76] and Drinfel'd in [Dri76]. These non-archimedean uniformisations describe p-adic integral models of Shimura curves associated to indefinite quaternion algebras of discriminant Dp, together with its bad special fibre, using the language of rigid analytic geometry. There are also some works that take a computational approach to the p-adic uniformisation of Shimura curves through the computation of their special points, for example [DP06], [Gre06] and [Gre09]. Recent results in this direction can be found in [FM14], where the authors give an algorithm to compute the reduction-graph with lengths of a Shimura curve associated to an arbitrary Eichler order.

In the second part of this thesis we will give some results about these p-adic uniformisations that hold for some infinite families of Shimura curves and that are approachable from a computational point of view. Our results have two sources of inspiration. The first one is the classical work of Hurwitz from 1896 ([Hur96]), where he introduces the Hurwitz quaternions and proves a unique factorisation result in analogy to that of the Gaussian integers. With this uniqueness he is then able to prove the well-known formula for the number of representations of a nonnegative integer as a sum of four squares. The second one is the more recent work of Gerritzen and van der Put [GvdP80], where they study Mumford curves covering Shimura curves of discriminant $2p$ and level $N = 1$. The combination and generalisation of these two works lead us to the study of the p-adic uniformisation of some families of Shimura curves through the study of certain Mumford curves covering them. More concretely, we will consider Shimura curves $X(Dp, N)$ of discriminant Dp and level N such that the associated Eichler order of level N inside the definite quaternion algebra of discriminant D has one-sided ideal class number $h(D, N)$ equal to 1.

Let $G \subseteq \mathrm{PGL}_2(\mathbb{Q}_p)$ be a discontinuous and finitely generated group. Then it is possible to find a normal subgroup $\Gamma \subseteq G$ of finite index which is torsion-free. In particular, this subgroup Γ is a p-adic Schottky group. The importance of p-adic Schottky groups lies in the fact that they provide the p-adic uniformisation of Mumford curves. Given a Schottky group $\Gamma \subseteq \mathrm{PGL}_2(\mathbb{Q}_p)$, Mumford shows how to attach to it a Mumford curve $\mathcal{C}_\Gamma$ (cf. Theorem 3.3 and Corollary 4.11 of [Mum72]). The curve $\mathcal{C}_\Gamma$ is uniquely determined, up to isomorphism, by the conjugacy class of the Schottky group inside $\mathrm{PGL}_2(\mathbb{Q}_p)$. In particular, when this Schottky group is a cocompact group, the stable reduction-graph of $\mathcal{C}_\Gamma$, with respect to the stable model associated to Γ, is the finite graph $\Gamma \setminus \mathcal{T}_p$, where $\mathcal{T}_p$ denotes the Bruhat-Tits tree associated to $\mathrm{PGL}_2(\mathbb{Q}_p)$.

The theorem of Čerednik-Drinfel'd provides a way to describe the set of $\mathbb{Q}_{p^2}$-points of the algebraic curve $X(Dp, N)$ as a quotient of the p-adic upper half-plane $\mathcal{H}_p$ by the action of a discrete cocompact subgroup $\Gamma_{p,+} \subseteq \mathrm{PGL}_2(\mathbb{Q}_{p^2})$. Moreover, the reduction-graph of the special fibre of the Drinfel'd integral model is the quotient graph $\Gamma_{p,+} \setminus \mathcal{T}_p$. Thus the theory of p-adic uniformisation of Shimura curves leads us to consider certain discrete and cocompact subgroups of $\mathrm{PGL}_2(\mathbb{Q}_p)$. The problem is that, in general, these groups are no longer torsion-free. Nevertheless, as said before it is possible to find a normal subgroup which is torsion-free. Moreover, by Satz 1 in [Ger74], we know that one can always find a system of generators for a Schottky group Γ in such a way that there exists a *good* fundamental domain for Γ with respect to this system. In [MR15] they show how to find, computationally, generators *in good position* for any Schottky group. The main aim of the second part of this thesis is to present a result in this setting that shows, in a very concrete way, how to find explicit generators for these Schottky groups using modular arithmetic in the definite quaternion algebra attached to the Shimura curve in question. Moreover we will do it in such a way that it will allow us to easily describe the stable reduction-graph of the Mumford curve covering

the p-adic Shimura curve.

We now make an outline of the thesis and summarise the important results.

In the first part of this document we will exhibit how a close study of mod p local Hecke algebras allows us to obtain results about the image of certain Galois representations with values in local mod p Hecke algebras. Moreover, this leads us to deduce the existence of p-elementary abelian extensions of big number fields, which are not computationally approachable so far.

Chapter 1 is an introductory chapter for the first part of the thesis. It is divided in three sections. We start by giving a short introduction to the theory of mod p Hecke algebras and modular forms. Afterwards we explain how via Carayol's result in [Car94] one can attach a Galois representation ρ_f to a local mod p Hecke algebra $\overline{\mathbb{T}}_f$ over some finite field $\mathbb{F}_q$ of characteristic p, under the assumption that the residual Galois representation $\overline{\rho}_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_q)$ is absolutely irreducible. Finally, since we are interested in computing the image of ρ_f, we include a section about images of residual Galois representations.

In chapter 2 we extend a result of J. Manoharmayum in [Man15] to subgroups of $\mathrm{GL}_n(A)$, where A denotes a complete local noetherian ring with finite residue field k. More concretely, let $W(k)$ denote the ring of Witt vectors of a finite field k of characteristic p. Let $T : k \hookrightarrow W(k)$ denote the Teichmüller lift and let $W(k)_A$ denote the image of the natural local homomorphism $\iota : W(k) \to A$. For a subgroup $D \subseteq \mathbb{F}_q^\times$ we consider the following groups:

$$\mathrm{GL}_n^D(W(k)_A) := \{g \in \mathrm{GL}_n(W(k)_A) \mid \det(g) \in \iota(T(D))\},$$

$$\mathrm{GL}_n^D(\mathbb{F}_q) := \{g \in \mathrm{GL}_n(\mathbb{F}_q) \mid \det(g) \in D\}.$$

Using similar technics as in [Man15], we prove the following result.

Theorem. *Let $(A, \mathfrak{m}_A)$ be a complete local noetherian ring with maximal ideal $\mathfrak{m}_A$ and finite residue field $A/\mathfrak{m}_A$ of characteristic p. Let $\pi : A \to A/\mathfrak{m}_A$ denote the natural projection. Suppose that we are given a subfield k of $A/\mathfrak{m}_A$ and a closed subgroup G of $\mathrm{GL}_n(A)$. Assume that the cardinality of k is at least 4 and that $k \neq \mathbb{F}_5$ if $n = 2$ and $k \neq \mathbb{F}_4$ if $n = 3$. Suppose that $\pi(G) \supseteq \mathrm{GL}_n^D(k)$. Then G contains a conjugate of $\mathrm{GL}_n^D(W(k)_A)$.*

This result turns out to be very useful for our purposes, since as a consequence we obtain the following corollary, which we strongly use in chapter 3.

Corollary. *Let k be a finite field of characteristic p with cardinality at least 4, $k \neq \mathbb{F}_5$ if $n = 2$ and $k \neq \mathbb{F}_4$ if $n = 3$. Let $(A, \mathfrak{m}_A)$ be a finite-dimensional commutative local k-algebra with residue field k and $\mathfrak{m}_A^2 = 0$. Let $G \subseteq \mathrm{GL}_n^D(A)$ be a subgroup. Suppose that $G \mod \mathfrak{m}_A = \mathrm{GL}_n^D(k)$. Then there exists an $\mathbb{F}_p[\mathrm{GL}_n^D(k)]$-submodule $M \subseteq \mathrm{M}_n^0(\mathfrak{m}_A)$ such that G is, up to conjugation by an element $u \in \mathrm{GL}_n(A)$ with $\pi(u) = 1$, a (non-twisted) semidirect product of the form*

$$G \simeq M \rtimes \mathrm{GL}_n^D(k).$$

In chapter 3 we study continuous odd Galois representations

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T})$$

where $(\mathbb{T}, \mathfrak{m})$ denotes a finite-dimensional local commutative algebra over a finite field $\mathbb{F}_q$ of characteristic p, equipped with the discrete topology and with $\mathbb{F}_q$ as residue field. The residual representations $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ of these Galois representations are well-studied and, after Serre's modularity theorem, one can attach to the irreducible odd ones a normalised eigenform of certain prescribed level, weight and character. One can also compute explicitly the image of these residual representations (see for example [Ann13]). We will be particularly interested in the case $\mathrm{Im}(\overline{\rho}) = \mathrm{GL}_2^D(\mathbb{F}_q)$, where $D \subseteq \mathbb{F}_q^\times$ indicates the image of the determinant of $\overline{\rho}$. Let $\mathrm{M}_2^0(\mathbb{F}_q)$ denote the trace 0 matrices with coefficients in $\mathbb{F}_q$. In this situation, we prove the following result.

Theorem. *Let $\mathbb{F}_q$ denote a finite field of characteristic p and $q = p^d$ elements, and suppose that $q \neq 2, 3, 5$. Let $(\mathbb{T}, \mathfrak{m}_{\mathbb{T}})$ be a finite-dimensional local commutative $\mathbb{F}_q$-algebra equipped with the discrete topology, and with residue field $\mathbb{T}/\mathfrak{m} \simeq \mathbb{F}_q$. Suppose that $\mathfrak{m}^2 = 0$. Let Γ be a profinite group and let $\rho : \Gamma \to \mathrm{GL}_2(\mathbb{T})$ be a continuous representation such that*

(*a*) $\mathrm{Im}(\rho) \subseteq \mathrm{GL}_2^D(\mathbb{T})$, *where $D \subseteq \mathbb{F}_q^\times$ is a subgroup.*

(*b*) $\mathrm{Im}(\overline{\rho}) = \mathrm{GL}_2^D(\mathbb{F}_q)$, *where $\overline{\rho}$ denotes the reduction $\rho \bmod \mathfrak{m}$.*

(*c*) *$\mathbb{T}$ is generated as $\mathbb{F}_q$-algebra by the set of traces of ρ.*

Let $m := \dim_{\mathbb{F}_q} \mathfrak{m}$ and let t be the number of different traces in $\mathrm{Im}(\rho)$.

(*i*) *If $p \neq 2$, then $t = q^{m+1}$ and*

$$\mathrm{Im}(\rho) \simeq (\underbrace{\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}_{m}) \rtimes \mathrm{GL}_2^D(\mathbb{F}_q) \simeq \mathrm{GL}_2^D(\mathbb{T}).$$

(*ii*) *If $p = 2$, then*

$$t = q^\alpha \cdot ((q-1)2^\beta + 1), \text{ for some unique } 0 \leq \alpha \leq m \text{ and } 0 \leq \beta \leq d(m-\alpha),$$

and in this case $\mathrm{Im}(\rho) \simeq M \rtimes \mathrm{SL}_2(\mathbb{F}_q)$, where M is an $\mathbb{F}_2[\mathrm{SL}_2(\mathbb{F}_q)]$-submodule of $\mathrm{M}_2^0(\mathfrak{m})$ of the form

$$M \simeq \underbrace{\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}_{\alpha} \oplus \underbrace{C_2 \oplus \cdots \oplus C_2}_{\beta},$$

where $C_2 \subseteq \mathbb{S}$ is a subgroup with 2 elements of the scalar matrices. Moreover, M is determined uniquely by t up to isomorphism.

We apply this theorem to concrete examples coming from modular forms and summarise the results in some tables. A closer look at these tables allows us to state some conjectures about the images of the corresponding Galois representations $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{T}}_{\mathfrak{m}_f})$ coming from mod 2 modular forms.

In chapter 4 we translate the previous results into results on the arithmetic of certain p-elementary abelian field extensions. The explicit description that we give in chapter 3 of the image of $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T})$ allows us to compute a certain part of a certain ray class field of the field K cut out by $\overline{\rho}$. In particular, for characteristic $p \neq 2$ we prove that K admits a p-elementary abelian extension of degree p^{3dm}, where d denotes the degree of $\mathbb{F}_q$ and $m = \dim_{\mathbb{F}_q} \mathfrak{m}/\mathfrak{m}^2$. When the characteristic is $p = 2$, we prove that K admits a 2-elementary abelian extension of degree $2^{3d\alpha+\beta}$,

where α and β depend on the number of different traces of $\mathrm{Im}(\rho)$, as explained in the previous theorem.

Finally, in this chapter we include a section on some natural questions that arise in this context, and that indicate a direction for further research.

Part II is the continuation of a joint work with Piermarco Milione, started in his thesis [Mil16], also under the direction of Professor Pilar Bayer, and an adapted version of that can be found in [AM16]. In this part we give an explicit description of fundamental domains associated to the p-adic uniformisation of families of Shimura curves of discriminant Dp and level $N \geq 1$, for which $h(D, N) = 1$.

In chapter 5 we introduce the p-adic upper half-plane and the Bruhat-Tits tree together with the reduction map identifying it with the reduction of this rigid analytic variety. We also summarise the results of the theory of Mumford curves that we need for the rest of the chapters and relate these to the theory of p-adic uniformisation of Shimura curves.

In chapter 6 we briefly introduce the theory of arithmetic of quaternion algebras. We develop some tools on the modular arithmetic of Eichler orders $\mathcal{O}$ over $\mathbb{Z}$ with $h(D, N) = 1$ in a definite quaternion algebra H. We are particularly interested in quotients of the form $\mathcal{O}/\xi\mathcal{O}$, where $\xi\mathcal{O}$ is an integral principal right ideal. We extend the notion of *primary quaternion* introduced in [Hur96] for the order of Hurwitz quaternions to Eichler orders $\mathcal{O}$ over $\mathbb{Z}$ with $h(D, N) = 1$. This notion turns out to be crucial in order to prove a unique factorisation result in these Eichler orders, a result that extends the *Zerlegungsatz* for the Hurwitz quaternions. Indeed, once a quaternion $\xi \in \mathcal{O}$ satisfying certain property (what we call the *right-unit property*, cf. Definition 6.2.5) is fixed, any quaternion $\alpha \in \mathcal{O}$ is associated to a unique ξ-primary quaternion (cf. Definition 6.2.3), i.e. there exists a unique unit (up to sign if $2 \in \xi\mathcal{O}$) $\varepsilon \in \mathcal{O}^\times$ such that $\varepsilon\alpha$ is ξ-primary. This fact allows us to focus only on the factorisation of ξ-primary quaternions, and we are able to prove the following result.

Theorem. *Let H be a definite quaternion algebra of discriminant D and let $\mathcal{O}$ be an Eichler order over $\mathbb{Z}$ of level N with $h(D, N) = 1$. Let $\xi \in \mathcal{O}$ be an integral quaternion such that the abelian quotient group $\mathcal{O}/\xi\mathcal{O}$ contains a ξ-primary class set $\mathcal{P}$. Let $\alpha \in \mathcal{O}$ be a primitive and ξ-primary quaternion with respect to $\mathcal{P}$ such that its norm has a decomposition in prime factors*

$$\mathrm{Nm}(\alpha) = p_1 \cdot \ldots \cdot p_s.$$

Then α admits a decomposition in primitive irreducible and ξ-primary quaternions with respect to $\mathcal{P}$:

$$\alpha = \pi_1 \cdot \ldots \cdot \pi_s$$

with $\mathrm{Nm}(\pi_i) = p_i$, for every $1 \leq i \leq s$. Moreover, if $2 \notin \xi\mathcal{O}$ this decomposition is unique and, if $2 \in \xi\mathcal{O}$, the decomposition is unique up to sign.

This theorem will be very useful in chapter 7, where we will find generators for the Schottky groups arising from the p-adic uniformisation of Shimura curves.

In chapter 7 we apply the arithmetic results obtained in the previous chapter to prove the main result of this part of the thesis. This result gives a concrete and explicit way to find generators for certain Schottky groups arising from p-adic quaternion groups that uniformise p-adic Shimura

curves. The main results of this chapter (Theorem 7.1.5 and Corollary 7.2.3) can be summarised in the following statement.

Theorem. *Let $X(Dp, N)$ be the Shimura curve associated to an Eichler order of level N inside the indefinite quaternion algebra of discriminant Dp, and let $\mathcal{O}$ be an Eichler order of level N inside the definite quaternion algebra of discriminant D. Assume that*

(*i*) $h(D, N) = 1$.

(*ii*) *There exists $\xi \in \mathcal{O}$ such that $2 \in \xi\mathcal{O}$ and the map*

$$\varphi : \mathcal{O}^\times/\mathbb{Z}^\times \to (\mathcal{O}/\xi\mathcal{O})_r^\times, \quad \varphi(u) = \lambda_r(u + \mathrm{Nm}(\xi)\mathcal{O})$$

is a bijection, where $(\mathcal{O}/\xi\mathcal{O})_r^\times$ denotes the image of $(\mathcal{O}/\mathrm{Nm}(\xi)\mathcal{O})^\times$ under the natural projection $\lambda_r : \mathcal{O}/\mathrm{Nm}(\xi)\mathcal{O} \twoheadrightarrow \mathcal{O}/\xi\mathcal{O}$.

(*iii*) *The prime p satisfies*

$$t(p) := \#\{\alpha \in \mathcal{O} \mid \mathrm{Nm}(\alpha) = p,\, \alpha - 1 \in \xi\mathcal{O},\, \mathrm{Tr}(\alpha) = 0\} = 0.$$

Then there exists a Mumford curve C covering the p-adic Shimura curve $X(Dp, N) \otimes_{\mathbb{Q}} \mathbb{Q}_p$ such that:

(*a*) *the curve C has genus $(p + 1)/2$,*

(*b*) *the degree of the cover is $\#\mathcal{O}^\times/\mathbb{Z}^\times$,*

(*c*) *a finite set of generators for the Schottky group uniformising the Mumford curve C is given by the image, inside $\mathrm{PGL}_2(\mathbb{Q}_p)$, of the set of matrices*

$$\widetilde{S} := \Phi_p(\{\alpha \in \mathcal{O} \mid \mathrm{Nm}(\alpha) = p,\, \alpha - 1 \in \xi\mathcal{O}\}) \subseteq \mathrm{GL}_2(\mathbb{Q}_p),$$

where Φ_p denotes a matrix immersion of the definite quaternion algebra inside $\mathrm{M}_2(\mathbb{Q}_p)$.

In Table 6.1 we exhibit a quaternion $\xi \in \mathcal{O}$ satisfying condition (*ii*) for all definite quaternion algebras with $h(D, N) = 1$, except for the cases $(D, N) = (2, 5)$ and $(7, 1)$, for which this quaternion does not exist.

It is interesting to remark that point (*a*) of the theorem is a consequence of a result that we prove concerning the number of representations of the prime p by a quaternary quadratic form with some congruence conditions on the coefficients.

Theorem. *Let $\xi \in \mathcal{O}$ be a quaternion that satisfies condition (ii) of the previous theorem. Then the finite set*

$$\{\alpha \in \mathcal{O} \mid \mathrm{Nm}(\alpha) = p,\, \alpha - 1 \in \xi\mathcal{O}\}$$

has cardinality $2(p + 1)$.

Using these results we are able to construct good fundamental domains for the associated Mumford curves and, consequently, to obtain also the stable reduction-graph for these curves.

In chapter 8 we show how the detailed study that we did of the p-adic Shimura curve as a rigid analytic variety allows us to easily obtain formulas that describe the reduction-graph with lengths of these Shimura curves, as well as formulas for their genus and for the genus of certain Atkin-Lehner quotients.

Finally in chapter 9 we describe an algorithm that we have implemented in Magma to compute the reduction-graphs described before, in order to make our method effective. We show how to compute, in concrete examples, a free system of generators for a Schottky group as in the theorem above, a p-adic good fundamental domain for the action of the Schottky group on $\mathcal{H}_p$, and its stable reduction-graph.

Acknowledgments

This thesis is the result of a co-tutelle between the Université du Luxembourg and the Universitat de Barcelona. I would like to thank first of all my two advisors for their guidance and support during these years. Thanks Gabor, for giving me the chance to learn more about this beautiful area of mathematics, for all the time, for sharing ideas and thoughts, and for sharing lunch and even some dinner. Gràcies Pilar, per tots aquests anys en que m'has ajudat a descobrir aquest món meravellós de la teoria de nombres, per les llargues converses al teu despatx, on tot sembla tenir un sentit que va més enllà de les matemàtiques i s'enllaça amb la física, la música i la filosofia.

I would also like to thank all the former and current members of the Number Theory group in Luxembourg, for the nice seminars that we shared, for the discussions and for sharing lunch together. Un agradecimiento especial a Sara, por leer y comentar partes inacabadas de la tesis, y por las charlas sobre matemáticas que me ayudaron a aclarar algunas ideas.

I extend my thanks to all my mathematician friends and colleagues in Luxembourg. Among many, I would like to mention Anna, Christian, Diu, Héctor, Janne, Maurizia, Sasha and Tiffany. I really enjoyed sharing these years with you, you made my stay in Luxembourg much more interesting and fun. Janne, it was a pleasure to share the office with you.

M'agradaria donar les gràcies també al Seminari de Teoria de Nombres de Barcelona UB-UPC-UAB, per compartir cada any aquesta passió per les matemàtiques. En particular me gustaría agradecer a Luis Dieulefait, por alguna que otra conversación interesante cuando ha habido ocasión.

Un agradecimiento especial va sin duda a Piermarco, mi compañero de tesis en Barcelona y gran amigo, por los (muchos) buenos momentos que hemos pasado juntos, con o sin matemáticas, y sin el cual esta tesis habría quedado coja.

Vull donar les gràcies a les meves matemàtiques preferides, Celia, Elba i Marta. Amb vosaltres va començar tot, i us vull agrair de tot cor que seguim estant juntes des de la distància després de tants anys. També faig extensiu l'agraiment al David i al Gerard, per la vostra ajuda quan vaig començar aquest doctorat a Luxemburg, i juntament amb la Mireira us agraeixo per compartir cafès, dinars i sopars quan estava per Barcelona, i per les converses tan interessants que sempre tenim, no només de matemàtiques.

Finalment vull donar les gràcies a la meva família. Al meu pare i a la meva mare pel seu suport i per haver-me animat sempre a estudiar i fer el que més m'agrada. A l'Olga, al Pol i al Marc, que

sé que sempre puc comptar amb vosaltres quan us necessito. Al Gerard i a l'Aïda, per haver-me ajudat a començar aquest doctorat.

Per acabar, vull agrair a l'Albert que m'hagi acompanyat en aquest viatge. Gràcies pel teu suport, per les llargues converses malgrat la distància i per la teva visió no-matemàtica del món. I perquè tot i els quilòmetres que ens separen hem aconseguit passar molt temps junts.

Contents

Part I

Images of Galois representations with values in mod p Hecke algebras

Chapter 1

Introduction to Galois representations on mod p Hecke algebras

This is an introductory chapter that contains the basic notions and necessary results for the first part of this thesis. The first section contains a short introduction to the theory of mod p Hecke algebras. For an extensive introduction to these topics the reader is referred to [Wie06], section 12.4 of [DI95] or to chapter 4 of [DDT94]. Section 1.2 introduces the reader to the theory of Galois representations with values in these mod p Hecke algebras. Their existence and the properties that they enjoy are consequence of Theorem 3 in [Car94].

Since in the next chapters we will be interested in computing the image of these Galois representations, we include a section about images of residual Galois representations, i.e Galois representations that take images on finite fields.

Notation

In the first part of the thesis, by G_L we always mean the absolute Galois group of a number field L.

1.1 Modular forms and Hecke algebras mod p

Let us fix a weight $k \geq 2$, a level $N \geq 1$ and a Dirichlet character $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ with $\varepsilon(-1) = 1$. Let $\mathrm{S}_k(N, \varepsilon; \mathbb{C})$ denote the complex vector space of cusp forms of weight k, level N and character ε. Denote by $\mathbb{Q}[\varepsilon]$ the extension of $\mathbb{Q}$ defined by attaching all the values of ε, and let $\mathcal{O} := \mathbb{Z}[\varepsilon]$ denote its ring of integers. We let $S_k(N, \varepsilon; \mathcal{O})$ denote the abelian group of cusp forms with coefficients in $\mathcal{O}$.

The space $S_k(N, \varepsilon; \mathbb{C})$ is furnished with Hecke operators T_p for every prime p. These operators commute with one another and they generate a finite-dimensional commutative $\mathcal{O}$-subalgebra inside $\mathrm{End}_{\mathbb{C}}(S_k(N, \varepsilon; \mathbb{C}))$, called the *Hecke algebra* of $S_k(N, \varepsilon; \mathbb{C})$ and denoted by $\mathbb{T}_k(N, \varepsilon)$. A modular form $f = \sum_{n \geq 0} a_n(f) q^n$ that is a simultaneous eigenvector for all Hecke operators is called an *eigenform* or *Hecke eigenform*. It is said to be *normalised* if $a_1(f) = 1$.

The action of $\mathbb{T}_k(N,\varepsilon)$ on $S_k(N,\varepsilon;\mathbb{C})$ respects $S_k(N,\varepsilon;\mathcal{O})$, so we can define a bilinear q-pairing

$$\begin{array}{rcl} \mathrm{S}_k(N,\varepsilon;\mathcal{O}) \times \mathbb{T}_k(N,\varepsilon) & \to & \mathcal{O} \\ (f,T) & \mapsto & a_1(Tf). \end{array}$$

which is a perfect pairing (cf. [Rib83], 2.2). For any $\mathcal{O}$-algebra $\sigma : \mathcal{O} \to R$, we let $S_k(N,\varepsilon;R) := S_k(N,\varepsilon;\mathbb{Z}) \otimes_{\mathcal{O}} R$. There is a natural isomorphism of $\mathcal{O}$-modules

$$\begin{array}{rccl} \lambda : & S_k(N,\varepsilon;R) & \to & \mathrm{Hom}_{\mathcal{O}}(\mathbb{T}_k(N,\varepsilon),R) \\ & f & \mapsto & \lambda_f : T_n \mapsto \sigma(a_n(f)) \end{array}$$

Let $\mathbb{T}_R := \mathbb{T}_k(N,\varepsilon) \otimes_{\mathcal{O}} R$. Then we also have the following isomorphism (cf. [Wie06])

$$\mathrm{Hom}_{\mathcal{O}}(\mathbb{T}_k(N,\varepsilon),R) \simeq \mathrm{Hom}_R(\mathbb{T}_R,R).$$

Thus, every element $f \in S_k(N,\varepsilon;R)$ corresponds to a linear function $\Phi : \mathbb{T}_R \to R$ and is uniquely identified by its formal q-expansion $f = \sum_n \Phi(T_n)q^n = \sum_n a_n(f)q^n$,

Now let us restrict to the case where $R = \mathbb{F}$ is a either $\overline{\mathbb{F}}_p$ or a finite field of characteristic p. Consider the character $\overline{\varepsilon} : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{F}$ defined as $\overline{\varepsilon} := \sigma \circ \varepsilon$. We then denote by $\mathrm{S}_k(N,\overline{\varepsilon};\mathbb{F})$ the space of *mod p cusp forms*, of weight k, level N and character $\overline{\varepsilon}$ (over $\mathbb{F}$).

We denote by $\overline{\mathbb{T}} \subseteq \mathbb{T}_{\mathbb{F}_q}$ the *mod p Hecke algebra* associated to $S_k(N,\overline{\varepsilon};\mathbb{F}_q)$ generated by the *good* operators T_ℓ, i.e. those with $\ell \nmid Np$. It is a finite-dimensional artinian commutative $\mathbb{F}_q$-algebra. We have the following decomposition ([DDT94], chapter 4)

$$\overline{\mathbb{T}} \simeq \prod_{\mathfrak{m}\,\text{maximal}} \overline{\mathbb{T}}_{\mathfrak{m}},$$

where $\overline{\mathbb{T}}_{\mathfrak{m}}$ denotes the localisation of $\overline{\mathbb{T}}$ at a maximal ideal $\mathfrak{m}$ of $\overline{\mathbb{T}}$. Every normalised mod p eigenform $f(z) = \sum_{n=0}^{\infty} a_n(f)q^n \in \mathrm{S}_k(N,\overline{\varepsilon};\mathbb{F}_q)$ gives rise to a maximal ideal $\mathfrak{m}_f := \ker \lambda_f$ of $\overline{\mathbb{T}}$ by considering the kernel of the $\mathcal{O}$-algebra homomorphism

$$\lambda_f : \overline{\mathbb{T}} \to \mathbb{F}_q, \quad T_n \mapsto a_n(f).$$

Actually, there is a correspondence between maximal primes in $\overline{\mathbb{T}}$ and $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_q)$-conjugacy classes of normalised eigenforms in $S_k(N,\varepsilon;\overline{\mathbb{F}}_q)$ (cf. [DDT94], chapter 4).

Given a normalised Hecke eigenform f as before, we are interested in the localised Hecke algebra $\overline{\mathbb{T}}_{\mathfrak{m}_f}$, which is a local finite-dimensional $\mathbb{F}_q$-algebra with residue field $\mathbb{F}_q$, where $\mathbb{F}_q$ denotes the finite field of characteristic p generated by the coefficients of f. We will call this Hecke algebra the *local mod p Hecke algebra* associated to the mod p modular form f.

1.2 Galois representations and mod p Hecke algebras

Let R be a complete local ring with residual field $\mathbb{F}$ of characteristic p. Fix a level $N \geq 1$, a weight $k \geq 2$ and a Dirichlet character $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$. Let $\mathcal{O} := \mathbb{Z}[\varepsilon]$ and suppose that $\sigma : \mathcal{O} \to R$ is an $\mathcal{O}$-algebra.

Let $f \in \mathrm{S}_k(N, \varepsilon; R)$ denote a normalised Hecke eigenform given by a ring homomorphism $\lambda_f : \mathbb{T}_k(N, \varepsilon) \to R$. Let $\overline{\varepsilon} := \sigma \circ \varepsilon$ and let $\overline{f} \in \mathrm{S}_k(N, \overline{\varepsilon}; \mathbb{F})$ denote the residual form with coefficients in $\mathbb{F}$, which corresponds to a homomorphism

$$\lambda_{\overline{f}} = \overline{\lambda}_f : \mathbb{T}_k(N, \varepsilon) \to \mathbb{F}$$

given by the reduction modulo the maximal ideal of R. In fact f has coefficients in some finite field $\mathbb{F}_q \subseteq \mathbb{F}$. Then it is well-known (cf. [DS74], Theorem 6.7) that we can attach to $\overline{f}$ a residual Galois representation

$$\overline{\rho}_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_q)$$

which is continuous, unramified outside Np and, for every $\ell \nmid Np$, the following relations hold

$$\mathrm{tr}(\overline{\rho}_f(\mathrm{Frob}_\ell)) = \overline{\lambda}_f(T_\ell) \quad \text{and} \quad \det(\overline{\rho}_f(\mathrm{Frob}_\ell)) = \ell^{k-1}\overline{\varepsilon}(\ell).$$

By Theorem 3 in [Car94], if the residual representation $\overline{\rho}_f$ is absolutely irreducible, then there exists a continuous Galois representation

$$\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(R)$$

which is unramified outside Np and, for every $\ell \nmid Np$, one has the following relations:

$$\mathrm{tr}(\rho_f(\mathrm{Frob}_\ell)) = \lambda_f(T_\ell) \quad \text{and} \quad \det(\rho_f(\mathrm{Frob}_\ell)) = \ell^{k-1}\varepsilon(\ell).$$

Moreover, this representation is unique up to conjugation.

Let now $f \in \mathrm{S}_k(N, \overline{\varepsilon}; \overline{\mathbb{F}}_p)$ be a normalised mod p Hecke eigenform, let $\mathbb{F}_q$ be the finite field generated by the coefficients of f, and let $\mathfrak{m}_f = \ker \lambda_f$ be the maximal ideal of $\overline{\mathbb{T}}$ given by $\lambda_f : \overline{\mathbb{T}} \to \mathbb{F}_q$ as in the previous section. Let $\overline{\mathbb{T}}_{\mathfrak{m}_f}$ denote the corresponding localisation. We are interested in the situation where $R = \overline{\mathbb{T}}_{\mathfrak{m}_f} =: \mathbb{T}_f$.

Let $D = \mathrm{Im}(\det \circ \overline{\rho}_f) \subseteq \mathbb{F}_q^\times$, let $\mathrm{GL}_2^D(\mathbb{T}_f) := \{g \in \mathrm{GL}_2(\mathbb{T}_f) : \det(g) \in D\}$ and $\mathrm{GL}_2^D(\mathbb{F}_q) := \{g \in \mathrm{GL}_2(\mathbb{F}_q) : \det(g) \in D\}$. We have the following commutative diagram

$$\begin{array}{ccc} \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & \xrightarrow{\rho_f} & \mathrm{GL}_2^D(\mathbb{T}_f) \\ & \searrow^{\overline{\rho}_f} & \downarrow \pi \\ & & \mathrm{GL}_2^D(\mathbb{F}_q) \end{array}$$

where π is given by the reduction of $\mathbb{T}_f$ modulo its maximal ideal $\mathfrak{m}_f$.

We will consider the quotient $(\mathbb{T}, \mathfrak{m}) := (\mathbb{T}_f/\mathfrak{m}_f^2, \mathfrak{m}_f/\mathfrak{m}_f^2)$ (so we have $\mathfrak{m}^2 = 0$) since, as it will become clear soon, this situation will allow us to determine the image of the Galois representation

$$\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T})$$

under the extra condition that the residual Galois representation $\overline{\rho}_f$ has *big image*, i.e. the group $\mathrm{Im}(\overline{\rho}_f)$ contains $\mathrm{SL}_2(\mathbb{F}_q)$.

Let us consider the map $\pi : \mathrm{GL}_2^D(\mathbb{T}) \to \mathrm{GL}_2^D(\mathbb{T}/\mathfrak{m}) \simeq \mathrm{GL}_2^D(\mathbb{F}_q)$ and compute the kernel of π. Take $g = \left(\begin{smallmatrix} a_1+a_2\mathfrak{m} & b_1+b_2\mathfrak{m} \\ c_1+c_2\mathfrak{m} & d_1+d_2\mathfrak{m} \end{smallmatrix}\right) \in \ker(\pi)$, with $a_i, b_i, c_i, d_i \in \mathbb{F}_q$, $i = 1, 2$. Then:

$$g \in \ker(\pi) \Leftrightarrow g = \left(\begin{smallmatrix} 1+a_2\mathfrak{m} & b_2\mathfrak{m} \\ c_2\mathfrak{m} & 1+d_2\mathfrak{m} \end{smallmatrix}\right) \text{ and } \det(g) = 1 + (a_2 + d_2)\mathfrak{m} \in D \subseteq \mathbb{F}_q^\times.$$

Thus we conclude that, if $g \in \ker(\pi)$, then $d_2 = -a_2$. If we denote by $\mathrm{M}_2^0(\mathfrak{m})$ the group of matrices with coefficients in $\mathfrak{m}$ and trace 0, we have $\ker(\pi) = \mathrm{M}_2^0(\mathfrak{m})$ and we have the following short exact sequence

$$\begin{array}{ccccccccc} 0 & \to & \mathrm{M}_2^0(\mathfrak{m}) & \xrightarrow{\iota} & \mathrm{GL}_2^D(\mathbb{T}) & \xrightarrow{\pi} & \mathrm{GL}_2^D(\mathbb{F}_q) & \to & 1 \\ & & \left(\begin{smallmatrix} a\mathfrak{m} & b\mathfrak{m} \\ c\mathfrak{m} & -a\mathfrak{m} \end{smallmatrix}\right) & \mapsto & \left(\begin{smallmatrix} 1+a\mathfrak{m} & b\mathfrak{m} \\ c\mathfrak{m} & 1-a\mathfrak{m} \end{smallmatrix}\right) & & & & \\ & & & & \left(\begin{smallmatrix} a_1+a_2\mathfrak{m} & b_1+b_2\mathfrak{m} \\ c_1+c_2\mathfrak{m} & d_1+d_2\mathfrak{m} \end{smallmatrix}\right) & \mapsto & \left(\begin{smallmatrix} a_1 & b_1 \\ c_1 & d_1 \end{smallmatrix}\right). & \end{array}$$

Moreover this exact sequence is split, the split $s : \mathrm{GL}_2^D(\mathbb{F}_q) \to \mathrm{GL}_2^D(\mathbb{T})$ given by $s(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$.

The fact that we have $\mathfrak{m}^2 = 0$ is crucial since, thanks to this, the group $\mathrm{M}_2^0(\mathfrak{m})$ is abelian, so it turns out to be a $\mathbb{F}_p[\mathrm{GL}_2^D(\mathbb{F}_q)]$-module under the conjugation action of $\mathrm{GL}_2^D(\mathbb{F}_q)$ on $\mathrm{M}_2^0(\mathfrak{m})$.

Let $\overline{G} := \mathrm{Im}(\overline{\rho}_f)$. We are interested in determining $G := \mathrm{Im}(\rho_f)$, which fits in an exact sequence

$$\begin{array}{ccccccccc} 0 & \to & \mathrm{M}_2^0(\mathfrak{m}) & \xrightarrow{\iota} & \mathrm{GL}_2^D(\mathbb{T}) & \xrightarrow{\pi} & \mathrm{GL}_2^D(\mathbb{F}_q) & \to & 1 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \to & H & \to & G & \to & \overline{G} & \to & 1. \end{array}$$

Suppose that we know $\overline{G} = \mathrm{GL}_2^D(\mathbb{F}_q)$. Moreover, from the knowledge of the modular form f we know some traces of the elements in G. In the subsequent chapters we will see that with this information we are able to determine G (and also H).

1.3 Determination of the image of mod p Galois representations

Let $N \geq 1$ and $k \geq 2$ be integers, fix a prime p, and let $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{F}}_p^\times$ denote a Dirichlet character. Take a normalised mod p Hecke eigenform $f \in S_k(N, \varepsilon; \overline{\mathbb{F}}_p^\times)$, let $\mathbb{F}_q$ be the finite field generated by its coefficients and let $\overline{\rho}_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_q)$ denote its attached residual Galois representation. The image of $\overline{\rho}_f$ is determined, up to conjugation in $\mathrm{GL}_2(\overline{\mathbb{F}}_q)$, by the set of determinants of the representation and the projective image $\mathrm{Im}(\mathbb{P}\overline{\rho}_f) \subseteq \mathrm{PGL}_2(\mathbb{F}_{q'})$, where $\mathbb{F}_{q'}$ denotes the field of definition of the projective representation.

In this section we want to find sufficient conditions on the coefficients of the modular form f in order to have that the group $\overline{G} := \mathrm{Im}(\overline{\rho}_f)$ is of the form $\mathrm{GL}_2^D(\mathbb{F}_q)$, where $D = \mathrm{Im}(\det \circ \overline{\rho}_f) \subseteq \mathbb{F}_q^\times$. We first recall Dickson's theorem (cf. [Lan76], chapter XI, §2). Let $\mathcal{S}_n$ denote the symmetric group of n elements and $\mathcal{A}_n$ the alternating group of degree n.

Theorem 1.3.1 (Dickson)**.** *Let p be a prime and H a finite subgroup of $\mathrm{PGL}_2(\overline{\mathbb{F}}_p)$. Then H is conjugated to one of the following groups:*

(1) *a finite subgroup of the upper triangular matrices,*

(2) *a subgroup isomorphic to either $\mathcal{A}_4$, $\mathcal{S}_4$ or $\mathcal{A}_5$,*

(3) *a dihedral group* D_{2n} *with* $n \geq 3$ *and* $(p, n) = 1$,

(4) $\mathrm{PSL}_2(\mathbb{F}_q)$ *or* $\mathrm{PGL}_2(\mathbb{F}_q)$ *for* $\mathbb{F}_q$ *a finite subfield of* $\overline{\mathbb{F}}_p$.

Before we state the main result of this section, we need to introduce one last notion.

Definition 1.3.2. Let $N \geq 1$ and $k \geq 2$ be integers, and let $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a Dirichlet character. Then the *Sturm bound* of the Hecke algebra $\mathbb{T}_k(N, \varepsilon)$ is defined as

$$B(k, N) := \frac{kN}{12} \prod_{\ell | N} \left(1 + \frac{1}{\ell}\right),$$

where the product runs through all the prime divisors of N.

Proposition 1.3.3. *The Hecke algebra* $\mathbb{T}_k(N, \varepsilon)$ *is generated as an* $\mathbb{F}_q$*-algebra by the Hecke operators* T_n*, for* $n \geq 1$ *up to the Sturm bound* $B(k, N)$.

Proof. [LS02], Theorem 5.1. □

Let $\mathbb{P}\overline{\rho}_f : G_\mathbb{Q} \to \mathrm{PGL}_2(\mathbb{F}_q)$ denote the projective representation associated to the representation $\overline{\rho}_f$ through the quotient map $\pi : \mathrm{GL}_2(\mathbb{F}_q) \twoheadrightarrow \mathrm{PGL}_2(\mathbb{F}_q)$. This representation can be defined over field possibly different from the field of definition of $\overline{\rho}_f$.

Lemma 1.3.4 (Field of definition of $\mathbb{P}\overline{\rho}_f$)**.** *Fix a prime* p*, integers* $k \geq 2$ *and* N *with* $p \nmid N$ *and a character* $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{F}}_p^\times$*. Let* $f \in S_k(N, \varepsilon; \overline{\mathbb{F}}_p)$ *be a normalised Hecke eigenform and let* $\overline{\rho}_f : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ *denote its attached Galois representation. Suppose that* $\overline{\rho}_f$ *is irreducible and realised over* $\mathbb{F}_q$*. Then the field of definition of* $\mathbb{P}\overline{\rho}_f$ *is*

$$\mathbb{F} := \mathbb{F}_p\left[f(T_\ell)^2/(f(\langle \ell \rangle)\ell^{k-1}) \,:\, \ell \nmid Np\right].$$

Proof. See [Ann13], Proposition 9.2.2. □

Lemma 1.3.5 (Dihedral case)**.** *Fix a prime* p*, integers* $k \geq 2$ *and* N *with* $p \nmid N$ *and a character* $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{F}}_p^\times$*. Let* $f \in S_k(N, \varepsilon; \overline{\mathbb{F}}_p)$ *be a normalised Hecke eigenform and suppose that it is irreducible and realised over* $\mathbb{F}_q$*. Let* $\overline{\rho}_f : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ *denote the attached Galois representation to* f*. Then the projective image* $\mathrm{Im}(\mathbb{P}\overline{\rho}_f)$ *is dihedral if and only if there exists a quadratic character* $\alpha : (\mathbb{Z}/N\mathbb{Z})^\times \to \{\pm 1\}$ *such that* $\overline{\rho}_f \simeq \alpha \otimes \overline{\rho}_f$.

Proof. [Ann13], Proposition 10.1.1. □

In the rest of the thesis we will only consider those eigenforms whose attached residual Galois representation has big image, i.e such that $\mathrm{SL}_2(\mathbb{F}_q) \subseteq \overline{G}$. Thus the next result will be useful for computations later on.

Theorem 1.3.6. *Consider a normalised mod p Hecke eigenform $f = \sum_{n\geq 0} a_f(n)q^n \in S_k(N,\varepsilon;\overline{\mathbb{F}}_p)$ and let $\mathbb{F}_q$ be the finite field generated by its coefficients. Let $\overline{\rho}_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_q)$ be the residual Galois representation attached to f. Let $D = \mathrm{Im}(\det \circ \overline{\rho}_f) \subseteq \mathbb{F}_q$ and let $\overline{G} := \mathrm{Im}(\overline{\rho}_f) \subseteq \mathrm{GL}_2^D(\mathbb{F}_q)$. For a prime $\ell \nmid Np$, let $p_\ell(x) := x^2 - a_\ell(f)x + \ell^{k-1}\varepsilon(\ell)$ denote the corresponding characteristic polynomial. Suppose that the following conditions are satisfied:*

(a) $\mathbb{F}_p\left[f(T_\ell)^2/f(\langle\ell\rangle)\ell^{k-1} \,:\, \ell \nmid Np\right] = \mathbb{F}_q$;

(b) *there exists a prime ℓ such that $p_\ell(x)$ is irreducible over $\mathbb{F}_q$;*

(c) *there exists a prime ℓ such that $p_\ell(x) = (x-\alpha)(x-\beta) \in \mathbb{F}_{q^2}[x]$, with $\mathrm{ord}_{\mathbb{F}_{q^2}^\times}(\alpha) \nmid 2,3,5$ if $p = 3$, $\mathrm{ord}_{\mathbb{F}_{q^2}^\times}(\alpha) \nmid 3,4$ if $p = 5$, and $\mathrm{ord}_{\mathbb{F}_{q^2}^\times}(\alpha) \nmid 2,3,4,5$ if $p \geq 7$.*

(d) *there is no quadratic character $\alpha : (\mathbb{Z}/N\mathbb{Z})^\times \to \{\pm 1\}$ such that $\overline{\rho}_f \simeq \alpha \otimes \overline{\rho}_f$.*

Then $\overline{G} = \mathrm{GL}_2^D(\mathbb{F}_q)$.

Proof. Let $\mathbb{P}\overline{G} := \overline{G}/(\mathbb{F}_q^\times \cap \overline{G}) \subseteq \mathrm{PGL}_2(\mathbb{F}_q)$ denote the projective image of $\overline{G}$. By the classification of Dickson, $\mathbb{P}\overline{G}$ is conjugated to one of the following groups:

(1) a finite subgroup of the upper triangular matrices;

(2) $\mathcal{A}_4,\ \mathcal{S}_4,\ \mathcal{A}_5$;

(3) D_{2n} with $n \geq 3$ and $(p,n) = 1$;

(4) $\mathrm{PGL}_2(\mathbb{F}_{q'})$ or $\mathrm{PSL}_2(\mathbb{F}_{q'})$, where $\mathbb{F}_{q'} \subseteq \mathbb{F}_q$ is a subfield;

We will exclude one by one the cases (1), (2) and (3). From assumption (*b*) we can already exclude case (1). To exclude case (2) we need to consider different cases. If $p = 2$ the only case that can occur is $\mathcal{A}_5$, which is isomorphic to $\mathrm{SL}_2(\mathbb{F}_4)$. If $p = 3$, then we have the isomorphisms $\mathcal{S}_4 \simeq \mathrm{PGL}_2(\mathbb{F}_3)$ and $\mathcal{A}_4 \simeq \mathrm{PSL}_2(\mathbb{F}_3)$, so the only case we need to exclude is $\overline{G} = \mathcal{A}_5$. Since $\mathcal{A}_5$ only contains elements of order $1, 2, 3$ or 5, it suffices to find an element whose order does not divide $2, 3$ or 5. If $p = 5$, we have the isomorphism $\mathcal{A}_5 \simeq \mathrm{PSL}_2(\mathbb{F}_5)$, so we need to exclude $\mathcal{A}_4$ and $\mathcal{S}_4$. All the elements in the group $\mathcal{A}_4$ have order 1,2 or 3, and the elements of the group $\mathcal{S}_4$ have order 1,2,3 or 4. So if we find an element of order coprime with 12, it is enough to exclude case (2). Finally, if $p \geq 7$, then any of the groups $\mathcal{A}_4, \mathcal{S}_4$ and $\mathcal{A}_5$ can occur, but they are all excluded by assumption (c). We can exclude case (3) using the assumption (*d*) and Lemma 1.3.5.

So we have that $\mathbb{P}\overline{G}$ is either $\mathrm{PSL}_2(\mathbb{F}_{q'})$ of $\mathrm{PGL}_2(\mathbb{F}_{q'})$, for some subfield $\mathbb{F}_{q'}$ of $\mathbb{F}_q$. The field $\mathbb{F}_{q'}$ can be determined using Lemma 1.3.4:

$$\mathbb{F}_{q'} := \mathbb{F}_p\left[f(T_\ell)^2/f(\langle\ell\rangle)\ell^{k-1} \,:\, \ell \nmid Np\right],$$

which by assumption (1) coincides with $\mathbb{F}_q$. Then $\mathbb{P}\overline{G} = \mathrm{PSL}_2(\mathbb{F}_q)$ or $\mathrm{PGL}_2(\mathbb{F}_q)$.

Finally, we go back to $\overline{G}$ from $\mathbb{P}\overline{G}$. We have $\mathrm{SL}_2(\mathbb{F}_q) \subseteq \overline{G} \subseteq \mathrm{GL}_2(\mathbb{F}_q)$, and since we know $\det(\overline{G}) = D$, we obtain $\overline{G} = \mathrm{GL}_2^D(\mathbb{F}_q)$. □

Chapter 2

The image-splitting theorem

This chapter is devoted to prove the image-splitting theorem (Theorem 2.1.2), a result that generalises the Main Theorem in [Man15] from $\mathrm{SL}_n(k)$ to $\mathrm{GL}_n^D(k)$, where k denotes a finite field of characteristic p.

Let $(\mathbb{T}, \mathfrak{m}_{\mathbb{T}})$ denote a finite-dimensional commutative local $\mathbb{F}_q$-algebra with residue field $\mathbb{T}/\mathfrak{m}_{\mathbb{T}} \simeq \mathbb{F}_q$ of characteristic p, and denote by $\pi : \mathbb{T}/\mathfrak{m}_{\mathbb{T}}^2 \to \mathbb{T}/\mathfrak{m}_{\mathbb{T}}$ the natural projection. Consider a closed subgroup $G \subseteq \mathrm{GL}_2^D(\mathbb{T}/\mathfrak{m}_{\mathbb{T}}^2)$, where $D \subseteq \mathbb{F}_q^\times$ denotes a subgroup. Suppose that $\pi(G) = \mathrm{GL}_2^D(\mathbb{F}_q)$. This gives us a short exact sequence

$$1 \to H \to G \to \mathrm{GL}_2^D(\mathbb{F}_q) \to 1,$$

where H is an $\mathbb{F}_p[\mathrm{GL}_2^D(\mathbb{F}_q)]$-module inside the abelian group of trace 0 matrices $\mathrm{M}_2^0(\mathfrak{m}_{\mathbb{T}}/\mathfrak{m}_{\mathbb{T}}^2)$ with coefficients in $\mathfrak{m}_{\mathbb{T}}/\mathfrak{m}_{\mathbb{T}}^2 \simeq \mathbb{F}_q$. We are in the same situation as in section 1.2. The image-splitting theorem will allow us to describe the group G as a semidirect product $H \rtimes \mathrm{GL}_2^D(\mathbb{F}_q)$ (a result that will be explored in chapters 3 and 4). Equivalently, the image-splitting theorem tells us that the previous short exact sequence admits a splitting.

In the first section of this chapter we introduce the necessary notation for the rest of the chapter and we state the image-splitting theorem. In section 2.2 we summarise some results about $\mathbb{F}_p[\mathrm{GL}_n^D(\mathbb{F}_q)]$-modules that we will need for the proof of the image-splitting theorem, and in section 2.3 we recall a result in [Man15] about twisted-semidirect products that will also be very useful. Finally, in the last section we prove the image-splitting theorem using similar arguments as those in [Man15].

2.1 Statement of the image-splitting theorem

Let k be a finite field of characteristic p. Let $W(k)$ denote its ring of Witt vectors and denote by $T : k \to W(k) \subset \overline{\mathbb{Q}}_p$ the Teichmüller lift. Consider a complete local ring $(A, \mathfrak{m}_A)$ with residue field containing k and consider the inclusion $\iota_0 : k \to A/\mathfrak{m}_A$. Since $W(k)$ is a p-ring with residue field k, by the structure theorem for complete local rings ([Mat86], Theorem 29.2) we have that there exists a local homomorphism $\iota : W(k) \to A$ which induces ι_0 on the residue fields. Thus we have a

commutative diagram

$$\begin{array}{ccc} W(k) & \overset{\iota}{\dashrightarrow} & A \\ \uparrow{\scriptstyle T} & & \uparrow \\ k & \xrightarrow[\iota_0]{} & A/\mathfrak{m}_A \end{array}$$

Denote by $W(k)_A$ the image of $\iota : W(k) \to A$.

In this chapter we will prove a generalisation of the following result of J. Manoharmayum (cf. [Man15]).

Theorem 2.1.1 (Manoharmayum)**.** *Let $(A, \mathfrak{m}_A)$ be a complete local noetherian ring with maximal ideal $\mathfrak{m}_A$ and finite residue field $A/\mathfrak{m}_A$ of characteristic p. Let $\pi : A \to A/\mathfrak{m}_A$ be the natural projection. Suppose that we are given a subfield k of $A/\mathfrak{m}_A$ and a closed subgroup G of $\mathrm{GL}_n(A)$. Assume that:*

(1) *the cardinality of k is at least 4, $k \neq \mathbb{F}_5$ if $n = 2$ and $k \neq \mathbb{F}_4$ if $n = 3$;*

(2) *$\pi(G) \supseteq \mathrm{SL}_n(k)$.*

Then G contains a conjugate of $\mathrm{SL}_n(W(k)_A)$.

Consider a subgroup $D \subset k^\times$ and define the following groups:

$$\mathrm{GL}_n^D(W(k)) := \{g \in \mathrm{GL}_n(W(k)) \mid \det(g) \in T(D)\}.$$

For any subring $X \subseteq A$, we define the group

$$\mathrm{GL}_n^D(X) := \{g \in \mathrm{GL}_n(X) \mid \det(g) \in \iota(T(D))\}.$$

The following result will be proved in several steps along this chapter.

Theorem 2.1.2 (Image-splitting theorem)**.** *Let $(A, \mathfrak{m}_A)$ be a complete local noetherian ring with maximal ideal $\mathfrak{m}_A$ and finite residue field $A/\mathfrak{m}_A$ of characteristic p. Let $\pi : A \to A/\mathfrak{m}_A$ denote the natural projection. Suppose that we are given a subfield k of $A/\mathfrak{m}_A$ and a closed subgroup G of $\mathrm{GL}_n(A)$. Assume that the cardinality of k is at least 4 and that $k \neq \mathbb{F}_5$ if $n = 2$ and $k \neq \mathbb{F}_4$ if $n = 3$. Suppose that $\pi(G) \supseteq \mathrm{GL}_n^D(k)$. Then G contains a conjugate of $\mathrm{GL}_n^D(W(k)_A)$.*

2.2 Tools about $\mathbb{F}_p[\mathrm{GL}_n(\mathbb{F}_q)]$-modules

Let k be a finite field of characteristic p. In this section we will state some results about $\mathbb{F}_p[\mathrm{GL}_n(k)]$-modules that will be helpful later. Suppose that we are given two short exact sequences of groups such that there is a commutative diagram

$$\begin{array}{ccccccccc} 0 & \to & M & \overset{\iota}{\to} & E & \overset{\pi}{\to} & H & \to & 1 \qquad (1) \\ & & \uparrow & & \uparrow & & \| & & \\ 0 & \to & N & \overset{\iota}{\to} & G & \overset{\pi}{\to} & H & \to & 1 \qquad (2) \end{array}$$

where M is abelian and (1) is split. We want to compute all possible groups G that fit in the second exact sequence (with $N := M \cap G$).

Lemma 2.2.1. *Given a group G fitting in a diagram like the previous one, we have that N is an H-submodule of M for the conjugation action of H on M through preimages.*

Proof. The group H acts on M by conjugation through preimages: for every $h \in H$ choose a preimage $e_h \in E$ such that $\pi(e_h) = h$. Then since $M = \ker \pi \trianglelefteq E$, we have an action

$$\begin{array}{rccl} \varphi: & H & \to & \mathrm{Aut}(M) \\ & h & \mapsto & \varphi_h : m \mapsto e_h^{-1} m e_h \end{array}$$

Moreover, this action does not depend on the choice of the representative e_h because M is abelian. Now let $N := M \cap G = \ker \pi|_G \trianglelefteq G$. For every $h \in H$ we can choose a preimage $e_h \in G$, so the H-action on M restricts to an action on N. □

Let k be a finite field of characteristic p. Let $\mathrm{M}_n^0(k)$ denote the trace 0 matrices in the group of matrices $\mathrm{M}_n(k)$ and denote by $\mathbb{S}$ the subspace of scalar matrices in $\mathrm{M}_n^0(k)$. Then $\mathbb{S} = (0)$ when $p \nmid n$, and $\mathbb{S} = \{\lambda \mathrm{Id}_n : \lambda \in k\}$ otherwise. Define $\mathbb{V} := \mathrm{M}_n^0(k)/\mathbb{S}$. For any subgroup $D \subseteq k^\times$, we will consider the group $\mathrm{GL}_n^D(k) := \{g \in \mathrm{GL}_n(k) : \det(g) \in D\}$.

Lemma 2.2.2. *Assume that $k \neq \mathbb{F}_2$ if $n = 2$. Let $M \subseteq \mathrm{M}_n^0(k)$ be an $\mathbb{F}_p[\mathrm{GL}_n^D(k)]$-submodule for the conjugation action. Then, either M is a subspace of $\mathbb{S}$ over $\mathbb{F}_p$ or $M = \mathrm{M}_n^0(k)$. Thus $\mathrm{M}_n^0(k)/\mathbb{S}$ is a simple $\mathbb{F}_p[\mathrm{GL}_n^D(k)]$-module, and the sequence*

$$0 \to \mathbb{S} \to \mathrm{M}_n^0(k) \to \mathbb{V} \to 0$$

does not split when $p \mid n$.

Proof. Since any $\mathbb{F}_p[\mathrm{GL}_n^D(k)]$-submodule of $\mathrm{M}_n^0(k)$ is also an $\mathbb{F}_p[\mathrm{SL}_n(k)]$-submodule, we can apply Lemma 3.3 of [Man15]. □

Lemma 2.2.3. *Let R be a ring and M a semisimple left R-module which decomposes as $M = M_1 \oplus \ldots \oplus M_t$, with $M_i \subseteq M$ simple modules. Let $N \subseteq M$ be a submodule of M. Then N is semisimple and is isomorphic to a direct sum of a subset of the modules $M_1, \ldots, M_t$.*

Proof. By Proposition 3.12 in [CR81], for every submodule $N \subseteq M$ there exists a submodule $N' \subseteq M$ such that $M = N \oplus N'$. Now by Corollary 14.6 in [CR00] we have that, in this case, N is isomorphic to a direct sum of a subset of the modules $M_1, \ldots, M_t$. □

We are interested in the particular case where $M = \mathrm{M}_2^0(k) \oplus \ldots \oplus \mathrm{M}_2^0(k)$ and $H = \mathrm{GL}_2^D(k)$. Once we are able to determine all submodules N of M (up to isomorphism), we want to compute all the possible extensions of $\mathrm{GL}_2^D(k)$ by N that lead to a group G from which we only know some of its traces. Using a generalisation of the results in [Man15], we will see that we can assume (when $k \neq \mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5$) that the extension G is (up to conjugation) the trivial one (i.e, it corresponds to a non-twisted semidirect product).

2.3 Twisted semidirect products

Let G be a finite group. Given an $\mathbb{F}_p[G]$-module M and a normalised 2-cocycle $x : G \times G \to M$ (where *normalised* means that $x(1, g) = x(g, 1) = 0$, for every $g \in G$), one can define the *twisted semidirect product* $M \rtimes_x G$. It consists of elements (m, g) with $m \in M$, $g \in G$ and composition law given by

$$(m_1, g_1)(m_2, g_2) := (x(g_1, g_2) + m_1 + g_1 m_2, g_1 g_2).$$

The cohomology class of x in $H^2(G, M)$ represents the extension

$$\begin{array}{ccccccccc} 0 & \to & M & \to & M \rtimes_x G & \to & G & \to & 1 \\ & & m & \mapsto & (m, 1) & & & & \\ & & & & (m, g) & \mapsto & g. & & \end{array}$$

Proposition 2.3.1. *Let G be a finite group. Let M be an $\mathbb{F}_p[G]$-module of finite cardinality and let $N \subseteq M$ be an $\mathbb{F}_p[G]$-submodule such that the map $H^2(G, N) \to H^2(G, M)$ is injective. Fix a normalised 2-cocycle $x : G \times G \to N$. Let H be a subgroup $H \subseteq M \rtimes_x G$ extending G by N, i.e. such that the sequence*

$$0 \to N \to H \to G \to 1$$

is exact. Then this extension corresponds to x in $H^2(G, N)$ and there exists an isomorphism

$$\theta : N \rtimes_x G \to H$$

such that the diagram

$$\begin{array}{ccccccccc} 0 & \to & N & \to & N \rtimes_x G & \to & G & \to & 1 \\ & & \| & & \downarrow^{\theta} & & \| & & \\ 0 & \to & N & \to & H & \to & G & \to & 1 \end{array} \tag{2.1}$$

commutes.

This allows us to define a map $\xi : G \to M$ such that the relation $\theta(0, g) = (\xi(g), g)$ holds for every $g \in G$. Moreover, the following properties hold:

(i) *$\theta(n, g) = (n + \xi(g), g)$, for all $n \in N, g \in G$.*

(ii) *The map $\xi : G \to M$ is a 1-cocycle.*

(iii) *If $H^1(G, M) = 0$ then θ is the conjugation by $(m, 1)$ for some $m \in M$.*

Proof. [Man15], Proposition 2.2. □

2.4 Proof of the image-splitting theorem

From now on we fix a finite field k of characteristic p and set $W_m := W(k)/p^m$. We assume also that $n \geq 2$. We will use Proposition 2.3.1 to prove the image-splitting theorem. In order to do this, we need some knowledge of certain 1-cohomology and 2-cohomology groups. More concretely, let

$N \subseteq M$ be two $\mathbb{F}_p[\mathrm{GL}_n^D(k)]$-submodules of $\mathrm{M}_n^0(k)^r$, for some $r \geq 1$. We will prove that, after some small assumption on k, we have

$$H^1(\mathrm{GL}_n^D(W_m), k) = 0$$

and that there is an injection

$$H^2(\mathrm{GL}_n^D(W_m), N) \hookrightarrow H^2(\mathrm{GL}_n^D(W_m), M).$$

Assumption 2.4.1. *The cardinality of k is at least 4, $k \neq \mathbb{F}_5$ if $n = 2$ and $k \neq \mathbb{F}_4$ if $n = 3$.*

Lemma 2.4.2. *Let C be a finite group such that $(\#C, p) = 1$. Let V be an $\mathbb{F}_p$-vector space. Then*

$$H^i(C, V) = 0, \quad \forall i \geq 1.$$

Proof. Consider the restriction-corestriction map

$$H^i(C, V) \overset{\mathrm{res}}{\to} \underbrace{H^i(1, V)}_{0} \overset{\mathrm{cor}}{\to} H^i(C, V),$$

which corresponds to multiplication by $\#C =: c$. For $x \in H^i(C, V)$ we have that $cx = 0$. So since V is an $\mathbb{F}_p$-vector space and c is invertible in $\mathbb{F}_p$, we must have $x = 0$. Thus $H^i(C, V) = 0$ for all $i > 0$. □

Lemma 2.4.3. *Let k be a finite field of characteristic p satisfying Assumption* 2.4.1. *Let D be a subgroup of $k^\times$. Then*

(a) *$H^1(\mathrm{GL}_n^D(W_m), k) = 0$, for all $m \geq 1$.*

(b) *If $p \nmid n$ then $H^1(\mathrm{GL}_n^D(W_m), \mathrm{M}_n^0(k)) = 0$, for all $m \geq 1$.*

Proof. (a) Consider the short exact sequence

$$0 \to \mathrm{SL}_n(W_m) \to \mathrm{GL}_n^D(W_m) \overset{\det}{\to} T(D) \to 1.$$

We have the inflation-restriction exact sequence

$$0 \to H^1(T(D), k^{\mathrm{SL}_n(W_m)}) \to H^1(\mathrm{GL}_n^D(W_m), k) \to H^1(\mathrm{SL}_n(W_m), k)^{T(D)}.$$

Since $D \subseteq k^\times$, in particular $(\#D, p) = 1$, so $H^1(T(D), k^{\mathrm{SL}_n(W_m)}) = 0$ by Lemma 2.4.2. Moreover, by [Man15] Theorem 3.5, we have that $H^1(\mathrm{SL}_n(W_m), k) = 0$, so we conclude that $H^1(\mathrm{GL}_n^D(W_m), k) = 0$ from the inflation-restriction sequence.

(b) Consider the short exact sequence

$$0 \to \mathrm{SL}_n(W_m) \to \mathrm{GL}_n^D(W_m) \overset{\det}{\to} T(D) \to 1.$$

We have the inflation-restriction exact sequence

$$0 \to H^1(T(D), \mathrm{M}_n^0(k)^{\mathrm{SL}_n(W_m)}) \to H^1(\mathrm{GL}_n^D(W_m), \mathrm{M}_n^0(k)) \to H^1(\mathrm{SL}_n(W_m), \mathrm{M}_n^0(k))^{T(D)}.$$

By [Man15] (Theorem 3.2 and Proposition 3.6), $H^1(\mathrm{SL}_n(W_m), \mathrm{M}_n^0(k)) = 0$. Since $(\#D, p) = 1$, by Lemma 2.4.2 we have that $H^1(T(D), \mathrm{M}_n^0(k)^{\mathrm{SL}_n(W_m)}) = 0$. Thus, from the inflation-restriction sequence, we have that $H^1(\mathrm{GL}_n^D(W_m), \mathrm{M}_n^0(k)) = 0$. □

Lemma 2.4.4. *Let k be a finite field of characteristic p and cardinality at least 4. Let $D \subseteq k^\times$ be a subgroup. Let $N \subseteq M$ be finite $\mathbb{F}_p[\mathrm{GL}_n^D(W_m)]$-submodules of $\mathrm{M}_n^0(k)^r$, for some $r \geq 1$. Then there is an injection*

$$H^2(\mathrm{GL}_n^D(W_m), N) \hookrightarrow H^2(\mathrm{GL}_n^D(W_m), M), \quad \forall m \geq 1.$$

Proof. Put $G := \mathrm{GL}_n^D(W_m)$. Since taking cohomology is functorial, the following diagram commutes

$$\begin{array}{ccc} H^2(G,N) & \to & H^2(G, \mathrm{M}_n^0(k)^r) \\ & \searrow & \uparrow \\ & & H^2(G,M) \end{array}$$

Thus it is enough to prove that the map

$$H^2(G,M) \to H^2(G, \mathrm{M}_n^0(k)^r) \tag{2.2}$$

is injective for any $\mathbb{F}_p[G]$-submodule M of $\mathrm{M}_n^0(k)^r$. Put $Q := \mathrm{M}_n^0(k)^r/M$, $C := \det(G) \subseteq T(k^\times)$ and $\#C = c$. By Lemma 2.4.2, for any $\mathbb{F}_p$-vector space V, we have that $H^i(C,V) = 0$, for all $i \geq 1$. Thus, taking C-invariants is exact, and we have the following commutative diagram with exact rows and columns:

$$\begin{array}{ccccccc}
\overbrace{H^2(C, \mathrm{M}_n^0(k)^r)}^{=0} & & \overbrace{H^2(C, Q^{\mathrm{SL}_n(k)})}^{=0} & & & & \\
\uparrow & & \uparrow & & & & \\
H^1(\mathrm{SL}_n(W_m), \mathrm{M}_n^0(k)^r)^C & \overset{(1)}{\to} & H^1(\mathrm{SL}_n(W_m), Q)^C & \to & H^2(\mathrm{SL}_n(W_m), M)^C & \overset{(2)}{\to} & H^2(\mathrm{SL}_n(W_m), \mathrm{M}_n^0(k)^r)^C \\
\uparrow{\scriptstyle (a)}^{\mathrm{res}} & & \uparrow{\scriptstyle (b)}^{\mathrm{res}} & & \uparrow & & \uparrow \\
H^1(G, \mathrm{M}_n^0(k)^r) & \overset{(3)}{\to} & H^1(G,Q) & \to & H^2(G,M) & \overset{(4)}{\to} & H^2(G, \mathrm{M}_n^0(k)^r) \\
\uparrow^{\inf} & & \uparrow^{\inf} & & & & \\
\underbrace{H^1(C, \mathrm{M}_n^0(k)^r)}_{=0} & \to & \underbrace{H^1(C, Q^{\mathrm{SL}_n(k)})}_{=0} & & & &
\end{array}$$

By [Man15] Theorem 3.1, we know that $H^2(\mathrm{SL}_n(W_m), M) \to H^2(\mathrm{SL}_n(W_m), \mathrm{M}_n^0(k)^r)$ is injective. This implies that (1) is surjective. Arrows (a) and (b) are isomorphisms, and with the surjectivity of (1) we also have that (3) is surjective. Finally, this implies that arrow (4) is injective too. □

Corollary 2.4.5. *Let k be a finite field of characteristic p and cardinality at least 4. Let M, N be two $\mathbb{F}_p[\mathrm{GL}_n^D(W_m)]$-submodules of $\mathrm{M}_n^0(k)^r$ for some integer $r \geq 1$. Suppose that we are given $x \in H^2(\mathrm{GL}_n^D(W_m), M)$ and $y \in H^2(\mathrm{GL}_n^D(W_m), N)$ such that x and y represent the same cohomology class in $H^2(\mathrm{GL}_n^D(W_m), \mathrm{M}_n^0(k)^r)$. Then there exists $z \in H^2(\mathrm{GL}_n^D(W_m), M \cap N)$ such that $x = z$ in $H^2(\mathrm{GL}_n^D(W_m), M)$ and $y = z$ in $H^2(\mathrm{GL}_n^D(W_m), N)$.*

Proof. Consider the short exact sequence

$$0 \to M \cap N \overset{m \mapsto m \oplus m}{\longrightarrow} M \oplus N \overset{m \oplus n \mapsto m-n}{\longrightarrow} M + N \to 0.$$

For the sake of exposition, let us denote $H^2(\mathrm{GL}_n^D(W_B), X)$ only by $H^2(X)$. By the above lemma, we obtain an exact sequence

$$0 \to H^2(M \cap N) \overset{\alpha}{\to} H^2(M) \oplus H^2(N) \overset{\beta}{\to} H^2(M+N).$$

We have $x \oplus y \in H^2(M) \oplus H^2(N)$. Since $H^2(M+N) \to H^2(\mathrm{M}_n^0(k)^r)$ is injective, it follows that $x \oplus y \in \ker \beta$, and thus $x \oplus y \in \mathrm{Im}(\alpha)$. □

Let Γ denote the kernel of the mod p^m-reduction map $\mathrm{GL}_n^D(W_{m+1}) \to \mathrm{GL}_n^D(W_m)$. Then for any $m \geq 1$ we have

$$\Gamma = \{1 + p^m M \mod p^{m+1} \mid M \in \mathrm{M}_n^0(W(k))\} \overset{\phi}{\simeq} \mathrm{M}_n^0(k),$$

where $\phi(1 + p^m M) := M \mod p$, and this isomorphism is compatible with the $\mathrm{GL}_n^D(W_m)$-action by conjugation. Consider the subgroup $Z := \{(1+p^m\lambda)\mathrm{id}_n \mid \lambda \in k\} \subseteq \Gamma$. If $\mathbb{S}$ denotes the subspace of scalar matrices in $\mathrm{M}_n^0(k)$ and we set $\mathbb{V} := \mathrm{M}_n^0(k)/\mathbb{S}$, we then have $\phi(Z) = \mathbb{S}$ and $\phi(\Gamma/Z) = \mathbb{V}$.

Lemma 2.4.6. *Let k be a finite field of characteristic p and cardinality at least 4.*

(a) *Suppose that $k \neq \mathbb{F}_4$ if $n = 3$. Then the short exact sequence*

$$1 \to \Gamma \to \mathrm{GL}_n^D(W_{m+1}) \to \mathrm{GL}_n^D(W_m) \to 1$$

does not split for any integer $m \geq 1$.

(b) *If $p \mid n$, then the short exact sequence*

$$1 \to \Gamma/Z \to \mathrm{GL}_n^D(W_{m+1})/Z \to \mathrm{GL}_n^D(W_m) \to 1$$

does not split for any $m \geq 1$.

Proof. (a) Consider the following short exact sequences

$$\begin{array}{ccccccccc} 1 & \to & \Gamma & \to & \mathrm{GL}_n^D(W_{m+1}) & \overset{\pi}{\to} & \mathrm{GL}_n^D(W_m) & \to & 1 \\ & & \| & & \cup & & \cup & & \\ 1 & \to & \Gamma & \to & \mathrm{SL}_n(W_{m+1}) & \to & \mathrm{SL}_n(W_m) & \to & 1. \end{array}$$

By [Man15] Proposition 3.7, we know that the second exact sequence does not split. Suppose that the first one does, and denote by $s : \mathrm{GL}_n^D(W_m) \to \mathrm{GL}_n^D(W_{m+1})$ a splitting [1] such that $\pi \circ s = \mathrm{id}$. Let $g \in \mathrm{SL}_n(W_m) \subseteq \mathrm{GL}_n^D(W_m)$. We have $1 = \det(g) = \det(\pi(s(g))) = \pi \det(s(g))$, so $\det(s(g)) = 1 + p^m\lambda$, for some $\lambda \in W_{m+1}$. But this contradicts the fact that $\det(s(g)) \in T(D) \subseteq T(k^\times)$ unless $\lambda \equiv 0 \mod p$. In this case we obtain that $\det(s(g)) = 1$, so $g \in \mathrm{SL}_n(W_{m+1})$, which contradicts the non-splitting of the second exact sequence.

(b) Consider the following short exact sequences

$$\begin{array}{ccccccccc} 1 & \to & \Gamma/Z & \to & \mathrm{GL}_n^D(W_{m+1})/Z & \overset{\pi}{\to} & \mathrm{GL}_n^D(W_m) & \to & 1 \\ & & \| & & \cup & & \cup & & \\ 1 & \to & \Gamma/Z & \to & \mathrm{SL}_n(W_{m+1})/Z & \to & \mathrm{SL}_n(W_m) & \to & 1. \end{array}$$

By [Man15] Corollary 3.11 we know that the second exact sequence does not split. The same argument of (a) works to show that the first exact sequence does not split. □

[1] Given a short exact sequence of groups $1 \to M \to E \to G \to 1$ we say that a mapping of sets $s : G \to E$ is a *section* if $p \circ s = \mathrm{id}_G$. If the section is a group homomorphism we call it a *splitting*.

From now on assume that we are given fields $k \subseteq k'$ of characteristic p. Let $\mathcal{C}$ be the category of complete local noetherian rings $(A, \mathfrak{m}_A)$ with residue field $A/\mathfrak{m}_A = k'$ and with morphisms that are the identity on k'. For an object A in $\mathcal{C}$ we will write W and W_A for $W(k)$ and $W(k)_A$, respectively. The image-splitting theorem follows from the next result.

Proposition 2.4.7. *Let $\pi : (A, \mathfrak{m}_A) \to (B, \mathfrak{m}_B)$ be a surjection of artinian local rings in $\mathcal{C}$ with $\mathfrak{m}_A \ker \pi = 0$ and $B \neq 0$. Fix a subgroup $D \subseteq k^\times$. Let H be a subgroup of $\mathrm{GL}_n^D(A)$ such that $\pi(H) = \mathrm{GL}_n^D(W_B)$. Assume that k satisfies Assumption 2.4.1. Then there exists an element $u \in \mathrm{GL}_n(A)$ such that*

$$\pi(u) = 1 \quad \text{and} \quad uHu^{-1} \supseteq \mathrm{GL}_n^D(W_A).$$

Proof. Consider the induced map $\pi : \mathrm{GL}_n(A) \to \mathrm{GL}_n(B)$. We have the following short exact sequence:

$$\begin{array}{ccccccccc} 0 & \to & \mathrm{M}_n(\ker\pi) & \xrightarrow{j} & \pi^{-1}(\mathrm{GL}_n^D(W_B)) & \xrightarrow{\pi} & \mathrm{GL}_n^D(W_B) & \to & 1 \\ & & v & \mapsto & 1+v. & & & & \end{array}$$

Let $G := \pi^{-1}(\mathrm{GL}_n^D(W_B)) \cap \mathrm{GL}_n^D(A)$, and consider the restriction $\pi_{|_G} : G \to \mathrm{GL}_n^D(W_B)$, which is still surjective because we are assuming that there is a subgroup $H \subseteq \mathrm{GL}_n^D(A)$ such that $\pi(H) = \mathrm{GL}_n^D(W_B)$. Then $\ker(\pi_{|_G}) = \{v \in \mathrm{M}_n(\ker(\pi)) \mid \det(1+v) \in T(D)\}$, and for $v \in \ker\pi$ we have

$$\det(1+v) = \det \begin{pmatrix} 1+v_{11} & \dots & v_{1n} \\ \vdots & & \vdots \\ v_{n1} & \dots & 1+v_{nn} \end{pmatrix} = 1 + (v_{11} + v_{22} + \ldots + v_{nn}) + \{ \text{ things in } \ker(\pi)^2\}.$$

Since $\ker(\pi) \subseteq \mathfrak{m}_A$, we have $\ker(\pi)^2 \subseteq \mathfrak{m}_A \cdot \ker(\pi) = 0$. So $\det(1+v) = 1 + \sum_{i=1}^n v_{ii} = 1 + \mathrm{tr}(v) \in T(D) \subseteq T(k^\times)$. Thus we have $\det(1+v) \in (1+\mathfrak{m}_A) \cap T(D) \subseteq (1+\mathfrak{m}_A) \cap T(k^\times) = \{1\}$, so $\mathrm{tr}(v) = 0$ and $\ker(\pi_{|_G}) = \mathrm{M}_n^0(\ker\pi)$, and we have a second short exact sequence:

$$\begin{array}{ccccccccc} 0 & \to & \mathrm{M}_n(\ker\pi) & \xrightarrow{j} & \pi^{-1}(\mathrm{GL}_n^D(W_B)) & \xrightarrow{\pi} & \mathrm{GL}_n^D(W_B) & \to & 1 \\ & & \cup & & \cup & & \| & & \\ 0 & \to & \mathrm{M}_n^0(\ker\pi) & \xrightarrow{j} & G & \xrightarrow{\pi} & \mathrm{GL}_n^D(W_B) & \to & 1 \end{array}$$

For a subring $X \subseteq \mathrm{GL}_n^D(A)$, let $\mathrm{M}_n^0(X) := \{v \in \mathrm{M}_n^0(\ker\pi) : j(v) \in X\}$. Then $\ker(\pi|_{\mathrm{GL}_n^D(W_A)}) = \mathrm{M}_n^0(\mathrm{GL}_n^D(W_A))$ and we have the short exact sequence

$$0 \to \mathrm{M}_n^0(\mathrm{GL}_n^D(W_A)) \xrightarrow{j} \mathrm{GL}_n^D(W_A) \xrightarrow{\pi} \mathrm{GL}_n^D(W_B) \to 1.$$

Fix a section $s : \mathrm{GL}_n^D(W_B) \to \mathrm{GL}_n^D(W_A) \subseteq G$ that sends the identity to the identity and let $x : \mathrm{GL}_n^D(W_B) \times \mathrm{GL}_n^D(W_B) \to \mathrm{M}_n^0(\mathrm{GL}_n^D(W_A))$ be the 2-cocycle representing the previous extension. Since in particular $x \in H^2(\mathrm{GL}_n^D(W_B), \mathrm{M}_n(\ker\pi))$, the section s and the cocycle x give an identification

$$\begin{array}{rccc} \varphi : & \pi^{-1}(\mathrm{GL}_n^D(W_B)) & \xrightarrow{\sim} & \mathrm{M}_n(\ker\pi) \rtimes_x \mathrm{GL}_n^D(W_B) \\ & \mathrm{GL}_n^D(W_A) & \longmapsto & \mathrm{M}_n^0(\mathrm{GL}_n^D(W_A)) \rtimes_x \mathrm{GL}_n^D(W_B). \end{array}$$

We now want to apply Proposition 2.3.1. We have the following commutative diagram (cf. diagram (2.1) of Proposition 2.3.1, where the N used there is $\mathrm{M}_n^0(H)$ in this case).

$$\begin{array}{ccccccccc} 0 & \to & \mathrm{M}_n^0(H) & \to & \mathrm{M}_n^0(H) \rtimes_x \mathrm{GL}_n^D(W_B) & \to & \mathrm{GL}_n^D(W_B) & \to & 1 \\ & & \| & & \downarrow\theta & & \| & & \\ 0 & \to & \mathrm{M}_n^0(H) & \to & \varphi(H) & \to & \mathrm{GL}_n^D(W_B) & \to & 1. \end{array}$$

First suppose that $p \nmid n$. In this case, the role of M in Proposition 2.3.1 is played by $\mathrm{M}_n^0(\ker\pi)$. By the assumptions on k, we have that $H^1(\mathrm{GL}_n^D(W_B), \mathrm{M}_n^0(k)) = 0$ by Lemma 2.4.3. Thus $H^1(\mathrm{GL}_n^D(W_B), \mathrm{M}_n^0(\ker\pi)) = H^1(\mathrm{GL}_n^D(W_B), \mathrm{M}_n^0(k) \otimes_k \ker\pi) = H^1(\mathrm{GL}_n^D(W_B), \mathrm{M}_n^0(k)) \otimes_k \ker\pi = 0$. Furthermore, by Lemma 2.4.4 we have an injection

$$H^2(\mathrm{GL}_n^D(W_B), \mathrm{M}_n^0(H)) \hookrightarrow H^2(\mathrm{GL}_n^D(W_B), \mathrm{M}_n^0(\ker\pi)).$$

Hence we can apply Proposition 2.3.1 and conclude that

$$\mathrm{M}_n^0(H) \rtimes_x \mathrm{GL}_n^D(W_B) = v\varphi(H)v^{-1}$$

for some $(v, e) \in \mathrm{M}_n^0(\ker\pi) \rtimes_x \mathrm{GL}_n^D(W_B)$. Take $u \in G \subseteq \pi(\mathrm{GL}_n^D(W_B))$ such that $\varphi(u) = v$. Then

$$\mathrm{M}_n^0(H) \rtimes_x \mathrm{GL}_n^D(W_B) = \varphi(uHu^{-1}), \quad \text{where } u \in G \text{ such that } \pi(u) = 1.$$

Now suppose that $p \mid n$. In this case the role of M is played by $\mathrm{M}_n(\ker\pi)$. From the short exact sequence

$$1 \to \mathrm{SL}_n(W_B) \to \mathrm{GL}_n^D(W_B) \to T(D) \to 1$$

we obtain the following exact sequence

$$H^1(T(D), \mathrm{M}_n(\ker\pi)) \to H^1(\mathrm{GL}_n^D(W_B), \mathrm{M}_n(\ker\pi)) \to H^1(\mathrm{SL}_n(W_B), \mathrm{M}_n(\ker\pi)),$$

with $H^1(T(D), \mathrm{M}_n(\ker\pi)) = 0$ by Lemma 2.4.2 and $H^1(\mathrm{SL}_n(W_B), \mathrm{M}_n(\ker\pi)) = 0$ by [Man15], Proposition 4.2. Thus we also have that $H^1(\mathrm{GL}_n^D(W_B), \mathrm{M}_n(\ker\pi)) = 0$. On the other hand, since $H^1(\mathrm{GL}_n^D(W_B), k) = 0$ by Lemma 2.4.3, from the exact sequence $0 \to \mathrm{M}_n^0(k) \to \mathrm{M}_n(k) \to k \to 0$ we get the following exact sequence:

$$H^1(\mathrm{GL}_n^D(W_B), \mathrm{M}_n^0(k)) \to H^1(\mathrm{GL}_n^D(W_B), \mathrm{M}_n(k)) \to 0 \to$$

$$\to H^2(\mathrm{GL}_n^D(W_B), \mathrm{M}_n^0(k)) \to H^2(\mathrm{GL}_n^D(W_B), \mathrm{M}_n(k)).$$

Using the injection $H^2(\mathrm{GL}_n^D(W_B), \mathrm{M}_n^0(k)) \hookrightarrow H^2(\mathrm{GL}_n^D(W_B), \mathrm{M}_n(k))$ from the previous exact sequence and the fact that $\mathrm{M}_n(\ker\pi) \simeq \mathrm{M}_n(k) \otimes_k \ker\pi$, we have an injection

$$H^2(\mathrm{GL}_n^D(W_B), \mathrm{M}_n^0(\ker\pi)) \hookrightarrow H^2(\mathrm{GL}_n^D(W_B), \mathrm{M}_n(\ker\pi)).$$

By Lemma 2.4.4 we also have an injection $H^2(\mathrm{GL}_n^D(W_B), \mathrm{M}_n^0(H)) \hookrightarrow H^2(\mathrm{GL}_n^D(W_B), \mathrm{M}_n^0(\ker\pi))$, so we can conclude that

$$H^2(\mathrm{GL}_n^D(W_B), \mathrm{M}_n^0(H)) \to H^2(\mathrm{GL}_n^D(W_B), \mathrm{M}_n(\ker\pi))$$

is an injection. Hence, we can apply Proposition 2.3.1 and obtain

$$\mathrm{M}_n^0(H) \rtimes_x \mathrm{GL}_n^D(W_B) = v\varphi(H)v^{-1},$$

for some $(v, e) \in \mathrm{M}_n(\ker\pi) \rtimes_x \mathrm{GL}_n^D(W_B)$. Take $u \in \pi^{-1}(\mathrm{GL}_n^D(W_B))$ such that $\varphi(u) = v$. Then

$$\mathrm{M}_n^0(H) \rtimes_x \mathrm{GL}_n^D(W_B) = \varphi(uHu^{-1}), \quad \text{where } u \in \pi^{-1}(\mathrm{GL}_n^D(W_B)) \text{ with } \pi(u) = 1.$$

In both cases we have an element $u \in \mathrm{GL}_n(A)$ such that $\varphi(uHu^{-1}) = \mathrm{M}_n^0(H) \rtimes_x \mathrm{GL}_n^D(W_B)$ and $\pi(u) = 1$.

Claim: $\mathrm{M}_n^0(\mathrm{GL}_n^D(W_A)) \subseteq \mathrm{M}_n^0(H)$.

Suppose the previous claim is true. Then

$$\varphi(\mathrm{GL}_n^D(W_A)) = \mathrm{M}_n^0(\mathrm{GL}_n^D(W_A)) \rtimes_x \mathrm{GL}_n^D(W_B) \subseteq \mathrm{M}_n^0(H) \rtimes_x \mathrm{GL}_n^D(W_B) = \varphi(uHu^{-1}),$$

so $\mathrm{GL}_n^D(W_A) \subseteq uHu^{-1}$, and we are done.

Proof of the claim: If $W_A \to W_B$ is an injection, then $\mathrm{M}_n^0(\mathrm{GL}_n^D(W_A))$ is (0) and the claim is true. Otherwise, we identify W_A with W_n for some $n \geq 1$ and W_B with W_m for some $1 \leq m \leq n$. Since we have a filtration $\ldots \subseteq W_{m-1} \subseteq W_m \subseteq W_{m+1} \subseteq \ldots$, without loss of generality we may assume that $n = m + 1$. This gives a natural identification of $\Gamma := \ker \pi = \mathrm{M}_n^0(\mathrm{GL}_n^D(W_A))$ with $\mathrm{M}_n^0(k)$. We will use this identification in what follows.

Let $x \in H^2(\mathrm{GL}_n^D(W_B), \mathrm{M}_n^0(k))$ represent the extension

$$0 \to \mathrm{M}_n^0(k) \xrightarrow{j} \mathrm{GL}_n^D(W_A) \to \mathrm{GL}_n^D(W_B) \to 1, \tag{2.3}$$

and let $y \in H^2(\mathrm{GL}_n^D(W_B), \mathrm{M}_n^0(H))$ represent the extension

$$0 \to \mathrm{M}_n^0(H) \xrightarrow{j} H \to \mathrm{GL}_n^D(W_B) \to 1.$$

We have a commutative diagram

$$\begin{array}{ccccccccc}
0 & \to & \mathrm{M}_n^0(k) & \to & \mathrm{GL}_n^D(W_A) & \xrightarrow{\pi} & \mathrm{GL}_n^D(W_B) & \to & 1 \\
 & & \cap & & \cap & & \| & & \\
0 & \to & \mathrm{M}_n^0(\ker\pi) & \to & G & \xrightarrow{\pi} & \mathrm{GL}_n^D(W_B) & \to & 1 \\
 & & \cup & & \cup & & \| & & \\
0 & \to & \mathrm{M}_n^0(H) & \to & H & \xrightarrow{\pi} & \mathrm{GL}_n^D(W_B) & \to & 1
\end{array}$$

so x and y represent the same cohomology class in $H^2(\mathrm{GL}_n^D(W_B), \mathrm{M}_n^0(\ker\pi))$, namely

$$0 \to \mathrm{M}_n^0(\ker\pi) \to G \to \mathrm{GL}_n^D(W_B) \to 1.$$

By Corollary 2.4.5, there exists $z \in H^2(\mathrm{GL}_n^D(W_B), \mathrm{M}_n^0(k) \cap \mathrm{M}_n^0(H))$ such that x and z (respectively, y and z) represent the same cohomology class in $H^2(\mathrm{GL}_n^D(W_B), \mathrm{M}_n^0(k))$ (respectively, in $H^2(\mathrm{GL}_n^D(W_B), \mathrm{M}_n^0(H))$).

Suppose that $\mathrm{M}_n^0(k)$ is not contained in $\mathrm{M}_n^0(H)$. Then we have that $\mathrm{M}_n^0(k) \cap \mathrm{M}_n^0(H) \subseteq \mathbb{S}$ by Lemma 2.2.2. If $\mathrm{M}_n^0(k) \cap \mathrm{M}_n^0(H) = (0)$, then $x = 0$, which contradicts the non-splitting of the extension (2.3) (cf. Lemma 2.4.6). Thus $\mathrm{M}_n^0(k) \cap \mathrm{M}_n^0(H) \subseteq \mathbb{S}$ is a submodule of $\mathbb{S}$ different from (0), so we must be in the situation where $p \mid n$. Now the image of x in $H^2(\mathrm{GL}_n^D(W_B), \mathrm{M}_n^0(k)/\mathbb{S})$ represents the extension

$$0 \to \mathrm{M}_n^0(k)/\mathbb{S} \xrightarrow{j} \mathrm{GL}_n^D(W_{m+1})/Z \xrightarrow{\bmod p^m} \mathrm{GL}_n^D(W_m) \to 1.$$

(where we use that $Z \simeq \mathbb{S}$). Since this is non-split by Lemma 2.4.6 and $\mathbb{V} = \mathrm{M}_n^0(k)/\mathbb{S}$, the image of x in $H^2(\mathrm{GL}_n^D(W_B), \mathbb{V})$ is not 0. This contradicts the fact that x is in the image of the map $H^2(\mathrm{GL}_2^D(W_B), \mathbb{S}) \to H^2(\mathrm{GL}_n^D(W_B), \mathrm{M}_n^0(k))$. □

Now the only thing that we are left to do is to see how the image-splitting theorem follows from Proposition 2.4.7. Suppose that k is a finite field of characteristic p that satisfies Assumption 2.4.1. Let $(A, \mathfrak{m}_A)$ be a local ring in $\mathcal{C}$ and $\pi : A \to A/\mathfrak{m}_A$ denote the natural projection, and fix some subgroup $D \subseteq k^\times$. Consider a closed subgroup $G \subseteq \mathrm{GL}_n(A)$ such that $\pi(G) \supseteq \mathrm{GL}_n^D(k)$. We want to see that then G contains a conjugate of $\mathrm{GL}_n^D(W_A)$. We may assume that $\pi(G) = \mathrm{GL}_n^D(k)$ without loss of generality (indeed, consider $\overline{G} := G \cap \pi^{-1}(\mathrm{GL}_n^D(k))$. Then $\pi(\overline{G}) = \mathrm{GL}_n^D(k)$. If we see that $\overline{G}$ contains a conjugate of $\mathrm{GL}_n^D(W_A)$, then this conjugate also lies in G). The next step is to see that actually we can assume that $G \subseteq \mathrm{GL}_n^D(A)$. We will need the following two lemmas.

Lemma 2.4.8. *The group $G \cap \mathrm{GL}_n^D(A)$ is a closed normal subgroup of G and the quotient group $G/(G \cap \mathrm{GL}_n^D(A))$ is pro-p.*

Proof. Consider the group homomorphism $G \to \det(G) \to \det(G)/(T(D) \cap \det(G))$, whose kernel is $G \cap \mathrm{GL}_n^D(A)$. By the first isomorphism theorem, we have an isomorphism

$$G/(G \cap \mathrm{GL}_n^D(A)) \xrightarrow{\sim} \det(G)/(G \cap T(D)).$$

Let us show that $\det(G)/(T(D) \cap \det(G))$ is a pro-p group. We have $D \equiv \det(G) \mod \mathfrak{m}_A$, and if we consider this congruence multiplicatively, we have $D \equiv \det(G) \mod 1 + \mathfrak{m}_A$. Since $T(D) \equiv D \mod 1 + \mathfrak{m}_A$, we have

$$T(D) \equiv \det(G) \mod 1 + \mathfrak{m}_A \quad \Rightarrow \quad \det(G) \subseteq (1 + \mathfrak{m}_A) \cdot T(D)$$

$\Rightarrow \det(G)/(T(D) \cap \det(G)) \subseteq (1 + \mathfrak{m}_A)/(T(D) \cap (1 + \mathfrak{m}_A)) = 1 + \mathfrak{m}_A$. Since the 1-units are a pro-p group, any subgroup of them will also be a pro-p group and we are done. □

Since $G/(G \cap \mathrm{GL}_n^D(A))$ is pro-p, this implies that $\pi(G/(G \cap \mathrm{GL}_n^D(A)))$ is a p-group. Thus $\pi(G)/\pi(G \cap \mathrm{GL}_n^D(A)) = \mathrm{GL}_n^D(k)/\pi(G \cap \mathrm{GL}_n^D(A))$ is a p-group, so $\pi(G \cap \mathrm{GL}_n^D(A))$ is normal in $\mathrm{GL}_n^D(k)$ and has index a power of p.

Lemma 2.4.9. *Let k be a finite field of cardinality at least 4. Let J be a normal subgroup of $\mathrm{GL}_n^D(k)$ not contained in the scalar matrices $\mathbb{S}$ and with $\det(J) = D$. Denote by $\overline{J}$ its image in $\mathrm{PGL}_n^D(k)$. Then $\overline{J} = \mathrm{PGL}_n^D(k)$.*

Proof. Let $K := J \cap \mathrm{SL}_n(k)$. We have the following diagram

$$\begin{array}{ccccccc} K & \subseteq & J & \subseteq & \mathrm{GL}_n^D(k) & \subseteq & \mathrm{GL}_n(k) \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ \overline{K} & \subseteq & \overline{J} & \subseteq & \mathrm{PGL}_n^D(k) & \subseteq & \mathrm{PGL}_n(k) \\ \cap & & & & & & \\ \mathrm{PSL}_n(k) & & & & & & \end{array}$$

Since $J \trianglelefteq \mathrm{GL}_n^D(k)$ and $\mathrm{SL}_n(k) \trianglelefteq \mathrm{GL}_n^D(k)$, we also have that $K \trianglelefteq \mathrm{SL}_n(k)$. Thus $\overline{K} \trianglelefteq \mathrm{PSL}_n(k)$. Now $\mathrm{PSL}_n(k)$ is simple since $\#k \geq 4$, and since $K \not\subseteq k^\times$, we must have $\overline{K} = \mathrm{PSL}_n(k)$. Thus we have

$$\mathrm{PSL}_n(k) \subseteq \overline{J} \subseteq \mathrm{PGL}_n^D(k) \subseteq \mathrm{PGL}_n(k).$$

Since there is an isomorphism $\mathrm{PGL}_n(k)/\mathrm{PSL}_n(k) \simeq k^\times/(k^\times)^n$ given by the determinant map $\det : \mathrm{PGL}_n \to k^\times/(k^\times)^n$, and since $\det(J) = D$, we conclude that $\overline{J} = \mathrm{PGL}_n^D(k)$. □

Let $H := G \cap \mathrm{GL}_n^D(A)$ and $J := \pi(H) \trianglelefteq \mathrm{GL}_n^D(k)$. Since $\pi(G) = \mathrm{GL}_n^D(k)$, we have that J is not contained in $\mathbb{S}$. We thus can apply the previous lemma to J and we obtain that $\overline{J} = \mathrm{PGL}_n^D(k)$. Thus since $J \not\subseteq k^\times$, we have $J = \mathrm{GL}_n^D(k)$. Finally, since $\pi(H) = \mathrm{GL}_n^D(k)$, if we prove that H contains a conjugate of $\mathrm{GL}_n^D(W_A)$, this will also lie in G. So we can assume, without loss of generality, that $G \subseteq \mathrm{GL}_n^D(A)$.

Finally, suppose that the assumptions of Theorem 2.1.2 are satisfied. Then, without loss of generality, we can assume the following:

(T1) $G \subseteq \mathrm{GL}_n^D(A)$,

(T2) $G \equiv \mathrm{GL}_n^D(k) \mod \mathfrak{m}_A$,

(T3) k satisfies Assumption 2.4.1.

In order to apply Proposition 2.4.7, first note that the ring $(A, \mathfrak{m}_A)$ is the projective limit of the artinian quotients $A/\mathfrak{m}_A^i$, i.e. we have that $A = \varprojlim A/\mathfrak{m}_A^i$. Fix $i \geq 1$ and let $(A_i, \mathfrak{m}_i) := (A/\mathfrak{m}_A^i, \mathfrak{m}_A/\mathfrak{m}_A^i)$. Consider the projection $\pi_i : A_i \to A_{i-1}$. Let $G_i := G/\mathfrak{m}_A^i \subseteq \mathrm{GL}_n^D(A_i)$. To apply the proposition, the following two conditions have to be satisfied:

(P1) $\mathfrak{m}_i \ker \pi_i = 0$,

(P2) $\pi_i(G_i) = \mathrm{GL}_n^D(W_{A_{i-1}})$.

Condition (P1) follows from the easy computation

$$\ker \pi_i = \ker(A/\mathfrak{m}_A^i \to A/\mathfrak{m}_A^{i-1}) = \mathfrak{m}_A^{i-1}/\mathfrak{m}_A^i$$

so, in particular, $\mathfrak{m}_i \ker \pi_i = 0$.

We will use induction to prove that if condition (P2) is satisfied by a certain conjugate of the group G_i, for some $i \geq 2$, then it is also satisfied by a conjugate of G_{i+1}. This will be enough to conclude the image-splitting theorem. For $i = 2$ we have $\pi_2 : \mathrm{GL}_n(A_2) \to \mathrm{GL}_n(A_1)$ and

$$\pi_2(G_2) = G_1 = G/\mathfrak{m}_A \overset{\text{(T2)}}{=} \mathrm{GL}_n^D(k) = \mathrm{GL}_n^D(W_{A_1}).$$

Thus we can apply Proposition 2.4.7 and obtain that there exists $u_2 \in \mathrm{GL}_n(A_2)$ such that $\pi_2(u_2) = 1$ and

$$G_2 \supseteq u_2^{-1}\mathrm{GL}_n^D(W_{A_2})u_2.$$

We have $\pi_3(G_3) = G_2 \supseteq u_2^{-1}\mathrm{GL}_n^D(W_{A_2})u_2 \Rightarrow \pi_3(w_3 G_3 w_3^{-1}) \supseteq \mathrm{GL}_n^D(W_{A_2})$, for some $w_3 \in \mathrm{GL}_n(A_3)$ with $\pi_3(w_3) = u_2$. Let $H_3 := w_3 G_3 w_3^{-1}$. We can assume without loss of generality that $\pi_3(H_3) = \mathrm{GL}_n^D(W_{A_2})$ (indeed, if we put $\overline{H}_3 := H_3 \cap \pi_3^{-1}(\mathrm{GL}_n^D(W_{A_2}))$, then $\overline{H}_3 \subseteq \mathrm{GL}_n^D(A_3)$ and $\pi_3(\overline{H}_3) = \mathrm{GL}_n^D(W_{A_2})$). So H_3 satisfies condition (P2). Let us continue with the induction. Suppose that $\pi_i(H_i) = \mathrm{GL}_n^D(W_{A_{i-1}})$ holds for some $i \geq 3$, where $H_i := w_i G_i w_i^{-1}$ for some $w_i \in \mathrm{GL}_n(A_i)$ with $\pi_4 \circ \pi_5 \circ \ldots \circ \pi_i(w_i) = w_3$. Then by Proposition 2.4.7 there exists $u_i \in \mathrm{GL}_n(A_i)$ with $\pi_i(u_i) \in 1 + \mathfrak{m}_i$ such that $H_i \supseteq u_i^{-1}\mathrm{GL}_n^D(W_{A_i})u_i$, so

$$\mathrm{GL}_n^D(W_{A_i}) \subseteq u_i H_i u_i^{-1} = u_i w_i G_i w_i^{-1} u_i^{-1} = \pi_{i+1}(w_{i+1} G_{i+1} w_{i+1}^{-1}),$$

for some $w_{i+1} \in \mathrm{GL}_n(A_{i+1})$ with $\pi_{i+1}(w_{i+1}) = u_i w_i$. Thus if we put $H_{i+1} := w_{i+1} G_{i+1} w_{i+1}^{-1}$, we can assume (again without loss of generality) that $\pi_{i+1}(H_{i+1}) = \mathrm{GL}_n^D(W_{A_i})$. Thus H_{i+1} satisfies condition (P2).

Finally, from this we obtain that G contains a conjugate of $\mathrm{GL}_n^D(W(k)_A)$ taking the projective limit over i:

$$G = \varprojlim_i G_i = \varprojlim_i w_i^{-1} H_i w_i \supseteq \varprojlim_i w_i^{-1} \mathrm{GL}_n^D(W(k)_{A_i})\, w_i = w^{-1}\mathrm{GL}_n^D(W(k)_A)w,$$

where $w := \varprojlim w_i \in \mathrm{GL}_n^D(A)$. This finishes the proof of Theorem 2.1.2.

Corollary 2.4.10. *Let k be a finite field of characteristic p with cardinality at least 4, $k \neq \mathbb{F}_5$ if $n = 2$ and $k \neq \mathbb{F}_4$ if $n = 3$. Let $(A, \mathfrak{m}_A)$ be a finite-dimensional commutative local k-algebra with residue field k and $\mathfrak{m}_A^2 = 0$. Let $G \subseteq \mathrm{GL}_n^D(A)$ be a subgroup. Suppose that $G \mod \mathfrak{m}_A = \mathrm{GL}_n^D(k)$. Then there exists an $\mathbb{F}_p[\mathrm{GL}_n^D(k)]$-submodule $M \subseteq \mathrm{M}_n^0(\mathfrak{m}_A)$ such that G is, up to conjugation by an element $u \in \mathrm{GL}_n(A)$ with $\pi(u) = 1$, a (non-twisted) semidirect product of the form*

$$G \simeq M \rtimes \mathrm{GL}_n^D(k).$$

Proof. We are in the hypothesis of the image-splitting theorem, and since moreover we are assuming that A is a k-algebra, we have that $W(k)_A = k$. So in this situation there exists $u \in \mathrm{GL}_n(A)$ such that $\pi(u) = 1$ and $G \supseteq u^{-1}\mathrm{GL}_n^D(k)u$. Let $G' := uGu^{-1} \subseteq \mathrm{GL}_n^D(A)$. Denote by $\pi : A \to A/\mathfrak{m}_A \simeq k$ the natural projection and consider the following split short exact sequence:

$$\begin{array}{ccccccccc} 0 & \to & \mathrm{M}_n(\mathfrak{m}_A) & \to & \mathrm{GL}_n(A) & \xrightarrow{\pi} & \mathrm{GL}_n(k) & \to & 1 \\ & & m & \mapsto & 1+m. & & & & \end{array}$$

Take $m = (m_{ij})_{1\leq i,j\leq n} \in \mathrm{M}_n(\mathfrak{m}_A)$. An easy computation shows that $1 + m \in \mathrm{GL}_n^D(A)$ if and only if $\mathrm{tr}(m) = 0$:

$$\det(1+m) = \det \begin{pmatrix} 1+m_{11} & \dots & m_{1n} \\ \vdots & & \vdots \\ m_{n1} & \dots & 1+m_{nn} \end{pmatrix} = 1 + \mathrm{tr}(m) + \mathfrak{m}_A^2,$$

and $1+\mathrm{tr}(m)+\mathfrak{m}_A^2 = 1+\mathrm{tr}(m) \in k$ if and only if $\mathrm{tr}(m) = 0$. This gives a split short exact sequence

$$\begin{array}{ccccccccc} 0 & \to & \mathrm{M}_n^0(\mathfrak{m}_A) & \to & \mathrm{GL}_n^D(A) & \xrightarrow{\pi} & \mathrm{GL}_n^D(k) & \to & 1 \end{array}$$

and we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \to & \mathrm{M}_n^0(\ker\pi) & \to & \mathrm{GL}_n^D(A) & \xrightarrow{\pi} & \mathrm{GL}_n^D(k) & \to & 1 \\ & & \cup & & \cup & & \| & & \\ 0 & \to & M & \to & G' & \to & \mathrm{GL}_n^D(k) & \to & 1. \end{array}$$

with $G' \supseteq \mathrm{GL}_n^D(k)$ and $M \subseteq \mathrm{M}_n^0(\ker\pi)$ a $\mathrm{GL}_n^D(k)$-submodule. So in particular, the second short exact sequence splits and G' is of the form $G' = M \rtimes \mathrm{GL}_n^D(k)$. □

Chapter 3

Galois representations with values in Hecke algebras

In this chapter we study continuous odd Galois representations

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T}/\mathfrak{m}_{\mathbb{T}}^2)$$

where $(\mathbb{T}, \mathfrak{m}_{\mathbb{T}})$ denotes a finite-dimensional local commutative algebra over a finite field $\mathbb{F}_q$ of characteristic p, equipped with the discrete topology and with $\mathbb{F}_q$ as residue field. We assume that $\mathbb{T}/\mathfrak{m}_{\mathbb{T}}^2$ is generated by the traces of the image of ρ. In particular, note that we have that the maximal ideal $\mathfrak{m}_{\mathbb{T}}/\mathfrak{m}_{\mathbb{T}}^2$ of the algebra $\mathbb{T}/\mathfrak{m}_{\mathbb{T}}^2$ satisfies that $(\mathfrak{m}_{\mathbb{T}}/\mathfrak{m}_{\mathbb{T}}^2)^2 = 0$.

In sections 3.1 and 3.2 we use theorem 2.1.2 proved in chapter 2 to determine, under the hypothesis that ρ has big residual image, the image of ρ when $p \neq 2$ and $p = 2$, respectively. More concretely, if $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ denotes the corresponding residual Galois representation, we will assume that $\mathrm{Im}(\overline{\rho}) = \mathrm{GL}_2^D(\mathbb{F}_q)$, where $D \subseteq \mathbb{F}_q^\times$ indicates the image of the determinant of $\overline{\rho}$. Then we show that the number t of different traces in $\mathrm{Im}(\rho)$ and the dimension m of $\mathfrak{m}_{\mathbb{T}}/\mathfrak{m}_{\mathbb{T}}^2$ determine uniquely, up to isomorphism, the group $\mathrm{Im}(\rho)$. In the case where $p \neq 2$ we show that the image of ρ is always the biggest possible, i.e.

$$\mathrm{Im}(\rho) \simeq (\underbrace{\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}_{m}) \rtimes \mathrm{GL}_2^D(\mathbb{F}_q) \simeq \mathrm{GL}_2^D(\mathbb{T}/\mathfrak{m}_{\mathbb{T}}^2),$$

and this is equivalent to have $t = q^{m+1}$. When $p = 2$, we have

$$\mathrm{Im}(\rho) \simeq M \rtimes \mathrm{GL}_2^D(\mathbb{F}_q),$$

where M is an $\mathbb{F}_2[\mathrm{GL}_2^D(\mathbb{F}_q)]$-submodule of $\mathrm{M}_2^0(\mathfrak{m}_{\mathbb{T}}/\mathfrak{m}_{\mathbb{T}}^2)$ of the form

$$M \simeq \underbrace{\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}_{\alpha} \oplus \underbrace{C_2 \oplus \cdots \oplus C_2}_{\beta},$$

for some $0 \leq \alpha \leq m$ and $0 \leq \beta \leq d(m-\alpha)$, where d denotes the degree of the field $\mathbb{F}_q$ and $C_2 \subseteq \mathbb{S}$ an order 2 subgroup of the scalar matrices. The number of traces in this case is $t = q^\alpha \cdot ((q-1)2^\beta + 1)$. Moreover, t determines α and β uniquely.

In section 3.3 we describe an algorithm that will allow us to determine the image of a Galois representation $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T}_f/\mathfrak{m}_f^2)$, attached to a normalised Hecke eigenform $f \in S_2(N, \varepsilon; \overline{\mathbb{F}}_p)$, satisfying the hypothesis previously mentioned. The idea is to compute, up to some bound, the number $\widetilde{t}$ of different traces (Hecke operators) that we find.

In sections 3.4 and 3.5 we compute many examples for $p \neq 2$ and $p = 2$, respectively. In the case $p \neq 2$, we already know that the number of traces that we are supposed to obtain is $t = q^{m+1}$. In this situation we will see that, in most of the examples that we computed, we have $m = 1$. The case with $p = 2$ is more complicated, and we show a large variety of examples with $m = 1, 2$ and 3. In this case, since we have several possibilities for the image of ρ_f, which we can distinguish by the number of different traces $\widetilde{t}$ computed, we can only "guess" the group that we obtain. However, we will see that the possible numbers of traces that can be obtained in each case are integers enough separated so that it is very likely that we can guess the right number of traces.

3.1 Hecke algebras mod $p \neq 2$

Let $\mathbb{F}_q$ denote a finite field of characteristic $p \neq 2$, and let $(\mathbb{T}, \mathfrak{m}_{\mathbb{T}})$ be a finite-dimensional local commutative $\mathbb{F}_q$-algebra equipped with the discrete topology, and with residue field $\mathbb{T}/\mathfrak{m}_{\mathbb{T}} \simeq \mathbb{F}_q$. In this section we will determine the image of a continuous representation $\rho : \Gamma \to \mathrm{GL}_2(\mathbb{T}/\mathfrak{m}_{\mathbb{T}}^2)$ of a profinite group Γ, under the assumption that the image of the residual representation $\overline{\rho} : \Gamma \to \mathrm{GL}_2(\mathbb{F}_q)$ is of the form $\mathrm{Im}(\overline{\rho}) = \mathrm{GL}_2^D(\mathbb{F}_q)$, where $D \subseteq \mathbb{F}_q^{\times}$ denotes the image of the determinant of $\overline{\rho}$.

To make the exposition of the results more clear, we will assume that $\mathfrak{m}_{\mathbb{T}}^2 = 0$ (instead of considering $\mathfrak{m}_{\mathbb{T}}/\mathfrak{m}_{\mathbb{T}}^2$).

Theorem 3.1.1. *Let $\mathbb{F}_q$ denote a finite field of characteristic $p \neq 2$ and $q = p^d$ elements, and suppose that $q \neq 3, 5$. Let $(\mathbb{T}, \mathfrak{m}_{\mathbb{T}})$ be a finite-dimensional local commutative $\mathbb{F}_q$-algebra equipped with the discrete topology, and with residue field $\mathbb{T}/\mathfrak{m}_{\mathbb{T}} \simeq \mathbb{F}_q$. Suppose that $\mathfrak{m}_{\mathbb{T}}^2 = 0$. Let Γ be a profinite group and let $\rho : \Gamma \to \mathrm{GL}_2(\mathbb{T})$ be a continuous representation such that*

(a) $\mathrm{Im}(\overline{\rho}) = \mathrm{GL}_2^D(\mathbb{F}_q)$, *where $\overline{\rho}$ denotes the reduction $\rho \bmod \mathfrak{m}_{\mathbb{T}}$ and $D := \mathrm{Im}(\det \circ \overline{\rho})$,*

(b) $\mathrm{Im}(\rho) \subseteq \mathrm{GL}_2^D(\mathbb{T})$,

(c) *$\mathbb{T}$ is generated as $\mathbb{F}_q$-algebra by the set of traces of ρ.*

Let $m := \dim_{\mathbb{F}_q} \mathfrak{m}_{\mathbb{T}}$ and let t be the number of different traces in $\mathrm{Im}(\rho)$. Then $t = q^{m+1}$ and

$$\mathrm{Im}(\rho) \simeq (\underbrace{\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}_{m}) \rtimes \mathrm{GL}_2^D(\mathbb{F}_q) \simeq \mathrm{GL}_2^D(\mathbb{T}).$$

Proof. By Cohen Structure Theorem (cf. [Eis95] Theorem 7.7) and the assumption that $\mathfrak{m}_{\mathbb{T}}^2 = 0$, we have that $\mathbb{T} \simeq \mathbb{F}_q[X_1, \ldots, X_m]/(X_i X_j)_{1 \leq i,j \leq m}$. Let $\pi : \mathbb{T} \to \mathbb{T}/\mathfrak{m}_{\mathbb{T}} \simeq \mathbb{F}_q$. Then $\ker \pi = \mathfrak{m}_{\mathbb{T}}$ is an $\mathbb{F}_q$-vector space of dimension m. Put $G := \mathrm{Im}(\rho) \subseteq \mathrm{GL}_2^D(\mathbb{T})$. By the assumptions on $\mathbb{F}_q$ we know (after Corollary 2.4.10) that $G \simeq M \rtimes \mathrm{GL}_2^D(\mathbb{F}_q)$ for some $\mathrm{GL}_2^D(\mathbb{F}_q)$-submodule $M \subseteq \mathrm{M}_2^0(\ker \pi) \simeq \underbrace{\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}_{m}$.

Since $p \neq 2$, we are in the case where $\mathrm{M}_2^0(\mathbb{F}_q)$ is a simple $\mathbb{F}_p[\mathrm{GL}_2(\mathbb{F}_q)]$-module, so by Lemma 2.2.3 we know that M is isomorphic to a direct sum of, a priori, $\alpha \leq m$ copies of $\mathrm{M}_2^0(\mathbb{F}_q)$. Let us count the number of traces of G (depending on α). Consider the following split exact sequence

$$\begin{array}{ccccccccc}
0 & \to & \mathrm{M}_2^0(\ker\pi) & \xrightarrow{\iota} & \mathrm{GL}_2^D(\mathbb{T}) & \xrightarrow{\pi} & \mathrm{GL}_2^D(\mathbb{F}_q) & \to & 1 \\
 & & \| & & \| & & \| & & \\
0 & \to & \overbrace{\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}^{m} & \to & \mathrm{GL}_2^D(\mathbb{F}_q[X_1,\ldots,X_m]/(X_iX_j)_{1\leq i,j\leq m}) & \to & \mathrm{GL}_2^D(\mathbb{F}_q) & \to & 1 \\
 & & \left(\left(\begin{smallmatrix} a_1 & b_1 \\ c_1 & a_1 \end{smallmatrix}\right),\ldots,\left(\begin{smallmatrix} a_m & b_m \\ c_m & a_m \end{smallmatrix}\right)\right) & \mapsto & \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) + \left(\begin{smallmatrix} a_1 & b_1 \\ c_1 & a_1 \end{smallmatrix}\right) X_1 + \ldots + \left(\begin{smallmatrix} a_m & b_m \\ c_m & a_m \end{smallmatrix}\right) X_m & & & & \\
 & & & & \left(\begin{smallmatrix} a_0 & b_0 \\ c_0 & d_0 \end{smallmatrix}\right) & \mapsfrom & \left(\begin{smallmatrix} a_0 & b_0 \\ c_0 & d_0 \end{smallmatrix}\right) & &
\end{array}$$

After a possible reordering of the variables X_i, for an element $\mu \in M \subseteq \mathrm{M}_2^0(\ker\pi)$ we have $\iota(\mu) = 1 + A_1X_1 + \ldots + A_\alpha X_\alpha$, where $A_i \in \mathrm{M}_2^0(\mathbb{F}_q)$ for $1 \leq i \leq \alpha$. Then for an element $g \in G$, we have $g = (1+\mu)h$, with $\mu \in M$ and $h \in \mathrm{GL}_2^D(\mathbb{F}_q)$, and

$$\mathrm{tr}(g) = \mathrm{tr}((1+\mu)h) = \mathrm{tr}(h) + \mathrm{tr}(A_1h)X_1 + \ldots + \mathrm{tr}(A_\alpha h)X_\alpha.$$

Let t denote the number of different traces in G. Then

$$t = \#\left\{\mathrm{tr}(h) + \sum_{i=1}^{\alpha} \mathrm{tr}(A_ih)X_i : A_i \in \mathrm{M}_2^0(\mathbb{F}_q), h \in \mathrm{GL}_2^D(\mathbb{F}_q)\right\}$$

$$= \#\{\mathrm{tr}(h) : h \in \mathrm{GL}_2^D(\mathbb{F}_q)\} \cdot \prod_{i=1}^{\alpha} \#\left\{\mathrm{tr}(A_ih)X_i : A_i \in \mathrm{M}_2^0(\mathbb{F}_q), h \in \mathrm{GL}_2^D(\mathbb{F}_q)\right\}$$

$$= q \cdot \prod_{i=1}^{\alpha} \#\{0, X_i, aX_i, \ldots, a^{q-1}X_i\} = q^{\alpha+1},$$

where a is some element in $\mathbb{F}_q$ of order $q-1$.

Finally, note that if we had $t = q^{\alpha+1}$, with $\alpha < m$, then we can assume, without loss of generality, that the set of traces of G is $T := \{a_0 + a_1X_1 + \ldots + a_\alpha X_\alpha \mid a_0, \ldots a_\alpha \in \mathbb{F}_q\}$ and by assumption, $\mathbb{T} = \langle T \rangle$. On the other hand, we have an isomorphism

$$\mathrm{GL}_2^D(\mathbb{T}) \simeq (\underbrace{\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}_{m}) \rtimes \mathrm{GL}_2^D(\mathbb{F}_q)$$

given by the previous split short exact sequence. In particular, we have that $X_{\alpha+1} \in T$, so $X_{\alpha+1}$ is a linear combination of $X_1, \ldots, X_\alpha$, which is a contradiction. □

Remark 3.1.2. Theorem 3.1.1 shows that if the field cut out by $\overline{\rho}$ admits some abelian extension (of the type we are considering), then it is a "big one". So the cases $m \geq 2$ will occur rarely.

In order to apply this result to Galois representations coming from modular forms, let us recall some notation introduced in the first chapter. Fix a level $N \geq 1$, a weight $k \geq 2$, a prime $p \nmid N$ and a Dirichlet character $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{F}}_p$. Let $\overline{\mathbb{T}}$ denote the Hecke algebra of $S_k(N, \varepsilon; \mathbb{F}_q)$ generated by the *good* operators T_ℓ, i.e. those with $\ell \nmid Np$. For a normalised Hecke eigenform

$f(z) = \sum_{n=0}^{\infty} a_n(f)q^n \in S_k(N, \varepsilon; \overline{\mathbb{F}}_p)$, whose coefficients generate the field $\mathbb{F}_q$, let $\mathfrak{m}_f := \ker \lambda_f$ denote the maximal ideal of $\overline{\mathbb{T}}$ given by the ring homomorphism

$$\lambda_f : \overline{\mathbb{T}} \to \mathbb{F}_q, \quad T_n \mapsto a_n(f).$$

Finally, we consider the local algebra $\mathbb{T}_f := \overline{\mathbb{T}}_{\mathfrak{m}_f}$, which we will refer to as the *local mod p Hecke algebra* associated to the mod p modular form f.

Corollary 3.1.3. *Fix integers $k \geq 2$, $N \geq 1$, an odd prime $p \nmid N$ and a Dirichlet character $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{F}}_p^\times$. Take a normalised eigenform $f(z) = \sum_{n=0}^{\infty} a_n(f)q^n \in S_k(N, \varepsilon; \overline{\mathbb{F}}_p)$, and let $\mathbb{F}_q$ denote the finite field generated by its coefficients. Let $\mathfrak{m}_f$ denote the maximal ideal of $\overline{\mathbb{T}}$ corresponding to f and let $\mathbb{T}_f$ denote the local mod p Hecke algebra associated to f.*

Let $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T}_f/\mathfrak{m}_f^2)$ be the Galois representation attached to f and assume that $\mathrm{Im}(\overline{\rho}_f) = \mathrm{GL}_2^D(\mathbb{F}_q)$, where $D = \mathrm{Im}(\det \circ \overline{\rho}_f)$ and $\overline{\rho}_f : G_{\mathbb{Q}} \to \mathrm{GL}_2^D(\mathbb{F}_q)$ denotes the attached residual Galois representation. Let $m := \dim_{\mathbb{F}_q} \mathfrak{m}_f/\mathfrak{m}_f^2$ and let t be the number of different traces in $\mathrm{Im}(\rho_f)$. Then $t = q^{m+1}$ and

$$\mathrm{Im}(\rho_f) \simeq (\underbrace{\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}_{m}) \rtimes \mathrm{GL}_2^D(\mathbb{F}_q).$$

Proof. Since $\mathrm{Im}(\overline{\rho}_f) = \mathrm{GL}_2^D(\mathbb{F}_q)$, it follows that $\mathrm{Im}(\rho_f) \subseteq \mathrm{GL}_2^D(\mathbb{T}_f/\mathfrak{m}_f^2)$. Moreover, the Hecke algebra $\mathbb{T}_f$ is, by definition, generated by the set of traces of ρ_f. Thus we are in the hypothesis of Theorem 3.1.1 and the result follows. □

3.2 Hecke algebras mod 2

Let $\mathbb{F}_q$ denote a finite field of characteristic 2, and let $(\mathbb{T}, \mathfrak{m}_{\mathbb{T}})$ be a finite-dimensional local commutative $\mathbb{F}_q$-algebra equipped with the discrete topology, and with residue field $\mathbb{T}/\mathfrak{m}_{\mathbb{T}} \simeq \mathbb{F}_q$. In this section we will prove the analogous result of the previous section in characteristic 2. We will determine the image of a continuous representation $\rho : \Gamma \to \mathrm{GL}_2(\mathbb{T}/\mathfrak{m}_{\mathbb{T}}^2)$ of a profinite group Γ, under the assumption that the image of the residual representation $\overline{\rho} : \Gamma \to \mathrm{GL}_2(\mathbb{F}_q)$ is of the form $\mathrm{Im}(\overline{\rho}) = \mathrm{GL}_2^D(\mathbb{F}_q)$, where $D \subseteq \mathbb{F}_q^\times$ denotes the image of the determinant of $\overline{\rho}$, and $q \geq 4$.

As we will see, the case of characteristic 2 is more complicated, due to the fact that the module $\mathrm{M}_2^0(\mathbb{F}_q)$ of trace 0 matrices is no longer a simple module. Thus more work needs to be done. We start with a technical lemma that will be needed afterwards.

Lemma 3.2.1. *Let k be a field with trivial Brauer group, G a finite group and M an indecomposable $k[G]$-module. Suppose that M has a semisimple submodule $S \subseteq M$ such that M/S is simple, and such that all the other submodules of M are contained in S. Consider a submodule $N \subseteq \bigoplus_{i=1}^n M$. Then $N \simeq N_1 \oplus \ldots \oplus N_n$, with $N_i \subseteq M$ submodule.*

Proof. For any module M, denote by M^n the direct sum $\oplus_{i=1}^n M$. Let T denote the simple module M/S and consider the projection $\pi : M^n \twoheadrightarrow T^n$, which gives a commutative diagram

$$\begin{array}{ccccccccc} 0 & \to & S^n & \to & M^n & \overset{\pi}{\twoheadrightarrow} & T^n & \to & 0 \\ & & \uparrow & & \uparrow \iota & & \uparrow \iota & & \\ 0 & \to & N \cap S^n & \to & N & \overset{\pi}{\twoheadrightarrow} & \pi(N) & \to & 0. \end{array}$$

Note that, since T^n is a semisimple module, by Lemma 2.2.3 we have that $\pi(N) \simeq T^k$, for some $0 \leq k \leq n$. Let $\alpha : T^k \to \pi(N)$ denote this isomorphism. We will see that we can assume that $\pi(N)$ maps onto the first k copies of T (after isomorphism). Consider the composition

$$\varphi_{ij} : T \overset{\iota_j}{\hookrightarrow} T^k \overset{\alpha}{\to} \pi(N) \overset{\iota}{\hookrightarrow} T^n \overset{\pi_i}{\twoheadrightarrow} T,$$

where ι_j denotes the natural inclusion of T into the j-th component of T^k, for $1 \leq j \leq k$, and π_i denotes the natural projection from T^n to the ith component T, for $1 \leq i \leq n$. Now, since φ_{ij} is an endomorphism of a simple $k[G]$-module, by Schur's lemma (cf. [CR81], 3.17) we have that $\mathrm{End}_{k[G]}(M)$ is a division ring. Since we are assuming that the Brauer group of k is trivial, this gives that $\mathrm{End}_k(M) = k$, so $\mathrm{End}_{k[G]}(M) \subseteq k$. Thus we have that φ_{ij} is just multiplication by a scalar, so we can write $\varphi_{ij}(t) = a_{ij}t$, for $a_{ij} \in k,\ t \in T$. We then can express $\varphi := \iota \circ \alpha$ as

$$\begin{array}{rccc} \varphi : & T^k & \to & T^n \\ & \begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_k \end{pmatrix} & \mapsto & \begin{pmatrix} a_{11} & \dots & a_{1k} \\ a_{21} & \dots & a_{2k} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nk} \end{pmatrix} \begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_k \end{pmatrix}. \end{array}$$

Since φ is injective, the matrix $A := \begin{pmatrix} a_{11} & \dots & a_{1k} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nk} \end{pmatrix}$ has rank k. Using Gauß elimination, we can find an invertible $n \times n$ matrix C such that

$$CA = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 1 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}.$$

Note that $\cdot C : M^n \to M^n$ and $\cdot C : T^n \to T^n$ are isomorphisms of $k[G]$-modules. By construction we obtain

$$C \cdot \iota(\pi(N)) = C \cdot \iota \cdot \alpha(T^k) = C \cdot \varphi(T^k) = \underbrace{T \oplus \ldots \oplus T}_{k} \oplus \underbrace{0 \oplus \ldots \oplus 0}_{n-k}.$$

So, without loss of generality, we can assume that

$$\pi(N) = \underbrace{T \oplus \ldots \oplus T}_{k} \oplus \underbrace{0 \oplus \ldots \oplus 0}_{n-k} \subseteq T^n.$$

Let T_i denote the ith component of T in T^n. Consider the submodule $N \cap M_i \subseteq M$, for $1 \leq i \leq n$. For $1 \leq i \leq k$, we have that $\pi(N) \cap T_i = T$, which implies that $S \subsetneq N \cap M_i$, and by the assumptions on M, we have $N \cap M_i = M$. For $k+1 \leq i \leq n$, we have that $\pi(N) \cap T_i = 0$, and thus $N \cap M_i \subseteq S$.

If we put $S = S_1 \oplus \ldots \oplus S_t$, with $S_i \subseteq S$ simple modules for $1 \leq i \leq t$, we obtain

$$N \simeq \underbrace{M \oplus \ldots \oplus M}_{k} \oplus L,$$

where $L \subseteq S^l$, for some $0 \leq l \leq n-k$, is isomorphic to a direct sum of a subset of the modules $S_1, \ldots, S_l$ (after Lemma 2.2.2). □

Using the previous lemma we can prove an analog of Theorem 3.1.1 for characteristic 2. As before, instead of working with the algebra $\mathbb{T}/\mathfrak{m}_{\mathbb{T}}^2$, we will just assume that $\mathfrak{m}_{\mathbb{T}}^2 = 0$.

Theorem 3.2.2. *Let $\mathbb{F}_q$ be a finite field of characteristic 2 and degree $d \geq 2$. Let $(\mathbb{T}, \mathfrak{m}_{\mathbb{T}})$ be a finite-dimensional local commutative $\mathbb{F}_q$-algebra equipped with the discrete topology, and with residue field $\mathbb{T}/\mathfrak{m}_{\mathbb{T}} \simeq \mathbb{F}_q$. Suppose that $\mathfrak{m}_{\mathbb{T}}^2 = 0$. Let Γ be a profinite group and consider a continuous representation $\rho : \Gamma \to \mathrm{GL}_2(\mathbb{T})$ such that*

(a) $\mathrm{Im}(\overline{\rho}) = \mathrm{GL}_2^D(\mathbb{F}_q)$, *where $\overline{\rho}$ denotes the reduction $\rho \bmod \mathfrak{m}_{\mathbb{T}}$ and $D := \mathrm{Im}(\det \circ \overline{\rho})$,*

(b) $\mathrm{Im}(\rho) \subseteq \mathrm{GL}_2^D(\mathbb{T})$,

(c) *$\mathbb{T}$ is generated as $\mathbb{F}_q$-algebra by the set of traces of ρ.*

Let $m := \dim_{\mathbb{F}_q} \mathfrak{m}_{\mathbb{T}} \geq 1$ and let t be the number of different traces in $\mathrm{Im}(\rho)$. Then

$$t = q^{\alpha} \cdot ((q-1)2^{\beta} + 1), \text{ for some } 0 \leq \alpha \leq m \text{ and } 0 \leq \beta \leq d(m-\alpha),$$

and in this case $\mathrm{Im}(\rho) \simeq M \rtimes \mathrm{GL}_2^D(\mathbb{F}_q)$, where M is an $\mathbb{F}_2[\mathrm{GL}_2^D(\mathbb{F}_q)]$-submodule of $\mathrm{M}_2^0(\mathfrak{m}_{\mathbb{T}})$ of the form

$$M \simeq \underbrace{\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}_{\alpha} \oplus \underbrace{C_2 \oplus \cdots \oplus C_2}_{\beta},$$

where $C_2 \subseteq \mathbb{S}$ is a subgroup of order 2 of the scalar matrices. Moreover, M is determined uniquely by t up to isomorphism.

Proof. By Cohen Structure Theorem (cf. [Eis95] Theorem 7.7) and the assumption that $\mathfrak{m}_{\mathbb{T}}^2 = 0$, we have that $\mathbb{T} \simeq \mathbb{F}_q[X_1, \ldots, X_m]/(X_i X_j)_{1 \leq i,j \leq m}$. Let $\pi : \mathbb{T} \to \mathbb{T}/\mathfrak{m}_{\mathbb{T}} \simeq \mathbb{F}_q$. Then $\ker \pi = \mathfrak{m}_{\mathbb{T}}$ is an $\mathbb{F}_q$-vector space of dimension m. Let $G := \mathrm{Im}(\rho) \subseteq \mathrm{GL}_2^D(\mathbb{T})$. By the assumptions on $\mathbb{F}_q$ we can apply Corollary 2.4.10 and obtain that $G \simeq M \rtimes \mathrm{GL}_2^D(\mathbb{F}_q)$ for some $\mathbb{F}_2[\mathrm{GL}_2^D(\mathbb{F}_q)]$-submodule $M \subseteq \mathrm{M}_2^0(\ker \pi) \simeq \underbrace{\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}_{m}$.

Since $p = 2$, we are in the case where $\mathrm{M}_2^0(\mathbb{F}_q)$ is indecomposable, it contains the semisimple $\mathbb{F}_2[\mathrm{GL}_2^D(\mathbb{F}_q)]$-module $\mathbb{S} = \{\lambda \mathrm{Id}_2 : \lambda \in \mathbb{F}_q\}$, and $\mathrm{M}_2^0(\mathbb{F}_q)/\mathbb{S}$ is simple (cf. Lemma 2.2.2). Thus we can apply Lemma 3.2.1 and we obtain that

$$M \simeq N_1 \oplus \ldots \oplus N_m, \quad \text{with } N_i \subseteq \mathrm{M}_2^0(\mathbb{F}_q),$$

where each N_i is either $\mathrm{M}_n^0(\mathbb{F}_q)$ or an $\mathbb{F}_2$-subspace of $\mathbb{S}$, for $1 \leq i \leq m$. Since the indecomposable subspaces of $\mathbb{S}$ are of the form $C_2 \simeq \{0, \lambda\}$ with $\lambda \in \mathbb{S}$, we have $\mathbb{S} \simeq C_2^d$, and

$$M \simeq \underbrace{\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}_{\alpha} \oplus \underbrace{C_2 \oplus \cdots \oplus C_2}_{\beta}, \quad 0 \leq \alpha \leq m,\ 0 \leq \beta \leq d(m-\alpha).$$

Consider the following split short exact sequence:

$$\begin{array}{ccccccccc}
0 & \to & \mathrm{M}_2^0(\ker\pi) & \xrightarrow{\iota} & \mathrm{GL}_2^D(\mathbb{T}) & \xrightarrow{\pi} & \mathrm{GL}_2^D(\mathbb{F}_q) & \to & 1 \\
 & & \| & & \| & & \| & & \\
0 & \to & \overbrace{\mathrm{M}_2^0(\mathbb{F}_q)\oplus\ldots\oplus\mathrm{M}_2^0(\mathbb{F}_q)}^{m} & \to & \mathrm{GL}_2^D(\mathbb{F}_q[X_1,\ldots,X_m]/(X_iX_j)_{1\le i,j\le m}) & \to & \mathrm{GL}_2^D(\mathbb{F}_q) & \to & 1 \\
 & & \left(\left(\begin{smallmatrix}a_1 & b_1\\ c_1 & a_1\end{smallmatrix}\right),\ldots,\left(\begin{smallmatrix}a_m & b_m\\ c_m & a_m\end{smallmatrix}\right)\right) & \mapsto & \left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)+\left(\begin{smallmatrix}a_1 & b_1\\ c_1 & a_1\end{smallmatrix}\right)X_1+\ldots+\left(\begin{smallmatrix}a_m & b_m\\ c_m & a_m\end{smallmatrix}\right)X_m & & & & \\
 & & & & \left(\begin{smallmatrix}a_0 & b_0\\ c_0 & d_0\end{smallmatrix}\right) & \leftarrow\!\shortmid & \left(\begin{smallmatrix}a_0 & b_0\\ c_0 & d_0\end{smallmatrix}\right) & &
\end{array}$$

In this setting, after a possible reordering of the variables X_i, for an element $\mu\in M$ we have

$$\iota(\mu)=1+\mu=1+A_1X_1+\ldots+A_\alpha X_\alpha+B_1X_{\alpha+1}+\ldots+B_sX_m,$$

where

$$A_k\in N_k\simeq\mathrm{M}_2^0(\mathbb{F}_q),\ \text{for } 1\le k\le\alpha,$$

$$B_k=\left(\begin{smallmatrix}b_k & 0\\ 0 & b_k\end{smallmatrix}\right)\in N_{\alpha+k}\simeq\underbrace{C_2\oplus\ldots\oplus C_2}_{e_k}\ \text{for } 1\le k\le s=m-\alpha,\ \text{and}\ \sum_{k=1}^{s}e_k=\beta.$$

We want to compute the number of different traces in G depending on the module M. For an element $g\in G$ we have $g=(1+\mu)h$ with $\mu\in M$ and $h\in\mathrm{GL}_2^D(\mathbb{F}_q)$, and

$$\begin{aligned}
\mathrm{tr}(g)&=\mathrm{tr}((1+\mu)h)\\
&=\mathrm{tr}(h)+\mathrm{tr}(A_1h)X_1+\ldots+\mathrm{tr}(A_\alpha h)X_\alpha+\mathrm{tr}(B_1h)X_{\alpha+1}+\ldots+\mathrm{tr}(B_sh)X_m\\
&=\mathrm{tr}(h)+\mathrm{tr}(A_1h)X_1+\ldots+\mathrm{tr}(A_\alpha h)X_\alpha+\mathrm{tr}(h)b_1X_{\alpha+1}+\ldots\mathrm{tr}(h)b_sX_m\\
&=\mathrm{tr}(A_1h)X_1+\ldots+\mathrm{tr}(A_\alpha h)X_\alpha+\mathrm{tr}(h)(1+b_1X_{\alpha+1}+\ldots+b_sX_m).
\end{aligned}$$

Let t denote the number of different traces in G. Then

$$\begin{aligned}
t&=\#\left\{\sum_{k=1}^{\alpha}\mathrm{tr}(A_kh)X_k+\mathrm{tr}(h)(1+\sum_{k=1}^{s}b_kX_{\alpha+k}):A_k\in\mathrm{M}_2^0(\mathbb{F}_q),b_k\in C_2^{e_k},\ h\in\mathrm{GL}_2^D(\mathbb{F}_q)\right\}\\
&=\#\left\{\sum_{k=1}^{\alpha}a_kX_k+\mathrm{tr}(h)(1+\sum_{k=1}^{s}b_kX_{\alpha+k}):a_k\in\mathbb{F}_q,b_k\in C_2^{e_k},\ h\in\mathrm{GL}_2^D(\mathbb{F}_q)\right\}\\
&=\underbrace{\#\left\{\sum_{k=1}^{\alpha}a_kX_k:a_k\in\mathbb{F}_q\right\}}_{t_1}\cdot\underbrace{\#\left\{\mathrm{tr}(h)(1+\sum_{k=1}^{s}b_kX_{\alpha+k}):b_k\in C_2^{e_k},h\in\mathrm{GL}_2^D(\mathbb{F}_q)\right\}}_{t_2},
\end{aligned}$$

where $t_1=q^\alpha$ and

$$\begin{aligned}
t_2&=\#\{0\}+\#\{x\cdot(1+b_{1j_1}X_{\alpha+1}+\ldots+b_{sj_s}X_m):b_{kj_k}\in C_2^{e_k},x\in\mathbb{F}_q^\times\}\\
&=1+(q-1)\cdot2^{e_1}\cdot\ldots\cdot2^{e_s}=1+(q-1)\cdot2^{\sum e_k}=1+(q-1)2^\beta.
\end{aligned}$$

So we obtain the formula

$$t = q^{\alpha} \cdot (1 + (q-1)2^{\beta}).$$

Finally, let us prove that the number of traces determines the module M up to isomorphism. Let $t' = q^{\alpha'} \cdot (1 + (q-1)2^{\beta'})$. Let us check that if $t = t'$ then one has $\alpha = \alpha'$ and $\beta = \beta'$. Recall that $q = 2^d$. Suppose that $\alpha \geq \alpha'$. Then

$$q^{\alpha}(1 + (q-1)2^{\beta}) = q^{\alpha'}(1 + (q-1)2^{\beta'}) \Leftrightarrow \underbrace{q^{\alpha-\alpha'}(1 + (q-1)2^{\beta})}_{(L)} = \underbrace{1 + (q-1)2^{\beta'}}_{(R)}.$$

If $\beta' > 0$ then $(R) \equiv 1 \bmod 2$, so $\alpha = \alpha'$ and then $\beta = \beta'$. If $\beta' = 0$ then $(R) = q$. Since $1 + (q-1)2^{\beta} \geq q$ and $q^{\alpha-\alpha'} \geq 1$, we necessarily have $\beta = 0 = \beta'$ and $\alpha = \alpha'$. □

Corollary 3.2.3. *Fix an integer $k \geq 2$, an odd integer $N \geq 1$ and a Dirichlet character $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^{\times} \to \overline{\mathbb{F}}_2^{\times}$. Take a normalised eigenform $f(z) = \sum_{n=0}^{\infty} a_n(f)q^n \in S_k(N, \varepsilon; \overline{\mathbb{F}}_2)$, and let $\mathbb{F}_q$ denote the finite field generated by its coefficients, of degree $d \geq 2$. Let $\mathfrak{m}_f$ denote the maximal ideal of $\overline{\mathbb{T}}$ corresponding to f and let $\mathbb{T}_f$ denote the local mod p Hecke algebra associated to f.*

Let $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2^D(\mathbb{T}_f/\mathfrak{m}_f^2)$ be the Galois representation attached to $\mathfrak{m}_f/\mathfrak{m}_f^2$ and assume that $\mathrm{Im}(\overline{\rho}_f) = \mathrm{GL}_2^D(\mathbb{F}_q)$, where $D = \mathrm{Im}(\det \circ \overline{\rho}_f)$ and $\overline{\rho}_f : G_{\mathbb{Q}} \to \mathrm{GL}_2^D(\mathbb{F}_q)$ denotes the residual representation. Let $m := \dim_{\mathbb{F}_q} \mathfrak{m}_f/\mathfrak{m}_f^2$ and let t be the number of traces in $\mathrm{Im}(\rho_f)$. Then t is of the form

$$t = q^{\alpha} \cdot ((q-1)2^{\beta} + 1), \text{ for some } 0 \leq \alpha \leq m \text{ and } 0 \leq \beta \leq d(m - \alpha),$$

and in this case $\mathrm{Im}(\rho_f) \simeq M \rtimes \mathrm{GL}_2^D(\mathbb{F}_q)$, where M is an $\mathbb{F}_2[\mathrm{GL}_2^D(\mathbb{F}_q)]$-submodule of $\mathrm{M}_2^0(\mathfrak{m}_f/\mathfrak{m}_f^2)$ of the form

$$M := \underbrace{\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}_{\alpha} \oplus \underbrace{C_2 \oplus \cdots \oplus C_2}_{\beta},$$

with $C_2 \subseteq \mathbb{S}$ a subgroup with 2 elements.

Proof. Apply Theorem 3.2.2. □

3.3 Computation of images of Galois representations with values in mod p Hecke algebras

Let p be a prime. In this section we explain how to compute local mod p Hecke algebras $(\mathbb{T}_f, \mathfrak{m}_f)$ associated to a mod p modular form f such that the corresponding Galois representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T}_f)$ satisfies the hypothesis of Corollary 3.1.3 if $p \neq 2$ or Corollary 3.2.3 if $p = 2$.

We use the packages `ArtinAlgebras` and `HeckeAlgebras` already implemented in Magma (cf. [Wie]) to compute the mentioned Hecke algebras. Moreover we have implemented an algorithm that allows us to use the results in the previous section in order to compute the image of these Hecke algebras. We next give a description of the algorithm.

First we fix the following data: a level $N \geq 1$, a weight $k \geq 2$, a prime p and a character $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^{\times} \to \overline{\mathbb{F}}_p^{\times}$. Then with the function `HeckeAlgebras` we obtain all local Hecke algebras

(up to Galois conjugacy) in the specified level and weight for the given Dirichlet character. More concretely, the output of the function `HeckeAlgebras` consists on 5 values `A,B,C,D,E`. The data in `A` is a list of records describing the local Hecke algebra factors, `B` is a list that contains the local Hecke algebra factors as matrix algebras, `C` is the space of modular symbols used in the computations, `D` is a tuple with the base change tuples describing the local Hecke factors and `E` is a tuple of all computed Hecke operators for each local factor of the Hecke algebra.

We fix a bound b up to which, for each local Hecke factor, we compute its Hecke operators. For a fixed local Hecke factor, let $\mathbb{T}_f$ denote the subalgebra generated by all Hecke operators away from Np. We then check if the associated residual Galois representation $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_q)$ has *big image*, i.e. if the image of the representation contains $\mathrm{SL}_2(\mathbb{F}_q)$, where $\mathbb{F}_q$ denotes the finite field generated by the coefficients of f. In the affirmative case, we keep the local Hecke algebra. Once we have found all local Hecke algebras that give rise to a Galois representation with big image, we need to check if they satisfy the hypothesis of Corollary 3.1.3 or Corollary 3.2.3.

Fix a local Hecke algebra $\mathbb{T}_f$ and let $f \in S_k(N, \varepsilon; \mathbb{F}_q)$ be the mod p eigenform associated to it, where $\mathbb{F}_q$ is the finite field generated by the coefficients of f. In order to apply the mentioned results, we need that $q \geq 4$ and $q \neq 5$. Let $\mathfrak{m}_f$ denote the maximal ideal of $\mathbb{T}_f$ and let $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T}_f)$ denote the Galois representation attached to f. Suppose that we have computed

$$\mathrm{Im}(\overline{\rho}_f) = \mathrm{GL}_2^D(\mathbb{F}_q), \text{ where } \overline{\rho}_f := \rho_f \bmod \mathfrak{m}_f,$$

and $D = \mathrm{Im}(\det \circ \overline{\rho})$. Then we know that $\mathrm{Im}(\rho) \subseteq \mathrm{GL}_2^D(\mathbb{T}_f)$. Consider the algebra $(\mathbb{T}, \mathfrak{m}) := (\mathbb{T}_f/\mathfrak{m}_f^2, \mathfrak{m}_f/\mathfrak{m}_f^2)$ (so we have, $\mathfrak{m}^2 = 0$) and consider the group

$$G := \mathrm{Im}(\rho_f) \bmod \mathfrak{m}_f^2 \subseteq \mathrm{GL}_2^D(\mathbb{T}).$$

Let t denote the number of different traces in G and let $m = \dim_{\mathbb{F}_q} \mathfrak{m}$. Then Corollary 3.1.3 tells us that, if $p \neq 2$, then $t = q^{m+1}$, and Corollary 3.2.3 tells us that, if $p = 2$, then $t = q^{\alpha} \cdot ((q-1)2^{\beta} + 1)$, for some $0 \leq \alpha \leq m$ and $0 \leq \beta \leq d(m - \alpha)$.

Let $\{T_1, \ldots, T_b\}$ denote the Hecke operators that we have computed earlier, where b denotes the bound fixed before. Since we have the relation

$$\mathrm{tr}(\rho_f(\mathrm{Frob}_\ell)) = T_\ell, \quad \text{for } \ell \nmid Np,$$

in order to compute the number of different traces in $\mathbb{T}$ we just need to compute the number $\widetilde{t}$ of different Hecke operators that we have. This number, if the bound is high enough, coincides with t, and as we saw in the previous two sections, the knowledge of t is enough to determine the group G.

As shown in section 3.1, when the characteristic p is different from 2, we already know the number t. The situation is completely different when we are in characteristic $p = 2$. In this case, as we have seen in section 3.2, we have more than one possibility for the number of traces t. Since we have no way of knowing when we have found all the different traces, the number $\widetilde{t}$ that we compute is then just an approximation of t. Nevertheless, as we will see in section 3.5, the *theoretical* number of traces t can only be one of few in a list that we will determine. Moreover, the integers in this list are separated enough so we can be *almost* sure, once $\widetilde{t}$ is computed, which t is highly likely to coincide with $\widetilde{t}$. We will see examples of this in section 3.5

3.4 Examples coming from mod $p \neq 2$ modular forms

Fix a level $N \geq 1$, a weight $k \geq 2$, a prime $p \neq 2$ and a character $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{F}}_p^\times$. Take a normalised Hecke eigenform $f \in S_k(N, \varepsilon; \overline{\mathbb{F}}_p)$ and let $\mathbb{F}_q$ denote the finite field generated by its coefficients over $\mathbb{F}_p$. Let $\mathbb{T}_f$ denote the attached local mod p Hecke $\mathbb{F}_q$-algebra of the fixed level, weight and character, which can be computed as explained in the previous section. Suppose that $q = p^d \neq 3, 5$.

Let $\mathfrak{m}_f$ denote the maximal ideal of $\mathbb{T}_f$. Let $\rho_f : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{T}_f)$ denote the attached Galois representation and suppose that $\mathrm{Im}(\overline{\rho}_f) = \mathrm{GL}_2^D(\mathbb{F}_q)$, where $\overline{\rho}_f := \rho_f \bmod \mathfrak{m}_f$ and $D = \mathrm{Im}(\det \circ \overline{\rho})$. Let $(\mathbb{T}, \mathfrak{m}) := (\mathbb{T}_f/\mathfrak{m}_f^2, \mathfrak{m}_f/\mathfrak{m}_f^2)$, and denote by m the dimension of $\mathfrak{m}$ over $\mathbb{F}_q$. Let $G := \mathrm{Im}(\rho_f) \bmod \mathfrak{m}_f^2 \subseteq \mathrm{GL}_2^D(\mathbb{T})$. Under these assumptions we are in the situation of Corollary 3.1.3, so we know that

$$G \simeq (\underbrace{\mathrm{M}_2^0(\mathbb{F}_p) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}_{m}) \rtimes \mathrm{GL}_2^D(\mathbb{F}_q).$$

In the following tables we summarise the examples that we have found, using the algorithm described before, in the following cases:

- $p = 3$, $k = 2$, $2 \leq d \leq 4$, $1 \leq N \leq 1500$.
- $p = 5$, $k = 2$, $2 \leq d \leq 4$, $1 \leq N \leq 1000$.
- $p = 7$, $k = 2$, $1 \leq d \leq 4$, $1 \leq N \leq 1000$.
- $p = 7$, $k = 3$, $1 \leq d \leq 4$, $1 \leq N \leq 600$.
- $p = 7$, $k = 5$, $1 \leq d \leq 4$, $1 \leq N \leq 600$.

We only consider examples with $m \geq 1$.

As explained in section 3.3, to determine the group G we compute the number of different traces (or Hecke operators) $\widetilde{t}$ up to a bound b that we fix. In the examples that we compute, this bound ranges between 1000 and 5000 (depending on the level). Since in this case we already know the number t of traces that we are supposed to obtain, we do not need to compute very far, and we normally find $\widetilde{t} < t$.

Examples 3.4.1. Let us give a some concrete examples with all details. Fix $k = 2$ and $p = 3$. All the examples that we found in this characteristic have $m = \dim_{\mathbb{F}_q} \mathfrak{m} = 1$.

(1) The first level in which we find an example fulfilling the previous hypothesis is $N = 203$. In this case the degree of $\mathbb{F}_q$ is $d = 2$. We fix the bound $b = 1000$, and we find $\widetilde{t} = 68$, quite close to the actual number of traces t, which is $t = 9^2 = 81$. If we compute up to $b = 2000$, we find $\widetilde{t} = 79$, and if we compute up to $b = 3000$, we find $\widetilde{t} = 80$. Finally, if we set the bound $b = 4000$ (up to 550 primes), we find all the 81 traces.

(2) If we look for an example in which the degree of the field $\mathbb{F}_q$ is $d = 3$, the first level in which we find something is $N = 451$. In this case we fix the bound $b = 1000$, and we find $\widetilde{t} = 145$ (from 168 primes up to 1000), already quite far from the theoretical number of traces $t = 27^2 = 729$.

(3) If we look for an example in which the degree of the field $\mathbb{F}_q$ is $d = 4$, the first level in which something appears is $N = 1010$. We fix the bound $b = 5000$, and we find $\widetilde{t} = 640$, very far away from the theoretical number of traces $t = (3^4)^2 = 6561$.

Remark 3.4.2. Note that although we did not impose any condition on m (a part from being greater than 0), most of the Hecke algebras that we find have $\dim_{\mathbb{F}_q} \mathfrak{m} = 1$. We only found few examples with $\dim_{\mathbb{F}_q} \mathfrak{m} = 2$, and none with $\dim_{\mathbb{F}_q} \mathfrak{m} \geq 3$.

Example 3.4.3. In characteristic $p = 7$ and weight $k = 2$ we start to find examples with $m = \dim_{\mathbb{F}_q} \mathfrak{m} = 2$. In characteristic 7 we can look for examples where the degree of the field $\mathbb{F}_q$ is $d = 1$. In this case, the first example that we find is in level $N = 258$. Here we take $b = 1500$, and we find $\widetilde{t} = 172$. The theoretical number of traces t that we would find in this case, if we compute far enough, is $t = 7^3 = 343$.

3.4.1 Examples with $m = 1$

In tables 3.1, 3.2 and 3.3 we list the examples that we have computed in characteristic $p = 3$ and 5 where the dimension of $\mathfrak{m}$ is $m = 1$. We group the examples that have the same characteristic, the same degree d and the same weight k together, and we separate those that have trivial character ε from those that do not (just for convenience). We list, with this data fixed, the levels that we find satisfying the required hypothesis described before.

Whenever we find two eigenforms f in the same space $S_k(N, \varepsilon; \mathbb{F}_q)$ that have the same coefficients (in the good primes), we denote it by writing $2\times$ in front of the level.

$p=3$, $d=2$				
N				
t	$k=2$, $\varepsilon=1$			
81	$203 = 7 \cdot 29$	$707 = 7 \cdot 101$	$2 \times 995 = 5 \cdot 199$	$1178 = 2 \cdot 19 \cdot 31$
	293	$710 = 2 \cdot 5 \cdot 71$	$995 = 5 \cdot 199$	$1211 = 7 \cdot 173$
	$2 \times 334 = 2 \cdot 167$	$778 = 2 \cdot 389$	$2 \times 998 = 2 \cdot 499$	$1226 = 2 \cdot 563$
	$385 = 5 \cdot 7 \cdot 11$	$778 = 2 \cdot 389$	$998 = 2 \cdot 499$	$2 \times 1238 = 2 \cdot 619$
	389	$778 = 2 \cdot 389$	$1015 = 5 \cdot 7 \cdot 29$	$1246 = 2 \cdot 7 \cdot 89$
	$391 = 17 \cdot 23$	$779 = 19 \cdot 41$	$2 \times 1030 = 2 \cdot 5 \cdot 103$	$2 \times 1247 = 29 \cdot 43$
	$2 \times 398 = 2 \cdot 199$	$793 = 13 \cdot 61$	$1037 = 17 \cdot 61$	$2 \times 1262 = 2 \cdot 631$
	$2 \times 406 = 2 \cdot 7 \cdot 29$	$803 = 11 \cdot 73$	$1045 = 5 \cdot 11 \cdot 19$	$1265 = 5 \cdot 11 \cdot 23$
	$406 = 2 \cdot 7 \cdot 29$	$803 = 11 \cdot 73$	$1046 = 2 \cdot 523$	$1265 = 5 \cdot 11 \cdot 23$
	$407 = 11 \cdot 37$	809	1049	$1270 = 2 \cdot 5 \cdot 127$
	$407 = 11 \cdot 37$	$814 = 2 \cdot 11 \cdot 37$	$1054 = 2 \cdot 17 \cdot 31$	1277
	433	$826 = 2 \cdot 7 \cdot 59$	$1055 = 5 \cdot 211$	1283
	$437 = 19 \cdot 23$	$2 \times 835 = 5 \cdot 167$	1061	$1286 = 2 \cdot 643$
	$437 = 19 \cdot 23$	839	$1066 = 2 \cdot 13 \cdot 41$	1289
	$466 = 2 \cdot 233$	$842 = 2 \cdot 421$	$1067 = 11 \cdot 97$	$1298 = 2 \cdot 11 \cdot 59$
	$469 = 7 \cdot 67$	857	$1067 = 11 \cdot 97$	$1343 = 17 \cdot 79$
	$515 = 5 \cdot 103$	859	$1073 = 29 \cdot 37$	$1355 = 5 \cdot 271$
	$566 = 2 \cdot 283$	859	$2 \times 1082 = 2 \cdot 541$	$1357 = 23 \cdot 59$
	587	$874 = 2 \cdot 19 \cdot 23$	1097	$2 \times 1370 = 2 \cdot 5 \cdot 137$
	$2 \times 598 = 2 \cdot 13 \cdot 23$	$2 \times 898 = 2 \cdot 449$	$1102 = 2 \cdot 19 \cdot 29$	$1387 = 19 \cdot 73$
	$598 = 2 \cdot 13 \cdot 23$	$2 \times 902 = 2 \cdot 11 \cdot 41$	1103	$1391 = 13 \cdot 107$
	$602 = 2 \cdot 7 \cdot 43$	$902 = 2 \cdot 11 \cdot 41$	$1105 = 5 \cdot 13 \cdot 17$	$1393 = 7 \cdot 199$
	617	$913 = 11 \cdot 83$	$2 \times 1114 = 2 \cdot 557$	1409
	$626 = 2 \cdot 313$	$923 = 13 \cdot 71$	$1130 = 2 \cdot 5 \cdot 113$	$2 \times 1414 = 2 \cdot 7 \cdot 101$
	631	$2 \times 946 = 2 \cdot 11 \cdot 43$	$2 \times 1135 = 5 \cdot 227$	$1414 = 2 \cdot 7 \cdot 101$
	$2 \times 667 = 23 \cdot 29$	$955 = 5 \cdot 191$	$1147 = 31 \cdot 37$	$1442 = 2 \cdot 7 \cdot 103$
	$2 \times 674 = 2 \cdot 337$	$958 = 2 \cdot 479$	$1147 = 31 \cdot 37$	$1486 = 2 \cdot 743$
	$674 = 2 \cdot 337$	$962 = 2 \cdot 13 \cdot 37$	$2 \times 1162 = 2 \cdot 7 \cdot 83$	
	$689 = 13 \cdot 53$	$962 = 2 \cdot 13 \cdot 37$	$1177 = 11 \cdot 107$	
	$k=2$, $\varepsilon \neq 1$			
	$305 = 5 \cdot 61$	$731 = 17 \cdot 43$	$1015 = 5 \cdot 7 \cdot 29$	1201
	$305 = 5 \cdot 61$	$754 = 2 \cdot 13 \cdot 29$	$1015 = 5 \cdot 7 \cdot 29$	$1226 = 2 \cdot 613$
	$346 = 2 \cdot 173$	$754 = 2 \cdot 13 \cdot 29$	$1015 = 5 \cdot 7 \cdot 29$	$1226 = 2 \cdot 613$
	$346 = 2 \cdot 173$	$814 = 2 \cdot 11 \cdot 37$	$1015 = 5 \cdot 7 \cdot 29$	$2 \times 1246 = 2 \cdot 7 \cdot 89$
	$362 = 2 \cdot 181$	$814 = 2 \cdot 11 \cdot 37$	$1073 = 29 \cdot 37$	$2 \times 1246 = 2 \cdot 7 \cdot 89$
	$362 = 2 \cdot 181$	$854 = 2 \cdot 7 \cdot 61$	$1073 = 29 \cdot 37$	$2 \times 1295 = 5 \cdot 7 \cdot 37$
	$610 = 2 \cdot 5 \cdot 61$	$854 = 2 \cdot 7 \cdot 61$	$1138 = 2 \cdot 569$	$2 \times 1295 = 5 \cdot 7 \cdot 37$
	$610 = 2 \cdot 5 \cdot 61$	$890 = 2 \cdot 5 \cdot 89$	$1138 = 2 \cdot 569$	$1315 = 5 \cdot 263$
	617	$890 = 2 \cdot 5 \cdot 89$	$1190 = 2 \cdot 5 \cdot 7 \cdot 17$	$1315 = 5 \cdot 263$
	617	$965 = 5 \cdot 193$	$1190 = 2 \cdot 5 \cdot 7 \cdot 17$	$1378 = 2 \cdot 13 \cdot 53$
	$715 = 5 \cdot 11 \cdot 13$	$965 = 5 \cdot 193$	$1190 = 2 \cdot 5 \cdot 7 \cdot 17$	$1378 = 2 \cdot 13 \cdot 53$
	$715 = 5 \cdot 11 \cdot 13$	$965 = 5 \cdot 193$	$1190 = 2 \cdot 5 \cdot 7 \cdot 17$	$1430 = 2 \cdot 5 \cdot 11 \cdot 13$
	$730 = 2 \cdot 5 \cdot 73$	$965 = 5 \cdot 193$	$1190 = 2 \cdot 5 \cdot 7 \cdot 17$	$1430 = 2 \cdot 5 \cdot 11 \cdot 13$
	$730 = 2 \cdot 5 \cdot 73$	$1010 = 2 \cdot 5 \cdot 101$	$1190 = 2 \cdot 5 \cdot 7 \cdot 17$	$1495 = 5 \cdot 13 \cdot 23$
	$731 = 17 \cdot 43$	$1010 = 2 \cdot 5 \cdot 101$	1201	$1495 = 5 \cdot 13 \cdot 23$

Table 3.1: Examples with $m = 1$, $p = 3$, $k = 2$, $d = 2$

$p = 3,\ d = 3$				
N				
t	$k = 2,\ \varepsilon = 1$			
729	$451 = 11 \cdot 41$	$2 \times 970 = 2 \cdot 5 \cdot 97$	$1159 = 19 \cdot 61$	$1351 = 7 \cdot 193$
	$458 = 5 \cdot 97$	$982 = 2 \cdot 491$	$1166 = 2 \cdot 11 \cdot 53$	$1378 = 2 \cdot 13 \cdot 53$
	617	$1042 = 2 \cdot 521$	$1235 = 5 \cdot 13 \cdot 19$	$2 \times 1414 = 2 \cdot 7 \cdot 101$
	$689 = 13 \cdot 53$	$1057 = 7 \cdot 151$	$1306 = 2 \cdot 653$	$1435 = 5 \cdot 7 \cdot 41$
	$778 = 2 \cdot 389$	$1094 = 2 \cdot 547$	$1306 = 2 \cdot 653$	1447
	$869 = 11 \cdot 79$	$1147 = 31 \cdot 37$	1321	
	$k = 2,\ \varepsilon \neq 1$			
	$962 = 2 \cdot 13 \cdot 37$	$962 = 2 \cdot 13 \cdot 37$	$1462 = 2 \cdot 17 \cdot 43$	
	$962 = 2 \cdot 13 \cdot 37$	$962 = 2 \cdot 13 \cdot 37$	$1462 = 2 \cdot 17 \cdot 43$	
$p = 3,\ d = 4$				
N				
t	$k = 2,\ \varepsilon = 1$			
6561	$1141 = 7 \cdot 163$	$1463 = 7 \cdot 11 \cdot 19$		
	$k = 2,\ \varepsilon \neq 1$			
	$1010 = 2 \cdot 5 \cdot 101$	$1015 = 5 \cdot 7 \cdot 29$	$1015 = 5 \cdot 7 \cdot 29$	$1435 = 5 \cdot 7 \cdot 41$
	$1010 = 2 \cdot 5 \cdot 101$	$1015 = 5 \cdot 7 \cdot 29$	$1015 = 5 \cdot 7 \cdot 29$	$1435 = 5 \cdot 7 \cdot 41$

Table 3.2: Examples with $m = 1$, $p = 3$, $k = 2$, $d = 3, 4$

$p = 5,\ d = 2$				
N				
t	$k = 2, \varepsilon = 1$			
625	137	487	$678 = 2 \cdot 3 \cdot 113$	$886 = 2 \cdot 443$
	173	$489 = 3 \cdot 163$	$679 = 7 \cdot 97$	$889 = 7 \cdot 127$
	199	$2 \times 502 = 2 \cdot 251$	$2 \times 682 = 2 \cdot 11 \cdot 31$	$897 = 3 \cdot 13 \cdot 23$
	$213 = 3 \cdot 71$	$511 = 7 \cdot 73$	$689 = 13 \cdot 53$	$899 = 29 \cdot 31$
	251	$526 = 2 \cdot 263$	$697 = 17 \cdot 41$	$922 = 2 \cdot 461$
	311	$534 = 2 \cdot 3 \cdot 89$	733	$923 = 13 \cdot 71$
	$374 = 2 \cdot 11 \cdot 17$	$542 = 2 \cdot 271$	$746 = 2 \cdot 373$	$2 \times 933 = 3 \cdot 311$
	$393 = 3 \cdot 131$	$2 \times 597 = 3 \cdot 199$	$767 = 13 \cdot 59$	$942 = 2 \cdot 3 \cdot 157$
	$394 = 2 \cdot 197$	601	$779 = 19 \cdot 41$	$962 = 2 \cdot 13 \cdot 37$
	$406 = 2 \cdot 7 \cdot 29$	$623 = 7 \cdot 89$	$794 = 2 \cdot 397$	$969 = 3 \cdot 17 \cdot 19$
	$2 \times 411 = 3 \cdot 137$	$633 = 3 \cdot 211$	$803 = 11 \cdot 73$	$2 \times 974 = 2 \cdot 487$
	$429 = 3 \cdot 11 \cdot 13$	$634 = 2 \cdot 317$	$807 = 3 \cdot 269$	$989 = 23 \cdot 43$
	431	$649 = 11 \cdot 59$	$818 = 2 \cdot 409$	997
	$434 = 2 \cdot 7 \cdot 31$	661	$826 = 2 \cdot 7 \cdot 59$	$998 = 2 \cdot 499$
	$478 = 2 \cdot 239$	$662 = 2 \cdot 331$	$862 = 2 \cdot 431$	
	$481 = 13 \cdot 37$	$671 = 11 \cdot 61$	881	
	$k = 2,\ \varepsilon \neq 1$			
	$339 = 3 \cdot 113$	$633 = 3 \cdot 13 \cdot 17$	$633 = 3 \cdot 13 \cdot 17$	$957 = 3 \cdot 11 \cdot 29$
	$339 = 3 \cdot 113$	$633 = 3 \cdot 13 \cdot 17$	$633 = 3 \cdot 13 \cdot 17$	$957 = 3 \cdot 11 \cdot 29$
	$357 = 3 \cdot 7 \cdot 17$	$633 = 3 \cdot 13 \cdot 17$	$633 = 3 \cdot 13 \cdot 17$	$957 = 3 \cdot 11 \cdot 29$
	$357 = 3 \cdot 7 \cdot 17$	$633 = 3 \cdot 13 \cdot 17$	$2 \times 714 = 2 \cdot 3 \cdot 7 \cdot 17$	$957 = 3 \cdot 11 \cdot 29$
	$374 = 2 \cdot 11 \cdot 17$	$633 = 3 \cdot 13 \cdot 17$	$2 \times 714 = 2 \cdot 3 \cdot 7 \cdot 17$	$959 = 7 \cdot 137$
	$374 = 2 \cdot 11 \cdot 17$	$633 = 3 \cdot 13 \cdot 17$	$771 = 3 \cdot 257$	$959 = 7 \cdot 137$
	601	$633 = 3 \cdot 13 \cdot 17$	$771 = 3 \cdot 257$	$979 = 11 \cdot 89$
	601	$633 = 3 \cdot 13 \cdot 17$	$822 = 2 \cdot 3 \cdot 137$	$979 = 11 \cdot 89$
	$633 = 3 \cdot 13 \cdot 17$	$633 = 3 \cdot 13 \cdot 17$	$822 = 2 \cdot 3 \cdot 137$	

Table 3.3: Examples with $m = 1$, $p = 5$, $k = 2$, $d = 2$

Examples 3.4.4 (Characteristic $p = 7$)**.** We also computed examples coming from mod 7 eigenforms. Since in this case we can also allow $d = 1$, we find a lot of examples (too many to list here). Just to give an example, for levels ranging between 1 and 500, we find 410 examples of mod 7 eigenforms f satisfying the required hypothesis, for which the attached local Hecke algebra $\mathbb{T}_f$ has $t = 7^2 = 49$ traces.

3.4.2 Examples with $m = 2$

In Table 3.4 we list the examples that we have computed in characteristic $p = 7$ where the dimension of $\mathfrak{m}$ is $m = 2$. In lower characteristics we did not find any example with $m > 1$.

As before, we group the examples that have the same characteristic, the same degree d and the same weight k together, and we separate those that have trivial character ε from those that do not. We list, with this data fixed, the levels that we find satisfying the required hypothesis described before.

When we find two congruent eigenforms f in the same space $S_k(N, \varepsilon; \mathbb{F}_q)$, we denote it by writing $2\times$ in front of the level.

$p = 7$, $d = 1$				
	N			
t	$k = 2$, $\varepsilon = 1$			
343	$258 = 2 \cdot 3 \cdot 43$	$669 = 3 \cdot 223$	$519 = 3 \cdot 173$	
	$417 = 3 \cdot 139$	$678 = 2 \cdot 3 \cdot 113$	$2 \times 834 = 2 \cdot 3 \cdot 139$	
	$k = 2$, $\varepsilon \neq 1$			
	$186 = 2 \cdot 3 \cdot 31$	$465 = 3 \cdot 5 \cdot 31$	$834 = 2 \cdot 3 \cdot 139$	$942 = 2 \cdot 3 \cdot 157$
	$190 = 2 \cdot 5 \cdot 19$	$2 \times 570 = 2 \cdot 3 \cdot 5 \cdot 19$	$858 = 2 \cdot 3 \cdot 11 \cdot 13$	$962 = 2 \cdot 13 \cdot 37$
	$222 = 2 \cdot 3 \cdot 37$	$583 = 11 \cdot 53$	$906 = 2 \cdot 3 \cdot 151$	$969 = 3 \cdot 17 \cdot 19$
	$310 = 2 \cdot 5 \cdot 31$	$598 = 2 \cdot 13 \cdot 23$	$915 = 3 \cdot 5 \cdot 61$	$970 = 2 \cdot 5 \cdot 97$
	$366 = 2 \cdot 3 \cdot 61$	$610 = 2 \cdot 5 \cdot 61$	$2 \times 930 = 2 \cdot 3 \cdot 5 \cdot 31$	$978 = 2 \cdot 3 \cdot 163$
	$386 = 2 \cdot 193$	$618 = 2 \cdot 3 \cdot 103$	$930 = 2 \cdot 3 \cdot 5 \cdot 31$	
	$429 = 3 \cdot 11 \cdot 13$	$626 = 2 \cdot 313$	$939 = 3 \cdot 313$	
	$442 = 2 \cdot 13 \cdot 17$	$741 = 3 \cdot 13 \cdot 19$	$942 = 2 \cdot 3 \cdot 157$	
	$k = 3$, $\varepsilon \neq 1$			
	$142 = 2 \cdot 71$	$330 = 2 \cdot 3 \cdot 5 \cdot 11$	$430 = 2 \cdot 5 \cdot 43$	$446 = 2 \cdot 223$
	223	$390 = 2 \cdot 3 \cdot 5 \cdot 13$	$430 = 2 \cdot 5 \cdot 43$	$447 = 3 \cdot 149$
	$330 = 2 \cdot 3 \cdot 5 \cdot 11$	$390 = 2 \cdot 3 \cdot 5 \cdot 13$	$446 = 2 \cdot 223$	$447 = 3 \cdot 149$
	$k = 5$, $\varepsilon \neq 1$			
	$158 = 2 \cdot 79$	$474 = 2 \cdot 3 \cdot 79$	$474 = 2 \cdot 3 \cdot 79$	$555 = 3 \cdot 5 \cdot 37$
	$158 = 2 \cdot 79$	$474 = 2 \cdot 3 \cdot 79$	$474 = 2 \cdot 3 \cdot 79$	$555 = 3 \cdot 5 \cdot 37$

Table 3.4: Examples with $m = 2$, $p = 7$, $k = 2, 3, 5$, $d = 1$

3.5 Examples coming from mod 2 modular forms

Fix a level $N \geq 1$, a weight $k \geq 2$ and a character $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{F}}_2^\times$. Take a normalised Hecke eigenform $f \in S_k(N, \varepsilon; \overline{\mathbb{F}}_2)$ and let $\mathbb{F}_q$ denote the finite field generated by its coefficients over $\mathbb{F}_2$. Suppose that $q \geq 4$. Let $\mathbb{T}_f$ denote the local mod 2 Hecke algebra over $\mathbb{F}_q$ corresponding to f, which can be computed as explained in section 3.3.

Let $\mathfrak{m}_f$ denote the maximal ideal of $\mathbb{T}_f$ and let $\overline{\rho}_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$ denote the attached residual Galois representation. Suppose that $\mathrm{Im}(\overline{\rho}_f) = \mathrm{GL}_2^D(\mathbb{F}_q)$, where $D = \mathrm{Im}(\det \circ \overline{\rho})$. Let $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2^D(\mathbb{T}_f)$ denote the Galois representation associated to $\mathfrak{m}_f$. Let $(\mathbb{T}, \mathfrak{m}) := (\mathbb{T}_f/\mathfrak{m}_f^2, \mathfrak{m}_f/\mathfrak{m}_f^2)$, and denote by m the dimension of $\mathfrak{m}$ over $\mathbb{F}_q$. Let $G := \mathrm{Im}(\rho_f) \bmod \mathfrak{m}_f^2 \subseteq \mathrm{GL}_2^D(\mathbb{T})$. Under these assumptions we are in the situation of Corollary 3.2.3, so we know that $G \simeq M \rtimes \mathrm{GL}_2^D(\mathbb{F}_q)$, where M is an $\mathbb{F}_2[\mathrm{GL}_2^D(\mathbb{F}_q)]$-submodule of $\mathrm{M}_2^0(\mathfrak{m})$ of the form

$$M := \underbrace{\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}_{\alpha} \oplus \underbrace{C_2 \oplus \cdots \oplus C_2}_{\beta},$$

for some $0 \leq \alpha \leq m$ and $0 \leq \beta \leq d(m-\alpha)$ that are determined by the number of different traces of G:

$$t = q^{\alpha} \cdot ((q-1)2^{\beta} + 1).$$

In the following tables we summarise the examples that we have found, using the algorithm described in section 3.3, in the following cases:

- $p = 2$, $k = 2$, $2 \leq d \leq 4$, $1 \leq N \leq 1500$.
- $p = 2$, $k = 3$, $2 \leq d \leq 4$, $1 \leq N \leq 1500$.

All the examples that we compute have trivial character, so we will not write it from now on. Note that, in this case, $D = 1$, so $\mathrm{GL}_2^D(\mathbb{F}_q) = \mathrm{SL}_2(\mathbb{F}_q)$ and $\mathrm{GL}_2^D(\mathbb{T}) = \mathrm{SL}_2(\mathbb{T})$.

As explained in section 3.3, to determine the group G we compute the number of different traces $\widetilde{t}$ in G up to a certain bound b that we fix. In the case of characteristic 2 though, we do not know the theoretical number t of traces that we are supposed to obtain, since now, contrary to the situation in characteristic $p > 2$, we have more than one possibility for the number t.

Thus, the number of traces of the examples that we computed (which we list in the tables that follow), and consequently the images G of the Galois representations ρ_f in characteristic 2, are only conjectural.

Remark 3.5.1. In contrast to the situation with characteristic $p > 2$, when the characteristic is 2 we find many examples where the maximal ideal has dimension $m = 2$ or 3.

3.5.1 Examples with $m = 1$

We begin with the examples that have $m = \dim_{\mathbb{F}_q} \mathfrak{m} = 1$. The next 3 tables show the possible number of traces t that can appear, depending on α, β and the degree d of $\mathbb{F}_q$ (for $d = 2, 3, 4$). According to Corollary 3.2.3, the number of traces is of the form $t = q^{\alpha} \cdot ((q-1)2^{\beta} + 1)$, for some $0 \leq \alpha \leq 1$ and $0 \leq \beta \leq d(1-\alpha)$.

$\mathbb{F}_{2^2}$		β		
		0	1	2
α	0	**4**	**7**	**13**
	1	**16**	-	-

$\mathbb{F}_{2^3}$		β			
		0	1	2	3
α	0	**8**	**15**	**29**	**57**
	1	**64**	-	-	-

$\mathbb{F}_{2^4}$		β				
		0	1	2	3	4
α	0	**16**	**31**	**61**	**121**	**241**
	1	**256**	-	-	-	-

Table 3.5: Possible number of traces when $m = 1$.

Let us first give some examples with $m = 1$ with all the details.

Examples 3.5.2. (1) The first example that we find with $d = 2$ is in level $N = 67$. In this case, by computing Hecke operators up to $b = 1000$, we find $\widetilde{t} = 7$. As the Table 3.5 shows, we have the following possibilities for t: 4,7,13 or 16. So we can only exclude $t = 4$. Let $T^{(1)}, \ldots, T^{(7)}$ denote the seven operators that we find. If we take a closer look to them, we observe the following multiplicities for each one:

$$21 \times T^{(1)},\ 31 \times T^{(2)},\ 15 \times T^{(3)},\ 14 \times T^{(4)},\ 39 \times T^{(5)},\ 16 \times T^{(6)},\ 30 \times T^{(7)}.$$

So if the theoretical number of traces were $t = 13$ or 16, it would mean that there are still at least 6 Hecke operators left to appear, which seems highly unlikely.

Just to be even more confident that $t = 7$, if we compute up to $b = 5000$, we still find $\widetilde{t} = 7$ and the following multiplicities:

$$58 \times T^{(1)},\ 114 \times T^{(2)},\ 69 \times T^{(3)},\ 67 \times T^{(4)},\ 185 \times T^{(5)},\ 63 \times T^{(6)},\ 111 \times T^{(7)}.$$

This means that the group G in this case would be $G \simeq C_2 \rtimes \mathrm{SL}_2(\mathbb{F}_4)$.

(2) For $d = 3$, the first example that we find is in level $N = 97$. We fix again the bound $b = 1000$ and compute the number of Hecke operators. This time we have more possibilities for t, namely: 8, 15, 29, 57 and 64. We find $\widetilde{t} = 15$. If we look at the multiplicities of each operator, they range from 8 to 18. And if we compute further, to $b = 5000$, we still get $\widetilde{t} = 15$, and the multiplicities go from 33 to 76. So it seems highly likely that $t = 15$. In this case, the group G would be $G \simeq C_2 \rtimes \mathrm{SL}_2(\mathbb{F}_8)$

(3) For $d = 4$ we find the first example in level $N = 137$. The possibilities for t in this case, according to table 3.5, are 16, 31, 61, 121, 241 or 256. If we compute up to $b = 1000$, we find $\widetilde{t} = 31$ traces. The multiplicities in this case range from 3 to 9. If we compute up to $b = 5000$, we still find $\widetilde{t} = 31$ traces, and the multiplicities of the traces go from 14 to 31. So again, it is highly likely that $t = 31$, and in this case the group is $G \simeq C_2 \rtimes \mathrm{SL}_2(\mathbb{F}_{16})$.

In Table 3.6 we show the examples that we computed for $m = 1$ and $N \leq 1500$.

$p=2,\ d=2$								
t	M	$N=p_1$					$N=p_1p_2$	
7	C_2	$k=2,k=3$						
		67	331	499	677	929	1283	$2\times 309=3\cdot 103$	$2\times 1177=11\cdot 107$
		73	347	509	709	937	1283	$2\times 335=5\cdot 67$	$2\times 1203=3\cdot 401$
		103	353	523	727	1061	1303	$2\times 511=7\cdot 73$	$2\times 1241=17\cdot 73$
		107	383	577	751	1063	1361	$2\times 573=3\cdot 191$	$2\times 1387=19\cdot 73$
		167	401	577	761	1063	1361	$2\times 579=3\cdot 193$	$2\times 1497=3\cdot 499$
		191	409	593	773	1069	1381	$2\times 721=7\cdot 103$	
		193	457	599	809	1171	1381	$2\times 737=11\cdot 67$	
		211	461	619	877	1181	1459	$2\times 749=7\cdot 107$	
		307	487	647	887	1217		$2\times 835=5\cdot 167$	
		313	491	677	919	1229		$2\times 965=5\cdot 193$	
$p=2,d=3$								
t	M	$N=p_1$					$N=p_1p_2$	
15	C_2	$k=2,k=3$						
		97	239	809	1303	1481		$2\times 339=3\cdot 113$	$2\times 763=7\cdot 109$
		109	359	1093	1319	1481		$2\times 381=3\cdot 127$	$2\times 889=7\cdot 127$
		113	397	1123	1429			$2\times 453=3\cdot 151$	$2\times 1043=7\cdot 149$
		127	397	1151	1429			$2\times 485=5\cdot 97$	$2\times 1067=11\cdot 97$
		139	449	1153	1439			$2\times 633=3\cdot 211$	$2\times 1077=3\cdot 359$
		149	461	1193	1447			$2\times 679=7\cdot 97$	$2\times 1135=5\cdot 227$
		151	587	1223	1447			$2\times 681=3\cdot 227$	$2\times 1191=3\cdot 397$
		179	641	1223	1447			$2\times 717=3\cdot 239$	$2\times 1199=11\cdot 109$
		211	641	1283	1453			$2\times 745=5\cdot 149$	$2\times 1417=13\cdot 109$
		227	739	1301	1471			$2\times 755=5\cdot 151$	
$p=2,d=4$								
t	M	$N=p_1$					$N=p_1p_2$	
31	C_2	$k=2,k=3$						
		137	349	739	929	1103	1291	$2\times 411=3\cdot 137$	$2\times 1255=5\cdot 251$
		173	419	839	967	1187	1423	$2\times 597=3\cdot 199$	$2\times 1293=3\cdot 431$
		199	431	853	967	1187		$2\times 933=3\cdot 311$	$2\times 1393=7\cdot 199$
		223	523	863	977	1201		$2\times 959=7\cdot 137$	
		251	619	911	997	1237		$2\times 995=5\cdot 199$	
		311	673	929	1097	1289		$2\times 1047=3\cdot 349$	

Table 3.6: Examples with $m=1$, $p=2$, $k=2,3$

Remark 3.5.3 ($m=1$)**.** As we can see from the previous table, it seems that the only group that appears when $m=1$ is $G\simeq C_2\times \mathrm{SL}_2(\mathbb{F}_q)$.

Remark 3.5.4 ($m=1$)**.** We observe that when N is prime, we never find the same eigenform twice, because there are no oldforms. However, when N is the product of two different primes, we always find that each eigenform mod 2 in this level appears twice.

3.5.2 Examples with $m=2$

Here we compute examples with $m=\dim_{\mathbb{F}_q}\mathfrak{m}=2$. The next 3 tables show the possible number of traces t that can appear, depending on α,β and the degree d of $\mathbb{F}_q$, for $d=2,3,4$, according to Corollary 3.2.3. In this case we have $0\leq\alpha\leq 2$ and $0\leq\beta\leq d(2-\alpha)$.

$\mathbb{F}_{2^2}$		β				
		0	1	2	3	4
α	0	**4**	**7**	**13**	**25**	**49**
	1	**16**	**28**	**52**	**100**	-
	2	**64**	-	-	-	-

$\mathbb{F}_{2^3}$		β						
		0	1	2	3	4	5	6
α	0	**8**	**15**	**29**	**57**	**113**	**225**	**449**
	1	**64**	**120**	**232**	**456**	-	-	-
	2	**512**	-	-	-	-	-	-

$\mathbb{F}_{2^4}$		β								
		0	1	2	3	4	5	6	7	8
α	0	**16**	**31**	**61**	**121**	**241**	**481**	**916**	**1921**	**3841**
	1	**256**	**496**	**976**	**1936**	**3856**	-	-	-	-
	2	**4096**	-	-	-	-	-	-	-	-

Table 3.7: Possible number of traces when $m = 2$.

The examples that we find in this case are richer than with $m = 1$. Let us first give some examples with $m = 2$ and $d = 2$ in more detail.

Examples 3.5.5 ($d = 2$)**.** When $d = 2$, we find 3 kinds of examples with different number of traces.

(1) Let us take level $N = 1003$ and weight $k = 2$, and and fix the bound $b = 1000$. Since now $m = 2$, we have more options for t than before (cf. Table 3.7). In this case we find $\widetilde{t} = 13$. When we rise the bound up to $b = 5000$, we still find $\widetilde{t} = 13$, so it is highly likely that $t = 13$. This corresponds to the group $G \simeq (C_2 \oplus C_2) \times \mathrm{SL}_2(\mathbb{F}_4)$.

(2) In level $N = 167$ and weight $k = 3$, we find an example with $\widetilde{t} = 25$ when the bound is $b = 1000$, so the possibilities in this case are reduced to $t = 25, 28, 49, 52, 64$ or 100. If we compute further, up to $b = 5000$, we still get $\widetilde{t} = 25$. In this case, it corresponds to the group $G \simeq (C_2 \oplus C_2 \oplus C_2) \times \mathrm{SL}_2(\mathbb{F}_4)$.

(3) Finally, for $N = 887$ we find an eigenform with $\widetilde{t} = 28$ traces (both up to $b = 1000$ and up to $b = 5000$). This corresponds to the group $G \simeq (\mathrm{M}_2^0(\mathbb{F}_4) \oplus C_2) \rtimes \mathrm{SL}_2(\mathbb{F}_4)$.

In Table 3.8 we show the examples that we computed for $m = 2$, $d = 2$ and $N \leq 1500$.

$p=2,\ d=2$						
t	M	$N=p_1$	$N=p_1p_2$			$N=p_1p_2p_3$
13	$C_2\oplus C_2$	$k=2,\ k=3$				
		1103	$133=7\cdot 19$	$669=3\cdot 223$	$1077=3\cdot 359$	$2\times 615=3\cdot 5\cdot 41$
			$177=3\cdot 59$	$707=7\cdot 101$	$1111=11\cdot 101$	$2\times 665=5\cdot 7\cdot 19$
			$205=5\cdot 41$	$721=7\cdot 103$	$1133=11\cdot 103$	$2\times 885=3\cdot 5\cdot 59$
			$213=3\cdot 71$	$745=5\cdot 149$	$1141=7\cdot 163$	$2\times 1023=3\cdot 11\cdot 31$
			$221=13\cdot 17$	$781=11\cdot 71$	$1149=3\cdot 383$	$2\times 1105=5\cdot 13\cdot 17$
			$265=5\cdot 53$	$799=17\cdot 47$	$1157=13\cdot 89$	$2\times 1455=3\cdot 5\cdot 97$
			$287=7\cdot 41$	$843=3\cdot 281$	$1255=5\cdot 251$	$2\times 1491=3\cdot 7\cdot 71$
			$291=3\cdot 97$	$949=13\cdot 73$	$1273=19\cdot 67$	
			$299=13\cdot 23$	$951=3\cdot 317$	$1347=3\cdot 449$	
			$341=11\cdot 31$	$955=5\cdot 191$	$1363=29\cdot 47$	
			$371=7\cdot 53$	$965=5\cdot 193$	$1371=3\cdot 457$	
			$415=5\cdot 83$	$989=23\cdot 43$	$1391=13\cdot 107$	
			$417=3\cdot 139$	$989=23\cdot 43$	$1405=5\cdot 281$	
			$453=3\cdot 151$	$1003=17\cdot 59$	$1417=13\cdot 109$	
			$471=3\cdot 157$	$1043=7\cdot 149$	$1437=3\cdot 479$	
			$635=5\cdot 127$	$1057=7\cdot 151$	$1473=3\cdot 491$	
		$k=3$				
		313 1129	$2\times 939=3\cdot 313$			
		439 1321	$2\times 1317=3\cdot 439$			
		479 1361	$2\times 1497=3\cdot 499$			
		499 1409				
		701 1429				
		751 1453				
		821 1439				
		853 1459				
		953 1499				
25	$C_2\oplus C_2\oplus C_2$	$k=3$				
		167 617	$2\times 591=3\cdot 197$			
		179 631	$2\times 723=3\cdot 241$			
		197 751	$2\times 753=3\cdot 251$			
		241 773	$2\times 835=5\cdot 167$			
		251 881	$2\times 895=5\cdot 179$			
		269 929	$2\times 1169=7\cdot 167$			
		337 971	$2\times 1253=7\cdot 179$			
		499 1069	$2\times 1379=7\cdot 197$			
		541 1283				
		571 1291				
28	$\mathrm{M}_2^0(\mathbb{F}_{2^2})\oplus C_2$	$k=2,\ k=3$				
		887				
		1061				

Table 3.8: Examples with $m=2$, $p=2$, $k=2,3$, $d=2$

Examples 3.5.6 ($d=3$)**.** When $d=3$, we find 3 kinds of examples with different number of traces.

(1) Take level $N=217$ and weight $k=2$. In this level, for $b=1500$, we find $\widetilde{t}=29$. If we rise the bound up to $b=5000$, we still find $\widetilde{t}=29$. Thus, we would expect from this that $t=29$, and in this case $G\simeq(C_2\oplus C_2)\times \mathrm{SL}_2(\mathbb{F}_8)$.

(2) The first example that we find for $d=3$ and weight $k=3$ is in level $N=191$. We find $\widetilde{t}=57$ up to the bound $b=1500$, as well as up to $b=5000$. Thus it seems highly likely that $t=57$, and in this case $G\simeq(C_2\oplus C_2\oplus C_2)\times \mathrm{SL}_2(\mathbb{F}_8)$.

(3) For $N=911$ and weight $k=2$ we find an example with $\widetilde{t}=116$ up to the bound $b=3000$. If we increase the bound to $b=5000$, we find $\widetilde{t}=120$. Finally, if we compute Hecke operators up

to $b = 10000$, we also find $\widetilde{t} = 120$. In this case, the group G is $G \simeq (\mathrm{M}_2^0(\mathbb{F}_8) \oplus C_2) \rtimes \mathrm{SL}_2(\mathbb{F}_8)$. Note that this is the first example in characteristic 2 that we find were the semidirect product is nontrivial, i.e it is not a direct product. This is because the the action of $\mathbb{F}_2[\mathrm{SL}_2(\mathbb{F}_8)]$ on the module $M = \mathrm{M}_2^0(\mathbb{F}_8) \oplus C_2$ is nontrivial.

In Table 3.9 we summarise the examples that we computed for $m = 2$, $d = 3$ and $N \leq 1500$.

$p = 2$, $d = 3$						
t	M	$N = p_1$	$N = p_1p_2$			$N = p_1p_2p_3$
29	$C_2 \oplus C_2$	$k = 2$, $k = 3$				
			$217 = 7 \cdot 31$	$597 = 3 \cdot 199$	$1227 = 3 \cdot 409$	$2 \times 651 = 3 \cdot 7 \cdot 31$
			$247 = 13 \cdot 19$	$851 = 23 \cdot 37$	$1253 = 7 \cdot 179$	$2 \times 741 = 3 \cdot 13 \cdot 19$
			$253 = 11 \cdot 23$	$923 = 13 \cdot 71$	$1255 = 5 \cdot 251$	$2 \times 759 = 3 \cdot 11 \cdot 23$
			$259 = 7 \cdot 37$	$943 = 23 \cdot 41$	$1257 = 3 \cdot 419$	$2 \times 885 = 3 \cdot 5 \cdot 59$
			$267 = 3 \cdot 89$	$1037 = 17 \cdot 61$	$1285 = 5 \cdot 257$	$2 \times 1235 = 5 \cdot 13 \cdot 19$
			$295 = 5 \cdot 59$	$1041 = 3 \cdot 347$	$1315 = 5 \cdot 263$	$2 \times 1265 = 5 \cdot 11 \cdot 23$
			$305 = 5 \cdot 61$	$1055 = 5 \cdot 211$	$1339 = 13 \cdot 103$	$2 \times 1335 = 3 \cdot 5 \cdot 89$
			$319 = 11 \cdot 29$	$1057 = 7 \cdot 151$	$1345 = 5 \cdot 269$	$2 \times 1407 = 3 \cdot 7 \cdot 67$
			$329 = 7 \cdot 47$	$1081 = 23 \cdot 47$	$1347 = 3 \cdot 449$	
			$365 = 5 \cdot 73$	$1099 = 7 \cdot 157$	$1349 = 19 \cdot 71$	
			$395 = 5 \cdot 79$	$1139 = 17 \cdot 67$	$1357 = 23 \cdot 59$	
			$411 = 3 \cdot 137$	$1147 = 31 \cdot 37$	$1357 = 23 \cdot 59$	
			$469 = 7 \cdot 67$	$1159 = 19 \cdot 61$	$1383 = 3 \cdot 461$	
			$519 = 3 \cdot 173$	$1189 = 29 \cdot 41$	$1403 = 23 \cdot 61$	
			$543 = 3 \cdot 181$	$1189 = 29 \cdot 41$	$1457 = 31 \cdot 47$	
			$559 = 13 \cdot 43$	$1207 = 17 \cdot 71$	$1469 = 13 \cdot 113$	
			$579 = 3 \cdot 193$	$1227 = 3 \cdot 409$	$1497 = 3 \cdot 499$	
		$k = 3$				
		797 1163				
		823 1259				
		977 1487				
		1093				
t	M	$N = p_1$	$N = p_1p_2$			$N = p_1p_2p_3$
57	$C_2 \oplus C_2 \oplus C_2$	$k = 3$				
		191 827	$2 \times 573 = 3 \cdot 191$			
		211 829	$2 \times 633 = 3 \cdot 211$			
		233 853	$2 \times 843 = 3 \cdot 281$			
		277 887	$2 \times 1101 = 3 \cdot 267$			
		281 919	$2 \times 1317 = 3 \cdot 439$			
		349 929	$2 \times 1337 = 7 \cdot 191$			
		367 1093	$2 \times 1385 = 5 \cdot 277$			
		439 1181	$2 \times 1401 = 3 \cdot 467$			
		467 1187	$2 \times 1405 = 5 \cdot 281$			
		499 1277	$2 \times 1477 = 7 \cdot 211$			
		571 1279	$2 \times 1497 = 3 \cdot 499$			
		673 1373				
		683 1439				
		811 1453				
		823				
120	$\mathrm{M}_2^0(\mathbb{F}_{2^3}) \oplus C_2$	$k = 2,\ k = 3$				
		911 1069				
		1231 1093				
		1361 1231				

Table 3.9: Examples with $m = 2$, $p = 2$, $k = 2, 3$, $d = 3$

Examples 3.5.7 ($d = 4$)**.** When $d = 3$, we find 2 kinds of examples with different number of traces.

(1) For $N = 301$ and $k = 2$, we compute up to $b = 1000$ and find $\widetilde{t} = 60$. When we increase the bound to $b = 5000$, we find $\widetilde{t} = 61$, which corresponds to one of the values in table 3.7. In this case, the group G would be $G \simeq (C_2 \oplus C_2) \times \mathrm{SL}_2(\mathbb{F}_{16})$.

(2) Let $N = 563$ and $k = 3$, and fix the bound $b = 1500$. We compute Hecke operators up to this bound and find, in this case, $\widetilde{t} = 106$. If we compute up to $b = 5000$, we find $\widetilde{t} = 121$. Finally, if we compute further, up to $b = 10000$, we still find $\widetilde{t} = 121$. So it seems reasonable to think that $t = 121$. In this case, the group G is $G \simeq (C_2 \oplus C_2 \oplus C_2) \times \mathrm{SL}_2(\mathbb{F}_{16})$.

In Table 3.10 we summarise the examples that we computed for $m = 2$, $d = 4$ and $N \leq 1500$.

$p = 2$, $d = 4$						
t	M	$N = p_1$	$N = p_1p_2$			$N = p_1p_2p_3$
61	$C_2 \oplus C_2$	$k = 2$, $k = 3$				
			$301 = 7 \cdot 43$	$679 = 7 \cdot 97$	$1111 = 11 \cdot 101$	$2 \times 903 = 3 \cdot 7 \cdot 43$
			$323 = 17 \cdot 19$	$679 = 7 \cdot 97$	$1141 = 7 \cdot 163$	$2 \times 969 = 3 \cdot 17 \cdot 19$
			$355 = 5 \cdot 71$	$713 = 23 \cdot 31$	$1147 = 31 \cdot 37$	
			$393 = 3 \cdot 131$	$717 = 3 \cdot 239$	$1147 = 31 \cdot 37$	
			$407 = 11 \cdot 37$	$755 = 5 \cdot 151$	$1159 = 19 \cdot 61$	
			$445 = 5 \cdot 89$	$767 = 13 \cdot 59$	$1189 = 29 \cdot 41$	
			$485 = 5 \cdot 97$	$791 = 17 \cdot 113$	$1203 = 3 \cdot 401$	
			$489 = 3 \cdot 163$	$793 = 13 \cdot 61$	$1203 = 3 \cdot 401$	
			$515 = 5 \cdot 103$	$813 = 3 \cdot 271$	$1247 = 29 \cdot 43$	
			$559 = 13 \cdot 43$	$851 = 23 \cdot 37$	$1315 = 5 \cdot 263$	
			$583 = 11 \cdot 53$	$899 = 29 \cdot 31$	$1349 = 19 \cdot 71$	
			$623 = 7 \cdot 89$	$973 = 7 \cdot 139$	$1383 = 3 \cdot 461$	
			$633 = 3 \cdot 211$	$1007 = 19 \cdot 53$	$1497 = 3 \cdot 499$	
			$649 = 11 \cdot 59$	$1073 = 29 \cdot 37$		
		$k = 3$				
		991				
121	$C_2 \oplus C_2 \oplus C_2$	$k = 3$				
		239 449 929	$2 \times 933 = 3 \cdot 311$			
		263 563 941	$2 \times 951 = 3 \cdot 317$			
		311 577 1117	$2 \times 993 = 3 \cdot 331$			
		317 643 1153	$2 \times 1119 = 3 \cdot 373$			
		331 683 1237	$2 \times 1195 = 5 \cdot 239$			
		373 733 1277	$2 \times 1263 = 3 \cdot 421$			
		389 789 1291	$2 \times 1315 = 5 \cdot 263$			
		373 789 1297				
		389 809 1471				
		409 823 1483				
		421 907				
		443 919				

Table 3.10: Examples with $m = 2$, $p = 2$, $k = 2, 3$, $d = 4$

Remark 3.5.8 ($m = 2$)**.** Tables 3.8, 3.9 and 3.10 suggest that, when the dimension of $\mathfrak{m}$ is $m = 2$, then the image of ρ_f is either isomorphic to $(C_2 \oplus C_2) \times \mathrm{SL}_2(\mathbb{F}_q)$, or $(C_2 \oplus C_2 \oplus C_2) \times \mathrm{SL}_2(\mathbb{F}_q)$ or $(\mathrm{M}_2^0(\mathbb{F}_q) \oplus C_2) \rtimes \mathrm{SL}_2(\mathbb{F}_q)$.

Moreover we observe that the most common group is $(C_2 \oplus C_2) \times \mathrm{SL}_2(\mathbb{F}_q)$, and that the group $(C_2 \oplus C_2 \oplus C_2) \times \mathrm{SL}_2(\mathbb{F}_q)$ occurs only in weight $k = 3$.

Remark 3.5.9 ($m = 2$)**.** Let us note the relation that appears to exist between the number of prime factors of the level N and the existence of repeated eigenforms. For $k = 2$ and $N = p_1p_2$, we never find the same eigenform twice. However, when $k = 2$ and $N = p_1p_2p_3$ all the mod p eigenforms appear twice.

In weight 3, this phenomenon seems to behave like the analogous situation with $m = 1$ and $k = 2$: when N is prime, there are no repeated eigenforms, and when N is the product of 2 primes, then all the eigenforms appear twice.

This can possibly be explained theoretically via oldforms.

3.5.3 Examples with $m = 3$

Finally we compute some examples with $m = \dim_{\mathbb{F}_q} \mathfrak{m} = 3$. The next 3 tables show the possible number of traces t that can appear, depending on α, β and the degree d of $\mathbb{F}_q$, for $d = 2, 3, 4$, according to Corollary 3.2.3. In this case we have $0 \leq \alpha \leq 3$ and $0 \leq \beta \leq d(3 - \alpha)$.

$\mathbb{F}_{2^2}$		β						
		0	1	2	3	4	5	6
α	0	**4**	**7**	**13**	**25**	**49**	**97**	**193**
	1	**16**	**28**	**52**	**100**	**196**	-	-
	2	**64**	**112**	**208**	-	-	-	-
	3	**256**	-	-	-	-	-	-

$\mathbb{F}_{2^3}$		β									
		0	1	2	3	4	5	6	7	8	9
α	0	**8**	**15**	**29**	**57**	**113**	**225**	**449**	**897**	**1793**	**3585**
	1	**64**	**120**	**232**	**456**	**904**	**1800**	**3592**	-	-	-
	2	**512**	**960**	**1856**	**3648**	-	-	-	-	-	-
	3	**4096**	-	-	-	-	-	-	-	-	-

$\mathbb{F}_{2^4}$		β								
		0	1	2	3	4	5	6	7	8
α	0	**16**	**31**	**61**	**121**	**241**	**481**	**961**	**1921**	**3841**
	1	**256**	**496**	**976**	**1936**	**3856**	**7969**	**15376**	**30736**	**61456**
	2	**4096**	**7936**	**15616**	**30976**	**61696**	-	-	-	-
	3	**65536**	-	-	-	-	-	-	-	-

		β			
		9	10	11	12
α	0	**7681**	**15361**	**30721**	**61441**

Table 3.11: Possible number of traces when $m = 3$.

Example 3.5.10 ($d = 2$)**.** When $d = 2$, we find 3 different cases of examples.

(1) The first example with $d = 2$ and $k = 2$ is in level $N = 483$. In this case, we find $\widetilde{t} = 25$ when we compute Hecke operators up to $b = 1000$, as well as up to $b = 5000$. Thus, it seems likely that $t = 25$. In this case, $G \simeq (C_2 \oplus C_2 \oplus C_2) \times \mathrm{SL}_2(\mathbb{F}_4)$.

(2) For $N = 391$ and $k = 3$, we compute up to $b = 1500$ and find an example with $\widetilde{t} = 48$. If we compute further, up to $b = 5000$, we find $\widetilde{t} = 49$, which corresponds to one of the values in table 3.11. In this case, the group G is $G \simeq (C_2 \oplus C_2 \oplus C_2 \oplus C_2) \times \mathrm{SL}_2(\mathbb{F}_4)$. Note that we only find this case for $k = 3$, and not for $k = 2$.

(3) Let $N = 1041$ and $k = 2$. In this case, if we compute up to $b = 2000$, we find $\widetilde{t} = 50$, and if we compute up to $b = 5000$, we find $\widetilde{t} = 52$. So it is likely that $t = 52$. This corresponds to the group $G \simeq (\mathrm{M}_2^0(\mathbb{F}_4) \oplus C_2 \oplus C_2) \rtimes \mathrm{SL}_2(\mathbb{F}_4)$.

In Table 3.12 we summarise the examples that we computed for $m = 3$, $d = 2$ and $N \leq 1500$.

$p = 2$, $d = 2$					
t	M	$N = p_1p_2$			$N = p_1p_2p_3$
25	$C_2 \oplus C_2 \oplus C_2$	$k = 2, k = 3$			
					$483 = 3 \cdot 7 \cdot 23$ $555 = 3 \cdot 5 \cdot 37$ $903 = 3 \cdot 7 \cdot 43$ $1095 = 3 \cdot 5 \cdot 73$ $1455 = 3 \cdot 5 \cdot 97$ $1479 = 3 \cdot 17 \cdot 29$
		$k = 3$			
		$973 = 7 \cdot 139$	$1199 = 11 \cdot 109$	$1263 = 3 \cdot 421$	
		$1111 = 11 \cdot 101$	$1333 = 31 \cdot 43$	$1389 = 3 \cdot 463$	
49	$C_2 \oplus C_2 \oplus C_2 \oplus C_2$	$k = 3$			
		$391 = 17 \cdot 23$	$901 = 17 \cdot 53$	$1219 = 23 \cdot 53$	$2 \times 1173 = 3 \cdot 17 \cdot 23$
		$451 = 11 \cdot 41$	$923 = 13 \cdot 71$	$1261 = 13 \cdot 97$	
		$481 = 12 \cdot 37$	$955 = 5 \cdot 191$	$1315 = 5 \cdot 263$	
		$535 = 5 \cdot 107$	$1003 = 17 \cdot 59$	$1355 = 5 \cdot 271$	
		$597 = 3 \cdot 199$	$1099 = 7 \cdot 57$	$1457 = 31 \cdot 47$	
		$685 = 5 \cdot 137$	$1135 = 5 \cdot 227$	$1465 = 5 \cdot 293$	
		$843 = 3 \cdot 281$	$1145 = 5 \cdot 229$		
		$869 = 11 \cdot 79$	$1189 = 29 \cdot 41$		
52	$\mathrm{M}_2^0(\mathbb{F}_{2^2}) \oplus C_2 \oplus C_2$	$k = 2, k = 3$			
		$1041 = 3 \cdot 347$	$1363 = 29 \cdot 47$	$1139 = 17 \cdot 67$	
		$1055 = 5 \cdot 211$	$1391 = 13 \cdot 107$		

Table 3.12: Examples with $m = 3$, $p = 2$, $k = 2, 3$, $d = 2$

Example 3.5.11 ($d = 3$)**.** When $d = 2$, we find 2 types of examples.

(1) Take $N = 595$ and $k = 2$. In this level we find an example with $\widetilde{t} = 57$ when we compute up to the bound $b = 1500$. We find the same $\widetilde{t} = 57$ when we compute up to $b = 5000$. Thus it seems highly likely that $t = 57$. This corresponds to the group $G \simeq (C_2 \oplus C_2 \oplus C_2) \times \mathrm{SL}_2^D(\mathbb{F}_8)$.

(2) Let $N = 515$, $k = 3$ and fix the bound $b = 1500$. We find in this case $\widetilde{t} = 105$. If we compute up to $b = 3000$, we find $\widetilde{t} = 113$, and if we compute up to $b = 5000$, we still find $\widetilde{t} = 113$. This coincides with one of the values in Table 3.11, and it corresponds to the group $G \simeq (C_2 \oplus C_2 \oplus C_2 \oplus C_2) \times \mathrm{SL}_2^D(\mathbb{F}_8)$.

In Table 3.13 we summarise the examples that we computed for $m = 3$, $d = 3$ and $N \leq 1500$.

$p=2,\ d=3$					
t	M	$N=p_1p_2$		$N=p_1p_2p_3$	
57	$C_2\oplus C_2\oplus C_2$	$k=2, k=3$			
				$595=5\cdot 7\cdot 17$	$1023=3\cdot 11\cdot 31$
				$627=3\cdot 11\cdot 19$	$1065=3\cdot 5\cdot 71$
				$795=3\cdot 5\cdot 53$	$1113=3\cdot 7\cdot 53$
				$805=5\cdot 7\cdot 23$	$1239=3\cdot 7\cdot 59$
				$897=3\cdot 13\cdot 23$	$1245=3\cdot 5\cdot 83$
				$957=3\cdot 11\cdot 29$	$1311=3\cdot 19\cdot 23$
				$987=3\cdot 7\cdot 47$	$1443=3\cdot 13\cdot 37$
				$1015=5\cdot 7\cdot 29$	
113	$C_2\oplus C_2\oplus C_2\oplus C_2$	$k=3$			
		$515=5\cdot 103$	$889=7\cdot 127$		
		$527=17\cdot 31$	$895=5\cdot 179$		
		$635=5\cdot 127$	$939=3\cdot 313$		
		$649=11\cdot 59$	$993=3\cdot 331$		
		$669=3\cdot 223$	$1133=11\cdot 103$		
		$679=7\cdot 97$	$1189=29\cdot 41$		
		$695=5\cdot 139$	$1205=5\cdot 241$		
		$749=7\cdot 107$	$1219=23\cdot 53$		
		$755=5\cdot 151$	$1329=3\cdot 443$		
		$793=13\cdot 61$	$1333=5\cdot 271$		
		$803=11\cdot 73$	$1441=17\cdot 83$		
		$807=3\cdot 269$	$1465=5\cdot 293$		

Table 3.13: Examples with $m=3$, $p=2$, $k=2,3$, $d=3$

Example 3.5.12 ($d=4$)**.** Finally we show one example of each case when the degree of $\mathbb{F}_q$ is $d=4$. We find 2 different types of examples.

(1) For $N=969$ and $k=2$, we find $\widetilde{t}=120$ when $b=5000$, and $\widetilde{t}=121$ when $b=10000$. Thus, it seems highly likely that $t=121$. In this case, the group G is $G\simeq(C_2\oplus C_2\oplus C_2)\times \mathrm{SL}_2(\mathbb{F}_{16})$.

(2) Take level $N=611$ and weight $k=3$. This is one of the cases that we find the highest value of $\widetilde{t}$, so we need to compute much further to be able guess the possible t. For $b=1500$, we find $\widetilde{t}=150$. For $b=3000$ we find $\widetilde{t}=208$. For $b=10000$ we find $\widetilde{t}=240$. Finally, for $b=20000$ we find $\widetilde{t}=241$. Since the value $t=241$ is in Table 3.11, it seems likely that this is the value that we are looking for. In this case, $G\simeq(C_2\oplus C_2\oplus C_2\oplus C_2)\times \mathrm{SL}_2(\mathbb{F}_{16})$.

In Table 3.14 we summarise the examples that we computed for $m=3$, $d=4$ and $N\leq 1500$.

$p=2$, $d=4$					
t	M	$N=p_1p_2$		$N=p_1p_2p_3$	
121	$C_2\oplus C_2\oplus C_2$	$k=2, k=3$			
				$969=3\cdot 17\cdot 19$	$1185=3\cdot 5\cdot 79$
				$1001=7\cdot 11\cdot 13$	$1281=3\cdot 7\cdot 61$
				$1005=3\cdot 5\cdot 67$	$1353=3\cdot 11\cdot 41$
				$1131=3\cdot 13\cdot 29$	$1419=3\cdot 11\cdot 43$
241	$C_2\oplus C_2\oplus C_2\oplus C_2$	$k=3$			
		$611=13\cdot 47$	$1047=3\cdot 349$		
		$707=7\cdot 101$	$1057=7\cdot 151$		
		$721=7\cdot 103$	$1079=13\cdot 83$		
		$731=17\cdot 43$	$1101=3\cdot 367$		
		$785=5\cdot 157$	$1121=19\cdot 59$		
		$813=3\cdot 271$	$1167=3\cdot 289$		
		$831=3\cdot 277$	$1255=5\cdot 251$		
		$893=19\cdot 47$	$1267=7\cdot 181$		
		$921=3\cdot 307$	$1293=3\cdot 431$		
		$949=13\cdot 73$	$1383=3\cdot 461$		
		$965=5\cdot 193$	$1393=7\cdot 199$		
		$989=23\cdot 43$	$1401=3\cdot 467$		
		$995=5\cdot 199$	$1477=7\cdot 211$		

Table 3.14: Examples with $m=3$, $p=2$, $k=2,3$, $d=4$

Remark 3.5.13 ($m=3$)**.** Tables 3.12, 3.13 and 3.14 suggest that when the dimension of $\mathfrak{m}$ is $m=3$, then the image of ρ_f is either isomorphic to $G\simeq (C_2\oplus C_2\oplus C_2)\times \mathrm{SL}_2(\mathbb{F}_q)$, or $G\simeq (C_2\oplus C_2\oplus C_2\oplus C_2)\times \mathrm{SL}_2(\mathbb{F}_q)$ or $G\simeq (\mathrm{M}_2^0(\mathbb{F}_q)\oplus C_2\oplus C_2)\rtimes \mathrm{SL}_2(\mathbb{F}_q)$.

Although the example $G\simeq (\mathrm{M}_2^0(\mathbb{F}_q)\oplus C_2\oplus C_2)\rtimes \mathrm{SL}_2(\mathbb{F}_q)$ does not appear for $d=4$, the previous tables suggest that this case might appear if we compute for high enough levels.

Moreover, we observe that the case $G\simeq (C_2\oplus C_2\oplus C_2\oplus C_2)\times \mathrm{SL}_2(\mathbb{F}_q)$ only appears in weight $k=3$.

Remark 3.5.14 ($m=3$)**.** Let us note that, in this case, we only find one level N in which one eigenform appears twice.

It might be that, as the analogous situations with $m=1$ and $m=2$ suggest, these only appear when the level N factorises into four different prime factors when $k=2$ (a phenomenon that we have not observed, maybe because we did not compute levels far enough), and when N factorises in three prime factors and $k=3$ (which is the case we observe).

3.6 Results and conjectures deduced from the examples

Let us recall the situation from the previous section. Let $\mathbb{F}_q$ be a finite field of characteristic 2. Let $\mathbb{T}_f$ denote a local mod 2 Hecke algebra over $\mathbb{F}_q$ of level $N\geq 1$, weight $k\geq 2$, and character $\varepsilon:(\mathbb{Z}/N\mathbb{Z})^\times\to\overline{\mathbb{F}}_p^\times$, and let $\mathfrak{m}_f$ denote its maximal ideal. Suppose that $q\geq 4$. Let $\overline{\rho}_f:G_{\mathbb{Q}}\to \mathrm{SL}_2(\mathbb{F}_q)$ denote the attached residual Galois representation, and suppose that $\mathrm{Im}(\overline{\rho}_f)=\mathrm{SL}_2(\mathbb{F}_q)$. Consider the Galois representation $\rho_f:G_{\mathbb{Q}}\to \mathrm{SL}_2(\mathbb{T}_f/\mathfrak{m}_f^2)$ associated to $\mathfrak{m}_f$, and suppose that $\mathrm{Im}(\rho_f)\subseteq \mathrm{SL}_2(\mathbb{T}_f/\mathfrak{m}_f^2)$.

From the examples computed in the previous section in characteristic 2, we can extract some general information.

The data that we have collected when the dimension $m = \dim_{\mathbb{F}_q} \mathfrak{m}_f/\mathfrak{m}_f^2$ is 1, 2 or 3, suggest the following conjecture in the same direction.

Conjecture 3.6.1. Let $\mathbb{F}_q$ be a finite field of characteristic 2. Let $\mathbb{T}_f$ denote a local mod 2 Hecke algebra over $\mathbb{F}_q$ of level $N \geq 1$, weight $k = 2$ or 3, and trivial character, and let $\mathfrak{m}_f$ denote its maximal ideal. Suppose that $q \geq 4$. Let $\overline{\rho}_f : G_{\mathbb{Q}} \to \mathrm{SL}_2(\mathbb{F}_q)$ denote the attached residual Galois representation, and suppose that $\mathrm{Im}(\overline{\rho}_f) = \mathrm{SL}_2(\mathbb{F}_q)$. Consider the Galois representation $\rho_f : G_{\mathbb{Q}} \to \mathrm{SL}_2(\mathbb{T}_f/\mathfrak{m}_f^2)$ associated to $\mathfrak{m}_f$, and suppose that $\mathrm{Im}(\rho_f) \subseteq \mathrm{SL}_2(\mathbb{T}_f/\mathfrak{m}_f^2)$.

If $\dim_{\mathbb{F}_q} \mathfrak{m}_f/\mathfrak{m}_f^2 = 1$, then

$$\mathrm{Im}(\rho_f) \simeq C_2 \times \mathrm{SL}_2(\mathbb{F}_q).$$

If $\dim_{\mathbb{F}_q} \mathfrak{m}_f/\mathfrak{m}_f^2 = 2$, then

$$\mathrm{Im}(\rho_f) \simeq \begin{cases} (C_2 \oplus C_2) \times \mathrm{SL}_2(\mathbb{F}_q), \text{ or} \\ (C_2 \oplus C_2 \oplus C_2) \times \mathrm{SL}_2(\mathbb{F}_q), \text{ or} \\ (\mathrm{M}_2^0(\mathbb{F}_q) \oplus C_2) \rtimes \mathrm{SL}_2(\mathbb{F}_q). \end{cases}$$

If $\dim_{\mathbb{F}_q} \mathfrak{m}_f/\mathfrak{m}_f^2 = 3$, then

$$\mathrm{Im}(\rho_f) \simeq \begin{cases} (C_2 \oplus C_2 \oplus C_2) \times \mathrm{SL}_2(\mathbb{F}_q), \text{ or} \\ (C_2 \oplus C_2 \oplus C_2 \oplus C_2) \times \mathrm{SL}_2(\mathbb{F}_q), \text{ or} \\ (\mathrm{M}_2^0(\mathbb{F}_q) \oplus C_2 \oplus C_2) \rtimes \mathrm{SL}_2(\mathbb{F}_q). \end{cases}$$

Finally, remarks 3.5.4, 3.5.9 and 3.5.14, suggest the following conjecture.

Conjecture 3.6.2. Consider the same hypothesis as in the previous conjecture. Let $m = \dim_{\mathbb{F}_q} \mathfrak{m}_f/\mathfrak{m}_f^2$ and suppose that $N = p_1 \dots p_r$, where the p_i are different primes.

If $k = 2$ and $1 \leq r \leq m$, then there are no repeated eigenforms mod 2 in level N. If $r = m + 1$ then there are 2 repeated eigenforms.

If $k = 3$ and $1 \leq r \leq m - 1$, then there are no repeated eigenforms (that do not come from weight $k = 2$) in level N. If $r = m$ then there are 2 repeated eigenforms.

Chapter 4

Application: abelian extensions of big non-solvable number fields

In this chapter we use the previous results to predict the existence of some p-elementary abelian field extensions. Let $\mathbb{F}_q$ denote a finite field of characteristic p and let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T})$ be a Galois representation that takes values in some finite-dimensional local commutative $\mathbb{F}_q$-algebra $\mathbb{T}$. Suppose that $\mathbb{T}$ is generated by the traces of ρ, and that ρ has big residual image, i.e. that $\mathrm{Im}(\overline{\rho}) = \mathrm{GL}_2^D(\mathbb{F}_q)$, where $D \subseteq \mathbb{F}_q^\times$.

The explicit description that we give in chapter 3 of the image of ρ in this situation allows us to compute a part of certain ray class field of the field K cut out by $\overline{\rho}$ (i.e. $G_K = \ker(\overline{\rho})$). More concretely, let $\mathfrak{m}$ denote the maximal ideal of $\mathbb{T}$ and $m = \dim_{\mathbb{F}_q} \mathfrak{m}/\mathfrak{m}^2$.

In section 4.1, for $p \neq 2$ and $q \neq 3, 5$ we prove that there exists an abelian extension L/K unramified outside Np and of degree p^{3dm} that cannot be defined over $\mathbb{Q}$, and

$$\mathrm{Gal}(L/\mathbb{Q}) = \underbrace{\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}_{m} \rtimes \mathrm{Gal}(K/\mathbb{Q}).$$

In section 4.2 we give an analogous result for $p = 2$ and $q \neq 2$, but since in this situation we have more than one possibility for the group $\mathrm{Gal}(L/\mathbb{Q})$ (cf. Section 3.5), with the same hypothesis we prove that there exists an abelian extension L/K unramified outside $2N$ and of degree $2^{3d\alpha+\beta}$ and there exist integers $0 \leq \alpha \leq m$ and $0 \leq \beta \leq m(d-\alpha)$ such that $t = q^\alpha((q-1)2^\beta) + 1)$ and

$$\mathrm{Gal}(L/\mathbb{Q}) = M \rtimes \mathrm{Gal}(K/\mathbb{Q}),$$

where M is an $\mathbb{F}_2[\mathrm{GL}_2^D(\mathbb{F}_q)]$-submodule of $\mathrm{M}_2^0(\mathfrak{m}/\mathfrak{m}^2)$ of the form $M := \mathrm{M}_2^0(\mathbb{F}_q)^\alpha \oplus C_2^\beta$. Moreover there exists an extension L_1 of K with $\mathrm{Gal}(L_1/K) \simeq \mathrm{M}_2^0(\mathbb{F}_q)^\alpha$ that cannot be defined over $\mathbb{Q}$ and an extension L_2 of K with $\mathrm{Gal}(L_2/K) = C_2^\beta$, such that $L = L_1L_2$.

Finally in section 4.3 we state some questions that arise in this context, and that could be a direction for further research.

4.1 Existence of p-elementary abelian extensions, $p \neq 2$

Let $\mathbb{F}_q$ be a finite field of characteristic p and let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T})$ be a Galois representation that takes values in some finite-dimensional local commutative $\mathbb{F}_q$-algebra $\mathbb{T}$. Suppose that $\mathbb{T}$ is generated by the traces of ρ, and that ρ has big residual image, i.e. $\mathrm{Im}(\overline{\rho}) = \mathrm{GL}_2^D(\mathbb{F}_q)$, where $D \subseteq \mathbb{F}_q^\times$. In this section we translate the results from section 3.4 to a computation of certain abelian extensions of K.

Proposition 4.1.1. *Let $\mathbb{F}_q$ be a finite field of characteristic $p \neq 2$ and degree d with $q \neq 3, 5$. Let $(\mathbb{T}, \mathfrak{m})$ be a finite-dimensional local commutative $\mathbb{F}_q$-algebra equipped with the discrete topology and with residue field $\mathbb{T}/\mathfrak{m} \simeq \mathbb{F}_q$. Suppose that $\mathfrak{m}^2 = 0$. Let $m := \dim_{\mathbb{F}_q} \mathfrak{m}$ and let t be the number of different traces in $\mathrm{Im}(\rho)$. Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T})$ be a Galois representation unramified outside Np such that*

(i) $\mathrm{Im}(\overline{\rho}) = \mathrm{GL}_2^D(\mathbb{F}_q)$, *where* $\overline{\rho} := G_{\mathbb{Q}} \to \mathrm{GL}_2^D(\mathbb{F}_q)$ *is the residual representation and* $D = \mathrm{Im}(\det \circ \overline{\rho})$.

(ii) $\mathrm{Im}(\rho) \subseteq \mathrm{GL}_2^D(\mathbb{T})$.

(iii) $\mathbb{T}$ *is generated as $\mathbb{F}_q$-algebra by the set of traces of ρ.*

Then there exist number fields $L/K/\mathbb{Q}$ with $G_L = \ker(\rho)$ and $G_K = \ker(\overline{\rho})$ such that $\mathrm{Gal}(K/\mathbb{Q}) = \mathrm{GL}_2^D(\mathbb{F}_q)$ *and*

$$\mathrm{Gal}(L/\mathbb{Q}) = \underbrace{\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}_{m} \rtimes \mathrm{Gal}(K/\mathbb{Q}),$$

with $\mathrm{Gal}(K/\mathbb{Q})$ *acting on* $\mathrm{Gal}(L/K)$ *by conjugation. Moreover, the extension L/K is an abelian extension of degree p^{3dm} that cannot be defined over $\mathbb{Q}$ and which is unramified at all primes $\ell \nmid Np$.*

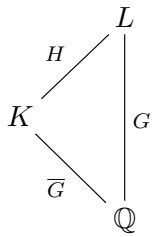
Proof. Let $\overline{G} := \mathrm{Im}(\overline{\rho})$, $G := \mathrm{Im}(\rho)$ and $H := \mathrm{M}_2^0(\mathbb{F}_q)^m$. By Theorem 3.1.1, we have that

$$G \simeq H \rtimes \overline{G}.$$

This gives a short exact sequence

$$1 \to H \to G \to \overline{G} \to 1,$$

so $\overline{G}$ acts on H by conjugation through preimages. Let $L := \overline{\mathbb{Q}}^{\ker(\rho)}$ and $K := \overline{\mathbb{Q}}^{\ker(\overline{\rho})}$. Then Galois theory tells us that we have field extensions as shown in the following diagram:



The group H is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{3dm}$, where $q = p^d$. Thus it is a p-elementary abelian group, so L/K is an abelian Galois extension, unramified outside Np and of degree p^{3dm}. Moreover, since H is a simple $\mathbb{F}_p[\mathrm{GL}_2^D(\mathbb{F}_q)]$-module and the conjugation action of $\overline{G}$ on H is nontrivial, we have that the extension L/K cannot be defined over $\mathbb{Q}$. □

4.2 Existence of 2-elementary abelian extensions

Proposition 4.2.1. *Let $\mathbb{F}_q$ be a finite field of characteristic 2 and degree $d \geq 2$. Let $(\mathbb{T}, \mathfrak{m})$ be a finite-dimensional local commutative $\mathbb{F}_q$-algebra equipped with the discrete topology and with residue field $\mathbb{T}/\mathfrak{m} \simeq \mathbb{F}_q$. Suppose that $\mathfrak{m}^2 = 0$. Let $m := \dim_{\mathbb{F}_q} \mathfrak{m}$ and let t be the number of different traces in $\mathrm{Im}(\rho)$. Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T})$ be a Galois representation such that*

(i) $\mathrm{Im}(\overline{\rho}) = \mathrm{GL}_2^D(\mathbb{F}_q)$, *where* $\overline{\rho} := G_{\mathbb{Q}} \to \mathrm{GL}_2^D(\mathbb{F}_q)$ *is the residual representation and* $D = \mathrm{Im}(\det \circ \overline{\rho})$.

(ii) $\mathrm{Im}(\rho) \subseteq \mathrm{GL}_2^D(\mathbb{T})$.

(iii) $\mathbb{T}$ *is generated as* $\mathbb{F}_q$*-algebra by the set of traces of* ρ.

Then there exist integers $0 \leq \alpha \leq m$ *and* $0 \leq \beta \leq d(m-\alpha)$ *such that* $t = q^\alpha \cdot ((q-1)2^\beta + 1)$, *and there exist number fields* $L/K/\mathbb{Q}$ *with* $G_L = \ker(\rho)$ *and* $G_K = \ker(\overline{\rho})$ *such that* $\mathrm{Gal}(K/\mathbb{Q}) = \mathrm{GL}_2^D(\mathbb{F}_q)$ *and*

$$\mathrm{Gal}(L/\mathbb{Q}) \simeq M \rtimes \mathrm{Gal}(K/\mathbb{Q}),$$

where M is an $\mathbb{F}_2[\mathrm{GL}_2^D(\mathbb{F}_q)]$-submodule of $\mathrm{M}_2^0(\mathfrak{m})$ of the form $M := \mathrm{M}_2^0(\mathbb{F}_q)^\alpha \oplus C_2^\beta$, and the group $\mathrm{Gal}(K/\mathbb{Q})$ acts by conjugation on $\mathrm{Gal}(L/K)$. The extension L/K is an abelian extension of degree $2^{3d\alpha+\beta}$ unramified at all primes $\ell \nmid 2N$.

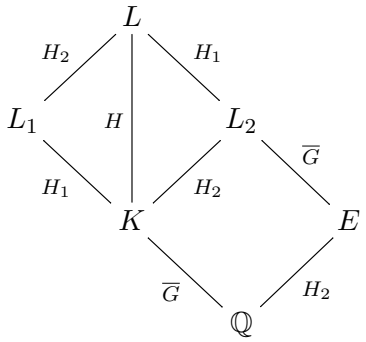
Moreover, if $\alpha \neq 0$ there exist an extension L_1 of K with $\mathrm{Gal}(L_1/K) \simeq \mathrm{M}_2^0(\mathbb{F}_q)^\alpha$ which cannot be defined over $\mathbb{Q}$ and an extension L_2 of K with $\mathrm{Gal}(L_2/K) = C_2^\beta$, such that $L = L_1 L_2$.

Proof. Let $\overline{G} := \mathrm{Im}(\overline{\rho})$, $G := \mathrm{Im}(\rho)$ and $H := \mathrm{M}_2^0(\mathbb{F}_q)^\alpha \oplus C_2^\beta \simeq C_2^{3d\alpha+\beta}$. By Proposition 3.2.2, we have that $G \simeq H \rtimes \overline{G}$. This gives a short exact sequence

$$1 \to H \to G \to \overline{G} \to 1,$$

so $\overline{G}$ acts on H by conjugation through preimages.

Let $L := \overline{\mathbb{Q}}^{\ker(\rho)}$ and $K := \overline{\mathbb{Q}}^{\ker(\overline{\rho})}$. Let $H_1 := \mathrm{M}_2^0(\mathbb{F}_q)^\alpha$, $H_2 := C_2^\beta$, $L_1 := \overline{\mathbb{Q}}^{H_1}$ and $L_2 := \overline{\mathbb{Q}}^{H_2}$. By Galois theory, we have field extensions as shown in the following diagram:



The group H is an abelian group of order $2^{3d\alpha+\beta}$, and the corresponding field extension is unramified outside $2N$ because ρ is. Moreover, since H_2 is contained in the centre of G, the action

of $\overline{G}$ on H_2 is trivial, so $L_1 = KE$, and the Galois group of the field extension L_1/K is isomorphic to the Galois group of $E/\mathbb{Q}$. On the other hand, H_2 is not contained in the centre of G, so the action of $\overline{G}$ on H_2 is nontrivial, and the extension L_2/K cannot be defined over $\mathbb{Q}$. □

Let us give an example that illustrates how one can compute explicitly some of these abelian extensions whose existence we deduce from the knowledge of the image of Galois representation with values in the mod p Hecke algebra.

Example 4.2.2. Let us take level $N = 67$ and weight $k = 2$. We can see in Table 3.8 that there exists a local Hecke algebra $(\mathbb{T}_f, \mathfrak{m}_f)$ associated to a mod p normalised eigenform $f \in S_k(N, 1; \mathbb{F}_4)$ such that the attached Galois representation

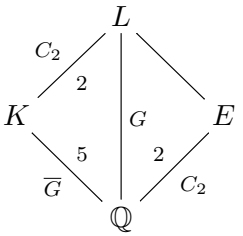
$$\rho_f : G_{\mathbb{Q}} \to \mathrm{SL}_2(\mathbb{T}_f)$$

has residual image $\mathrm{Im}(\overline{\rho}_f) = \mathrm{SL}_2(\mathbb{F}_q)$ and, by Conjecture 3.6.1, we have that the image of ρ_f is

$$G := \mathrm{Im}(\rho_f) \simeq C_2 \times \mathrm{SL}_2(\mathbb{F}_4),$$

where $C_2 \subseteq \mathrm{M}_2^0(\mathfrak{m}_f)$ denotes an order 2 subgroup of the trace 0 matrices with coefficients in $\mathfrak{m}_f \simeq \mathbb{F}_q$.

We use Proposition 4.2.1 to describe explicitly the number field L such that $G = \mathrm{Gal}(L/\mathbb{Q})$. Let K denote the number field such that $\overline{G} = \mathrm{Gal}(K/\mathbb{Q})$ and let E denote the quadratic number field such that $L = KE$.



We first will prove that

$$E \simeq \mathbb{Q}(\sqrt{-67}).$$

We know that L can only ramify at 2 and 67, since ρ_f is unramified at all $\ell \nmid 2 \cdot 67$. So E can only ramify there. This gives us only 7 possibilities for E:

$$\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{67}), \mathbb{Q}(\sqrt{-67}), \mathbb{Q}(\sqrt{2 \cdot 67}), \mathbb{Q}(\sqrt{-2 \cdot 67}).$$

Let D_E denote the discriminant of E. Since $\rho_f(\mathrm{Frob}_\ell)|_{\mathrm{Gal}(E/\mathbb{Q})} = \left(\frac{D_E}{\ell}\right)$ for $\ell \neq 2, 67$, we have that $\rho_f(\mathrm{Frob}_\ell) = \overline{\rho}_f(\mathrm{Frob}_\ell)$ if and only if ℓ splits in E. So if ℓ is split in E, $\mathrm{tr}(\rho_f(\mathrm{Frob}_\ell)) = \mathrm{tr}(\overline{\rho}_f(\mathrm{Frob}_\ell)) \in \mathbb{F}_4$, since $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathrm{SL}_2(\mathbb{F}_4)$. Now we only need to check when $\mathrm{tr}(\rho_f(\mathrm{Frob}_\ell))$ is not in $\mathbb{F}_4$ and compute the symbols $\left(\frac{E}{\ell}\right)$ for a few $\ell \nmid 2N$. For the 7 candidates that we have, we list here the results:

ℓ	$\mathrm{tr}(\rho_f(\mathrm{Frob}_\ell))$	$\left(\frac{\mathbb{Q}(\sqrt{-1})}{\ell}\right)$	$\left(\frac{\mathbb{Q}(\sqrt{2})}{\ell}\right)$	$\left(\frac{\mathbb{Q}(\sqrt{-2})}{\ell}\right)$	$\left(\frac{\mathbb{Q}(\sqrt{67})}{\ell}\right)$	$\left(\frac{\mathbb{Q}(\sqrt{-67})}{\ell}\right)$	$\left(\frac{\mathbb{Q}(\sqrt{2 \cdot 67})}{\ell}\right)$	$\left(\frac{\mathbb{Q}(\sqrt{-2 \cdot 67})}{\ell}\right)$
3	$\notin \mathbb{F}_4$	-1	-1	1	1	-1	-1	1
5	$\notin \mathbb{F}_4$	1	-1	-1	-1	-1	1	1
7	$\notin \mathbb{F}_4$	-1	1	-1	1	-1	1	-1

Thus we conclude that $E = \mathbb{Q}(\sqrt{-67})$.

Note that, among the 7 quadratic fields, we find the only one that ramifies at 67 and not at 2.

Now we want to compute the field K. We use Klüners' database on number fields to compute a defining polynomial for the field K. We know that $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathcal{A}_5$, so K has degree 5, and we also know that 67 divides the discriminant of K. If we set the following data

```
Degree 5
Group number 4
Maximal absolute value of the discriminant 10^50
Divisors of the discriminant 67
```

we find that there are two possibilities for K, namely:

- K_1 of discriminant $2^8 \cdot 67^2$, with generating polynomial: $x^5 + 2x^3 - 4x^2 + 6x - 4$,
- K_2 of discriminant $2^6 \cdot 67^2$, with generating polynomial: $x^5 - x^4 - x^3 + 7x^2 - 9x + 5$.

Since Klüners' database is complete up to a certain point, we know that there are no other $\mathcal{A}_5$ extensions with such a discriminant; hence, K is given by one of the two polynomials.

Let $\rho_i : G_{\mathbb{Q}} \to \mathrm{Gal}(K_i/\mathbb{Q}) \simeq \mathcal{A}_5$, for $i = 1, 2$. With a simple computation we can exclude K_2, since we have that $\rho_2(\mathrm{Frob}_5) = \rho_2(\mathrm{Frob}_{17}) = (1\ 2\ 3)$, but $\mathrm{tr}(\rho(\mathrm{Frob}_5)) = 1$ and $\mathrm{tr}(\rho(\mathrm{Frob}_{17})) = 0$. Thus the field we are looking for is $K = K_1 = \mathbb{Q}[x]/(x^5 + 2x^3 - 4x^2 + 6x - 4)$.

Finally, with Magma we can compute a generating polynomial $f(x)$ for the splitting field of the composite $L = EK$,

$$f(x) = x^{10} + 339x^8 - 8x^7 + 45442x^6 + 512x^5 + 3004454x^4 + 182712x^3 + 98136241x^2 + 6966880x + 1274297203.$$

The previous example, and many other similar examples that we have computed suggest the following.

Conjecture 4.2.3. Let $\mathbb{F}_q$ be a field of characteristic 2 and degree $d \geq 2$. Fix a level $N \geq 1$ and a weight $k \geq 2$. Let $f \in S_k(N, \varepsilon; \mathbb{F}_q)$ be a mod 2 normalised Hecke eigenform and let $(\mathbb{T}_f, \mathfrak{m}_f)$ denote its associated local mod 2 Hecke algebra over $\mathbb{F}_q$. Suppose that $\mathfrak{m}_f^2 = 0$. Let $\overline{\rho}_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_q)$ denote the attached residual Galois representation. Suppose that $\mathrm{Im}(\overline{\rho}_f) = \mathrm{GL}_2^D(\mathbb{F}_q)$, where $D = \mathrm{Im}(\det \circ \overline{\rho})$ and consider the Galois representation $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T}_f)$ attached to $\mathfrak{m}_f$. Assume that

(*i*) $\mathbb{T}_f$ is generated as $\mathbb{F}_q$-algebra by the set of traces of ρ_f,

(*ii*) $\mathrm{Im}(\rho_f) \subseteq \mathrm{GL}_2^D(\mathbb{T}_f)$,

(*iii*) we know that $t = (q-1)2^\beta + 1$, for some $0 \leq \beta \leq dm$ (equivalently, that $\mathrm{Im}(\rho) \simeq C_2^\beta \times \mathrm{GL}_2^D(\mathbb{F}_q)$).

Then, if E denotes the quadratic number field such that $C_2^\beta = \mathrm{Gal}(E/\mathbb{Q})$ and $L_2 = KE$, we have that

$$E = \mathbb{Q}\left(\sqrt{(-1)^{(N+1)/2}N}\right) = \begin{cases} \mathbb{Q}(\sqrt{N}) & \text{if} \quad N \equiv 1 \bmod 4, \\ \mathbb{Q}(\sqrt{-N}) & \text{if} \quad N \equiv 3 \bmod 4. \end{cases}$$

4.3 Further research

In this section we state some questions in order to suggest a possible direction for further research. The results of the previous chapters lead to the following natural question: is there a converse of Proposition 4.1.1 for characteristic $p \neq 2$ and a converse of Proposition 4.2.1 for characteristic 2? In other words, what predictions about local mod p Hecke algebras and congruences can be derived from class field theory?

Let us start with the case $p \geq 3$. Let $K/\mathbb{Q}$ be a totally imaginary Galois extension with Galois group $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathrm{GL}_2^D(\mathbb{F}_q)$, for some $D \subseteq \mathbb{F}_q^\times$ and $q \neq 3, 5$. Suppose that K admits a p-elementary abelian Galois extension L/K of degree q^{3m}, for some $m \geq 1$, such that:

(1) it is unramified outside Np, for some $N \geq 1$,

(2) $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathrm{Gal}(L/K) \rtimes \mathrm{Gal}(K/\mathbb{Q})$,

(3) $\mathrm{Gal}(L/K) \simeq \mathrm{M}_2^0(\mathbb{F}_q)^m$ as groups, and via the above identifications, the action of $\mathrm{GL}_2^D(\mathbb{F}_q)$ on $\mathrm{M}_2^0(\mathbb{F}_q)^m$ is by matrix conjugation.

Consider the local commutative $\mathbb{F}_q$-algebra $A := \mathbb{F}_q[X_1, \ldots, X_m]/(X_i X_j)_{1 \leq i,j \leq m}$. As explained in section 1.2, we have

$$\mathrm{M}_2^0(\mathbb{F}_q)^m \rtimes \mathrm{GL}_2^D(\mathbb{F}_q) \simeq \mathrm{GL}_2^D(A),$$

and we then get a Galois representation $\rho : G_\mathbb{Q} \to \mathrm{GL}_2(A)$ such that $\ker(\rho) = G_L$.

Question 4.3.1. Is A a quotient of some local mod p Hecke algebra $\mathbb{T}_f$ associated to a normalised Hecke eigenform $f \in S_k(N, \varepsilon; \overline{\mathbb{F}}_p)$ for some level $N \geq 1$, weight $k \geq 1$ and Dirichlet character $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{F}}_p^\times$?

Now suppose that $p = 2$ and $q \geq 4$. Let $K/\mathbb{Q}$ be a totally imaginary Galois extension with Galois group $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathrm{GL}_2^D(\mathbb{F}_q)$, for some $D \subseteq \mathbb{F}_q^\times$. Suppose that K admits an abelian Galois extension L/K of degree $q^{3\alpha} 2^\beta$, for some $0 \leq \alpha \leq m$ and $0 \leq \beta \leq d(m - \alpha)$ such that:

(1) it is unramified outside Np, for some $N \geq 2$,

(2) $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathrm{Gal}(L/K) \rtimes \mathrm{Gal}(K/\mathbb{Q})$,

(3) if $\alpha \neq 0$, there exists an extension L_1 of K with $\mathrm{Gal}(L_1/K) \simeq \mathrm{M}_2^0(\mathbb{F}_q)^\alpha$ which cannot be defined over $\mathbb{Q}$, and there exists an extension L_2/K with $\mathrm{Gal}(L_2/K) \simeq C_2^\beta$, such that $L = L_1 L_2$,

(4) via the above identifications, the action of $\mathrm{GL}_2^D(\mathbb{F}_q)$ on $\mathrm{M}_2^0(\mathbb{F}_q)^\alpha \oplus C_2^\beta$ is by matrix conjugation.

Consider the local commutative $\mathbb{F}_q$-algebra $A := \mathbb{F}_q[X_1, \ldots, X_m]/(X_i X_j)_{1 \leq i,j \leq m}$. Now we have

$$(\mathrm{M}_2^0(\mathbb{F}_q)^\alpha \oplus C_2^\beta) \rtimes \mathrm{GL}_2^D(\mathbb{F}_q) \subseteq \mathrm{GL}_2^D(A),$$

and we obtain a Galois representation $\rho : G_\mathbb{Q} \to \mathrm{GL}_2(A)$ such that $\ker(\rho) = G_L$.

In this setting, we ask ourselves the same question.

Part II

Mumford curves covering p-adic Shimura curves

Chapter 5

p-adic uniformisation of Shimura curves

In this chapter we introduce the reader to the theory of p-adic uniformisation of Shimura curves and we state the necessary results that will be needed afterwards.

First we briefly introduce the p-adic upper half-plane as a rigid analytic variety over $\mathbb{Q}_p$, a p-adic analog of the complex upper half-plane, which is the starting point of the construction of p-adic Shimura curves. Next we show how one constructs the Bruhat-Tits tree associated to $\mathrm{PGL}_2(\mathbb{Q}_p)$, an infinite graph that turns out to be the reduction of this p-adic upper half-plane, and we give a description of it that will allow us to make explicit computations on this tree later on. After that we recall the theorem of Čerednik and Drinfel'd (Theorem 5.3.1), which relates the complex and p-adic uniformisations of a Shimura curve by interchanging the local invariants p and ∞. This result together with Drinfel'd's theorem (Theorem 5.3.3) will be fundamental in the subsequent chapters. Finally we give a short exposition on the theory of Mumford curves over the ring of integers of a local field (cf. [Mum72]) and relate it to the theory of p-adic uniformisation of Shimura curves. For this, we introduce the notion of p-adic Schottky groups and recall the notion of *good* fundamental domains following [GvdP80].

Notation

From now on, p will denote a fixed odd prime integer and $\overline{\mathbb{Q}}_p$ a fixed algebraic closure of the field of p-adic numbers $\mathbb{Q}_p$. Once these data are fixed, $\mathbb{Q}_{p^2} \subseteq \overline{\mathbb{Q}}_p$ will denote the unramified quadratic extension of $\mathbb{Q}_p$ and $\mathbb{Z}_{p^2}$ its ring of integers, $\mathbb{Q}_p^{nr} \subseteq \overline{\mathbb{Q}}_p$ the maximal unramified extension of $\mathbb{Q}_p$ and $\mathbb{Z}_p^{nr}$ its ring of integers.

We take the usual convention for the p-adic absolute value to be defined as $|z| := 1/p^{v_p(z)}$, for every $z \in \mathbb{Q}_p$, where v_p denotes the p-adic valuation on $\mathbb{Q}_p$. Finally $\mathbb{C}_p$ will denote the completion of $\overline{\mathbb{Q}}_p$ with respect to the unique absolute value extending the p-adic absolute value.

5.1 The p-adic upper half-plane

Let us start denoting by $\mathbb{P}^{1,rig} := \mathbb{P}^{1,rig}_{\mathbb{Q}_p}$ the rigid analytic projective line over $\mathbb{Q}_p$. This is the rigidification of the algebraic projective line $\mathbb{P}^1_{\mathbb{Q}_p}$, as defined in [BGR84, 9.3.4], so that its set of L-points is $\mathbb{P}^{1,rig}(L) = \mathbb{P}^1(L)$, for every extension $\mathbb{Q}_p \subseteq L \subseteq \mathbb{C}_p$.

For $a = [a_0 : a_1] \in \mathbb{P}^1(\mathbb{Q}_p)$ and $r \in \mathbb{R}_{\geq 0}$, we denote by

$$\mathbb{B}^+(a, |p|^r) := \{[z_0 : z_1] \in \mathbb{P}^1(\mathbb{C}_p) : \ |z_0 a_1 - z_1 a_0| \leq |p|^r\} = \{z \in \mathbb{P}^1(\mathbb{C}_p) : \ v(z_0 a_1 - z_1 a_0) \geq r\},$$

$$\mathbb{B}^-(a, |p|^r) := \{[z_0 : z_1] \in \mathbb{P}^1(\mathbb{C}_p) : \ |z_0 a_1 - z_1 a_0| < |p|^r\} = \{z \in \mathbb{P}^1(\mathbb{C}_p) : \ v(z_0 a_1 - z_1 a_0) > r\},$$

the closed ball and open ball of $\mathbb{P}^{1,rig}$, respectively, with centre a and radius $|p|^r$. Obviously, the adjectives "closed" and "open" do not have any topological meaning, since in the topological space $\mathbb{Q}_p$, with its natural p-adic topology, all the balls are open and closed subsets. Alternatively, we can define the (open or closed) ball of $\mathbb{P}^{1,rig}$ with centre $[a_0 : a_1]$ and radius $|p|^r$ as one of the following subsets:

(i) if $[a_0 : a_1] = [a : 1] \simeq a \in \mathbb{Q}_p$, then $\{z \in \mathbb{C}_p : \ |z - a| \leq |p|^r\} = \mathbb{B}^+(a, |p|^r)$,

(ii) if $[a_0, a_1] = [1 : 0] =: \infty$, then $\{z \in \mathbb{C}_p : \ |z| \geq |p|^{-r}\} \cup \{\infty\} = \mathbb{B}^+(\infty, |p|^r)$.

It can be proven that a complement of open balls in $\mathbb{P}^1(\mathbb{C}_p)$ is an admissible open subset of $\mathbb{P}^{1,rig}$, and that every admissible open subset of $\mathbb{P}^{1,rig}$ is obtained as a union of such admissible open subsets (cf. [BGR84, 9.7.2/2]).

Definition 5.1.1. Let us consider a functor from the category of field extensions $\mathbb{Q}_p \subseteq L \subseteq \mathbb{C}_p$, to the category of sets defined as follows: for every extension L over $\mathbb{Q}_p$ consider the subset of points in $\mathbb{P}^{1,rig}(L)$

$$\mathcal{H}_p(L) := \mathbb{P}^1(L) \smallsetminus \mathbb{P}^1(\mathbb{Q}_p).$$

The set $\mathcal{H}_p(L)$ is not only a subset of $\mathbb{P}^1(L)$ but it is actually the set of L-points of a rigid analytic variety $\mathcal{H}_p$ over $\mathbb{Q}_p$ called the *p-adic upper half-plane* over $\mathbb{Q}_p$. One way to see this fact is by defining an open admissible cover of $\mathcal{H}_p(L)$.

Definition 5.1.2. For every integer $i \geq 0$ we define the following subsets of points of $\mathbb{P}^{1,rig}(L)$:

$$\mathcal{H}_p^{(i)}(L) := \mathbb{P}^1(L) \smallsetminus \bigcup_{a \in \mathbb{P}^1(\mathbb{Q}_p)} \mathbb{B}^-(a, |p|^i).$$

For every point $a = [a_0 : a_1] \in \mathbb{P}^1(\mathbb{Q}_p)$, one can choose *unimodular coordinates*, i.e. coordinates $(a_0, a_1) \in \mathbb{Z}_p^2$, so it makes sense to consider the reduction mod p^i of the point $a \in \mathbb{P}^1(\mathbb{Q}_p)$. The following easy lemma allows us to simplify the description of the subsets in Definition 5.1.2.

Lemma 5.1.3. *Let $i > 0$ be an integer and take $a, a' \in \mathbb{P}^1(\mathbb{Q}_p)$. Then*

(a) $\mathbb{B}^+(a, |p|^i) \cap \mathbb{B}^+(a', |p|^i) \neq \emptyset \Leftrightarrow a \equiv a' \pmod{p^i}$.

(b) $\mathbb{B}^-(a, |p|^i) \cap \mathbb{B}^-(a', |p|^i) \neq \emptyset \Leftrightarrow a \equiv a' \pmod{p^{i+1}}$. □

Let us denote by $\mathcal{P}_i$ a system of representatives for the points of $\mathbb{P}^1(\mathbb{Q}_p) = \mathbb{P}^1(\mathbb{Z}_p) \bmod p^i$, i.e. $\mathcal{P}_i$ is a system of representatives for the points $\mathbb{P}^1\left(\mathbb{Z}_p/p^i\mathbb{Z}_p\right)$ of the projective line. Therefore a point $a \in \mathcal{P}_i$ has unimodular coordinates (a_0, a_1) such that their reductions are $(\widetilde{a}_0, \widetilde{a}_1) \in \mathbb{Z}_p/p^i\mathbb{Z}_p \times \mathbb{Z}_p/p^i\mathbb{Z}_p$ not both $\equiv 0 \,(\mathrm{mod}\, p)$. Finally there is a bijection

$$\mathcal{P}_i \simeq \mathbb{Z}_p/p^i\mathbb{Z}_p \sqcup p\mathbb{Z}_p/p^i\mathbb{Z}_p.$$

In particular $\mathcal{P}_1 \simeq \mathbb{P}^1(\mathbb{F}_p) = \mathbb{F}_p \cup \{\infty\}$. The cardinality of the set $\mathcal{P}_i$ is $p^i + p^{i-1} = p^{i-1}(p+1)$. Therefore, by that basic property of non-archimedean balls to be either disjoint or one contained into the other, and applying Lemma 5.1.3, we find that, for every integer $i > 0$,

$$\mathcal{H}_p^{(i)}(L) = \mathbb{P}^1(L) \smallsetminus \bigcup_{a \in \mathcal{P}_i} \mathbb{B}^-(a, |p|^{i-1}).$$

As a consequence we obtain that the sets $\mathcal{H}_p^{(i)}$ are admissible affinoid subdomains of the rigid analytic projective line $\mathbb{P}^{1,rig}$. If one proves that the cover $\{\mathcal{H}_p^{(i)}\}_{i>0}$ is admissible, then $\mathcal{H}_p$ is proved to be a rigid analytic variety over $\mathbb{Q}_p$ (following definitions of [BGR84, Ch. 9.3]). A proof of this last assertion can be found in [SS91].

5.2 The Bruhat-Tits tree associated to $\mathrm{PGL}_2(\mathbb{Q}_p)$

A lattice $M \subseteq \mathbb{Q}_p^2$ is a free $\mathbb{Z}_p$-module of rank 2. Two lattices $M, M' \subseteq \mathbb{Q}_p^2$ are said to be homothetic if there exists $\lambda \in \mathbb{Q}_p^\times$ such that $M' = \lambda M$. We will denote by $\{M\}$ the homothety class of M. For every two homothety classes $\{M\}, \{M'\}$ we can always choose their representatives such that $p^n M \subseteq M' \subseteq M$, for some $n \in \mathbb{N}$ (cf. [Ser77, 1.1]). For example, if $M = \langle u, v\rangle$, then we can take $M' = \langle u, p^n v\rangle$. We say that two homothety classes $\{M\}, \{M'\}$ are *adjacent* if their representatives can be chosen so that $pM \subsetneq M' \subsetneq M$.

Definition 5.2.1. We define the graph $\mathcal{T}_p$ whose set of vertices $\mathrm{Ver}(\mathcal{T}_p)$ consists of the homothety classes of lattices of $\mathbb{Q}_p^2$ and whose set of oriented edges $\mathrm{Ed}(\mathcal{T}_p)$ is the set of pairs of adjacent classes. One can also consider the set of unoriented edges, which is formed by unordered pairs of adjacent classes. The graph $\mathcal{T}_p$ is a $(p+1)$-regular tree (cf. [Ser77, Ch. II]) which is known in the literature as the *Bruhat-Tits tree* associated to $\mathrm{PGL}_2(\mathbb{Q}_p)$.

The group $\mathrm{PGL}_2(\mathbb{Q}_p)$ acts transitively on the set of vertices $\mathrm{Ver}(\mathcal{T}_p)$: if $M = \langle u, v\rangle \subseteq \mathbb{Q}_p^2$ and $\gamma \in \mathrm{GL}_2(\mathbb{Q}_p)$ then $\gamma \cdot M := \langle \gamma u, \gamma v\rangle$, and the induced action of $\mathrm{PGL}_2(\mathbb{Q}_p)$ on the classes of lattices is then clearly well-defined and transitive.

Notation 5.2.2. If $e = (v, v') \in \mathrm{Ed}(\mathcal{T}_p)$ is an oriented edge then we denote by $-e := (v', v)$ the inverse edge and we will sometimes denote by $\{e, -e\}$ the corresponding unoriented edge (according to [Kur79, Definition 3-1]).

The tree $\mathcal{T}_p$, that we have defined as a combinatorial object, can be also realised as a topological space by the interpretation of its vertices as classes of norms over $\mathbb{Q}_p$ (cf. [BC91, Introduction, Sec. 1]). With this topology, the map $\gamma \in \mathrm{PGL}_2(\mathbb{Q}_p) \longmapsto \gamma \cdot v \in \mathrm{Ver}(\mathcal{T}_p)$ induces an homeomorphism

$$\mathrm{PGL}_2(\mathbb{Q}_p)/\mathrm{PGL}_2(\mathbb{Z}_p) \simeq \mathcal{T}_p,$$

where $\mathrm{PGL}_2(\mathbb{Q}_p)$ is taken with its natural topology. Therefore, we can represent each vertex by a class of matrices. Namely, if $v = \{M\}$ then v is represented by the class $\{\alpha_M\} \in \mathrm{PGL}_2(\mathbb{Q}_p)/\mathrm{PGL}_2(\mathbb{Z}_p)$ such that α_M is the matrix whose columns form a basis of M.

Remark 5.2.3. As usual, this homeomorphism is an immediate consequence of the fact that the action is transitive and the stabiliser of the vertex $v^0 := \{\langle (1,0),(0,1)\rangle\}$ inside $\mathrm{PGL}_2(\mathbb{Q}_p)$ is $\mathrm{PGL}_2(\mathbb{Z}_p)$ (cf. [Shi70, 1.2]). The analogous archimedean statement is the homeomorphism $\mathrm{PSL}_2(\mathbb{R})/\mathrm{SO}_2(\mathbb{R}) \simeq \mathcal{H}$, where $\mathcal{H}$ is the Poincar upper-half plane.

Remark 5.2.4. Note that matrices lying in the same class do not always have the same determinant. Their determinants, though, have the same parity in the p-adic valuation. So we can say that a vertex $v = \{\alpha\} \in \mathrm{PGL}_2(\mathbb{Q}_p)/\mathrm{PGL}_2(\mathbb{Z}_p)$ is *even* if $v_p(\det\alpha) \equiv 0 \pmod 2$ and that it is *odd* otherwise. Note also that a transformation $\gamma \in \mathrm{PGL}_2(\mathbb{Q}_p)$ sends a vertex v to another one with the same parity if and only if $v_p(\det\gamma)$ is even.

From now on we will denote by v^0 the vertex of $\mathcal{T}_p$ whose representative is the lattice $M^0 := \langle (1,0),(0,1)\rangle$. Once we have a distinguished vertex, we can describe the Bruhat-Tits tree $\mathcal{T}_p$ as follows.

(a) We begin by describing the set of vertices of $\mathcal{T}_p$ adjacent to v^0. For every $i \in \mathbb{P}^1(\mathbb{F}_p)$, let $v_i^{(1)}$ denote the vertex represented by the matrix $\alpha_i^{(1)}$ where

$$\alpha_i^{(1)} := \begin{cases} \begin{pmatrix} p & i \\ 0 & 1 \end{pmatrix}, & \text{if } i \neq \infty, \\ \\ \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}, & \text{if } i = \infty. \end{cases}$$

This defines $p+1$ different vertices $v_0^{(1)}, \ldots, v_{p-1}^{(1)}, v_\infty^{(1)}$ which are adjacent to v^0.

(b) For every new vertex $v_i^{(1)}$, we define the new p adjacent vertices as the vertices $v_j^{(2)}$ represented by the matrices

$$\alpha_{ij}^{(2)} := \begin{cases} \begin{pmatrix} p^2 & j \\ 0 & 1 \end{pmatrix}, & \text{if } i \neq \infty,\ \ 0 \leq j \leq p^2-1,\ \ j \equiv i \pmod p, \\ \\ \begin{pmatrix} 1 & 0 \\ j & p^2 \end{pmatrix}, & \text{if } i = \infty,\ \ 0 \leq j \leq p^2-1,\ \ j \equiv 0 \pmod p. \end{cases}$$

(c) Finally we denote by $e_i^{(1)}$ the oriented edge $(v^0, v_i^{(1)})$, by $e_{ij}^{(2)}$ the oriented edge $(v_i^{(1)}, v_{ij}^{(2)})$, etc.

The vertex v^0 corresponds to the projective line $\mathbb{P}^1_{\mathbb{Z}_p} = \mathbb{P}(M^0)$ associated to the lattice $M^0 = \mathbb{Z}_p^2$ in [Mum72, Sec. 2] and the $p+1$ adjacent vertices correspond to projective lines obtained by blowing up the $p+1$ $\mathbb{F}_p$-rational points of $\mathbb{P}^1_{\mathbb{F}_p}$ inside $\mathbb{P}^1_{\mathbb{Z}_p}$.

With this description of the tree in terms of matrices and taking the system of representatives defined above, we can define the following ascending chain of subtrees of $\mathcal{T}_p$. For every integer $i \geq 0$,

denote by $\mathcal{T}_p^{(i)}$ the subtree of $\mathcal{T}_p$ whose set of vertices is $\mathrm{Ver}(\mathcal{T}_p^{(i)}) := \{v = \{\alpha\} \mid \ v_p(\det\alpha) \leq i\}$. Then,

$$\mathrm{Ver}(\mathcal{T}_p^{(0)}) = \{v^0\},\ \mathrm{Ver}(\mathcal{T}_p^{(i)}) \subseteq \mathrm{Ver}(\mathcal{T}_p^{(i+1)}) \text{ for every } i \geq 0, \text{ and } \mathcal{T}_p = \bigcup_{i\geq 0} \mathcal{T}_p^{(i)}.$$

Remark 5.2.5. If we look back at the admissible cover defined for the upper half-plane $\mathcal{H}_p$, then we observe that the set of representatives $\mathcal{P}_i$ for the points of the projective line $\mathbb{P}(\mathbb{Z}_p/p^i\mathbb{Z}_p)$ corresponds bijectively with the set of "added vertices" of the subtree $\mathcal{T}_p^{(i)}$, i.e. there is a bijection of sets

$$\mathrm{Ver}(\mathcal{T}_p^{(i)}) \smallsetminus \mathrm{Ver}(\mathcal{T}_p^{(i-1)}) \simeq \mathcal{P}_i,$$

for every $i \geq 1$. The intuition then would suggest that removing open balls in $\mathbb{P}^{1,rig}(\mathbb{C}_p)$ with center in $\mathcal{P}_i$ corresponds through this bijection to adding to the subtree $\mathcal{T}_p^{(i-1)}$ the missing vertices of the subtree $\mathcal{T}_p^{(i)}$. This intuition finds its theoretical explanation in the following theorem (cf. [BC91] and [DT07] for a proof).

Theorem 5.2.6. *For every extension $\mathbb{Q}_p \subseteq L \subseteq \mathbb{C}_p$, there is a map*

$$\mathrm{Red} : \mathcal{H}_p(L) \to \mathcal{T}_p$$

satisfying the following properties.

(a) *It is equivariant with respect to the action of* $\mathrm{PGL}_2(\mathbb{Q}_p)$*, i.e.* $\mathrm{Red}(\gamma\cdot z) = \gamma\cdot\mathrm{Red}(z)$ *for every* $z \in \mathcal{H}_p(L)$ *and every* $\gamma \in \mathrm{PGL}_2(\mathbb{Q}_p)$.

(b) *The image* $\mathrm{Red}(\mathcal{H}_p^{(i)})$ *is the rational geometric realisation of the tree* $\mathcal{T}_p^{(i-1)}$*, for every* $i \geq 0$. □

We write this map as $\mathrm{Red} : \mathcal{H}_p \to \mathcal{T}_p$ and call it the *reduction map* associated to $\mathcal{H}_p$. This reduction map just defined owes its name to the fact that it is intimately related with the usual reduction modulo the prime p. Actually, the Tate algebra of series of the affinoid subdomains $\mathcal{H}_p^{(i)}$ can be reduced modulo p through the reduction mod p of restricted series, and this gives an algebraic variety over $\mathbb{F}_p$. It is then an exercise to see that the dual graph of the reduction mod p of $\mathcal{H}_p^{(i)}$ (i.e. the graph whose vertices are the irreducible components of the algebraic variety over $\mathbb{F}_p$ and such two vertices are adjacent if and only if the corresponding irreducible components meet) is the tree $\mathcal{T}_p^{(i-1)}$. This is done in [BC91, 2.3] where in fact the affinoid subdomain $\mathcal{H}_p^{(i)}$ is defined by $\mathcal{H}_p^{(i)} := \mathrm{Red}^{-1}(\mathcal{T}_{p,\mathbb{Q}}^{(i-1)})$.

Note here that the reduction mod p of $\mathcal{H}_p^{(i)}$ is a finite algebraic variety and the corresponding tree $\mathcal{T}_p^{(i-1)}$ is a finite tree, which makes perfect sense. Taking direct limit, we obtain that the dual graph of the reduction mod p of the rigid analytic variety $\mathcal{H}_p$ is the infinite tree $\mathcal{T}_p$. Finally we can claim concisely that "the reduction map Red is the dual of the reduction mod p associated to the rigid analytic space $\mathcal{H}_p$".

5.3 Čerednik-Drinfel'd theorem

Let B be an indefinite quaternion algebra over $\mathbb{Q}$ of discriminant Dp, and let $\mathcal{O}_B = \mathcal{O}_B(N) \subseteq B$ be an Eichler order of level N with $(Dp, N) = 1$. Once we have fixed a real matrix immersion

$\Phi_\infty : B \hookrightarrow \mathrm{M}_2(\mathbb{R})$, we consider the following discrete subgroup of $\mathrm{PGL}_2(\mathbb{R})_{>0} \simeq \mathrm{PSL}_2(\mathbb{R})$:

$$\Gamma_{\infty,+} := \Phi_\infty(\{\alpha \in \mathcal{O}_B^\times \mid \mathrm{Nm}(\alpha) > 0\})/\mathbb{Z}^\times.$$

By a fundamental result of Shimura [Shi67, Main Theorem I], there exists a proper algebraic curve $X(Dp, N)$ over $\mathbb{Q}$ such that its complex points are parametrised by a holomorphic bijective map

$$J : \Gamma_{\infty,+}\backslash\mathcal{H} \xrightarrow{\sim} X(Dp, N)(\mathbb{C}),$$

and which is characterised, up to isomorphisms over $\mathbb{Q}$, by the arithmetic property that the values of J at certain special parameters $\tau \in \Gamma_{\infty,+}\backslash\mathcal{H}$ are algebraic points $J(\tau) \in X(Dp, N)(\mathbb{Q}^{ab})$ defined over some ray class field of $\mathbb{Q}$. These special parameters are sometimes referred to as CM parameters and the corresponding algebraic points are called CM points. The curve $X(Dp, N)$ satisfying this property is called *the Shimura curve* of discriminant Dp and level N.

Since $X(Dp, N)$ is a scheme of locally finite type over $\mathbb{Q}$ we can consider, on one hand, its complex analytification $(X(Dp, N) \otimes_{\mathbb{Q}} \mathbb{C})^{an}$ (given by Serre's GAGA functor), which is a complex manifold, and on the other hand its p-adic rigidification $(X(Dp, N) \otimes_{\mathbb{Q}} \mathbb{Q}_p)^{rig}$ which is a rigid analytic variety over $\mathbb{Q}_p$ (cf. [Bos14]). While the complex analytification is uniformised by the discrete cocompact subgroup $\Gamma_{\infty,+} \subseteq \mathrm{Aut}(\mathcal{H})$, as we have recalled above, the p-adic rigidification also admits a uniformisation by a discrete cocompact subgroup $\Gamma_p \subseteq \mathrm{PGL}_2(\mathbb{Q}_p) \simeq \mathrm{Aut}(\mathcal{H}_p)$, which is known as the p-adic uniformisation of the Shimura curve $X(Dp, N)$ (or as the Čerednik-Drinfel'd uniformisation).

The group Γ_p is defined, following Čerednik [Cer76, Theorem 2.1], by *interchanging the local invariants* p and ∞ in the quaternion algebra B. More concretely, let H be the definite quaternion algebra of discriminant D, let $\mathcal{O}_H = \mathcal{O}_H(N) \subseteq H$ be an Eichler order of level N, and consider the localised order $\mathcal{O}_H[1/p] := \mathcal{O}_H \otimes_{\mathbb{Z}} \mathbb{Z}[1/p]$ over $\mathbb{Z}[1/p]$. Once we have fixed a p-adic matrix immersion $\Phi_p : H \hookrightarrow \mathrm{M}_2(\mathbb{Q}_p)$, let us consider the following discrete cocompact subgroup of $\mathrm{PGL}_2(\mathbb{Q}_p)$:

$$\Gamma_p := \Phi_p(\mathcal{O}_H[1/p]^\times)/\mathbb{Z}[1/p]^\times.$$

Then the Čerednik-Drinfel'd Theorem can be stated in the following way.

Theorem 5.3.1. *There is an isomorphism*

$$\Gamma_p\backslash(\mathcal{H}_p \otimes_{\mathbb{Q}_p} \mathbb{Q}_{p^2}) \simeq (X(Dp, N) \otimes_{\mathbb{Q}} \mathbb{Q}_p)^{rig}$$

of rigid analytic varieties over $\mathbb{Q}_p$.

Remark 5.3.2. Note that even if the $\mathbb{Z}$-order $\mathcal{O}_H$ is not always unique up to conjugation, the $\mathbb{Z}[1/p]$-order $\mathcal{O}_H[1/p]$ is, since this one satisfies Eichler's condition (cf. [Vig80, Corollaire 5.7]). Therefore the conjugacy class of the group Γ_p inside $\mathrm{PGL}_2(\mathbb{Q}_p)$ is well determined and gives rise to a rigid analytic variety $\Gamma_p\backslash\mathcal{H}_p$, which is well-defined up to rigid analytic isomorphisms. The same arguments as in the complex case show that the isomorphism class over $\mathbb{Q}$ of the curve $X(Dp, N)$ does not depend on the Eichler order chosen in the conjugacy class of $\mathcal{O}_B(N)$.

Now recall that since the curve $X(Dp, N) \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is proper, by a theorem of Raynaud its rigidification can be interpreted as the generic fibre of a $\mathbb{Z}_p$-formal scheme, which is obtained as the

completion of an adequate integral model $\mathcal{X}(Dp,N)$ over $\mathbb{Z}_p$ of $X(Dp,N)$ along its special fibre. We call *Drinfel'd integral model* over $\mathbb{Z}_p$ of the Shimura curve $X(Dp,N)$ the integral model $\mathcal{X}(Dp,N)$ over $\mathbb{Z}_p$ whose completion along its special fibre is the following formal scheme over $\operatorname{Spf}\mathbb{Z}_p$:

$$\Gamma_p\backslash(\widehat{\mathcal{H}}_p\otimes_{\operatorname{Spf}\mathbb{Z}_p}\operatorname{Spf}\mathbb{Z}_{p^2})\simeq\widehat{\mathcal{X}(Dp,N)}.$$

Drinfel'd constructed this integral model in [Dri76] as a solution of a moduli problem over $\mathbb{Z}_p$, extending the modular interpretation of $X(Dp,N)(\mathbb{C})$. As a direct consequence of Theorem 5.3.1, algebraising the rigid analytic spaces above we find the following more precise statement (cf. [JL84] for more details).

Theorem 5.3.3 (Drinfel'd theorem)**.** *Let $\Gamma_{p,+}$ be the subgroup of $\mathrm{PGL}_2(\mathbb{Q}_p)$ defined by*

$$\Gamma_{p,+}:=\Phi_p(\{\alpha\in\mathcal{O}_H[1/p]^\times\mid v_p(\mathrm{Nm}_{H/\mathbb{Q}}(\alpha))\equiv 0\bmod 2\})/\mathbb{Z}[1/p]^\times,$$

and let $X_{p,+}$ be the algebraic curve over $\mathbb{Q}_p$ such that

$$\Gamma_{p,+}\backslash\mathcal{H}_p\simeq X_{p,+}^{rig}.$$

Then the p-adic Shimura curve $X(Dp,N)\otimes_{\mathbb{Q}}\mathbb{Q}_p$ is a quadratic twist over $\mathbb{Q}_{p^2}$ of the algebraic curve $X_{p,+}$, i.e. there exists an isomorphism of curves over $\mathbb{Q}_{p^2}$

$$(X(Dp,N)\otimes_{\mathbb{Q}}\mathbb{Q}_p)\otimes_{\mathbb{Q}_p}\mathbb{Q}_{p^2}\simeq X_{p,+}\otimes_{\mathbb{Q}_p}\mathbb{Q}_{p^2}.$$

In particular, there is a bijection between the following sets of $\mathbb{Q}_{p^2}$-points:

$$\Gamma_{p,+}\backslash\mathcal{H}_p(\mathbb{Q}_{p^2})\simeq X(Dp,N)(\mathbb{Q}_{p^2}),$$

and the reduction-graph of the special fibre of $\mathcal{X}(Dp,N)$ is the quotient graph $\Gamma_{p,+}\backslash\mathcal{T}_p$. □

Remark 5.3.4. If we think the field of complex numbers $\mathbb{C}$ as the quadratic unramified extension of $\mathbb{Q}_\infty=\mathbb{R}$, we obtain the well-known bijection of sets:

$$\Gamma_{\infty,+}\backslash\mathcal{H}\simeq X(Dp,N)(\mathbb{C}),$$

describing the complex uniformisation of the Shimura curves $X(Dp,N)$.

Remark 5.3.5. The group $\Gamma_{p,+}$ is not always torsion-free but, as we shall see in the following, it admits a torsion-free normal and finite index subgroup (cf. Lemma 5.4.6). Therefore we will see that the curve $X_{p,+}$ is actually a finite quotient of a Mumford curve.

5.4 p-adic Schottky groups and good fundamental domains

Denote by $K\subseteq\overline{\mathbb{Q}}_p$ a finite extension of $\mathbb{Q}_p$, by $\mathcal{O}_K$ its ring of integers (which is a local noetherian ring of Krull dimension 1), and by k its residue field.

Remark 5.4.1. First of all, let us observe that the definition we have given of p-adic upper half-plane and p-adic Bruhat-Tits tree can be easily extended to an arbitrary local field K. We would then find a rigid analytic variety $\mathcal{H}$ over K whose set of L-points is $\mathcal{H}(L)=\mathbb{P}^1_K(L)\smallsetminus\mathbb{P}^1(K)$ together with the Bruhat-Tits tree $\mathcal{T}$ associated to $\mathrm{PGL}_2(K)$, which can be identified with the reduction of $\mathcal{H}$.

Definition 5.4.2. Let $\Gamma \subseteq \mathrm{PGL}_2(\mathbb{Q}_p)$ be a subgroup. A point $z \in \mathbb{P}^1(\mathbb{C}_p)$ is called a *limit point with respect to* Γ if there exist a point $y \in \mathbb{P}^1(\mathbb{C}_p)$ and a sequence $\{\gamma_n\}_{n\in\mathbb{N}}$ of different elements in Γ such that $\lim \gamma_n y = z$.

Let $\mathcal{L}_\Gamma \subseteq \mathbb{P}^1(\mathbb{C}_p)$ denote the set of limit points with respect to Γ.

Definition 5.4.3. A subgroup $\Gamma \subseteq \mathrm{PGL}_2(K)$ is called a *p-adic Schottky group* if it satisfies the following conditions:

(i) it is discontinuous, i.e. its associated set of limit points $\mathcal{L}_\Gamma$ is different from $\mathbb{P}^1(\mathbb{C}_p)$,

(ii) it is finitely generated,

(iii) it has no elements of finite order different from the identity I_2; equivalently, all transformations $\gamma \in \Gamma, \gamma \neq \mathrm{I}_2$, are hyperbolic.

Given a Schottky group $\Gamma \subseteq \mathrm{PGL}_2(K)$, let us denote by $\widehat{\mathcal{H}}_\Gamma$ the admissible formal scheme over $\mathrm{Spf}\,\mathcal{O}_K$ whose generic fibre is the rigid analytic variety $\mathcal{H}_\Gamma := \mathbb{P}^{1,rig} \smallsetminus \mathcal{L}_\Gamma$, and by $\mathcal{T}_\Gamma$ the dual graph of its special fibre. Note that since $\mathcal{L}_\Gamma \subseteq \mathbb{P}^1(K)$, we have that $\mathcal{H}_\Gamma$ is a subdomain of $\mathcal{H}$ and $\mathrm{Ver}(\mathcal{T}_\Gamma)$ a subset of the vertices of $\mathcal{T}$. Moreover, we also know that, actually, $\mathcal{T}_\Gamma$ is a subtree of $\mathcal{T}$, since $\dim(\mathcal{O}_K) = 1$.

In his celebrated paper [Mum72] Mumford proved that for every Schottky group Γ there exists a proper curve $\mathcal{C}_\Gamma$ over $\mathcal{O}_K$ such that $\Gamma\backslash\widehat{\mathcal{H}}_\Gamma \simeq \widehat{\mathcal{C}}_\Gamma$ is an isomorphism of formal schemes over $\mathrm{Spf}\,\mathcal{O}_K$. The curve $\mathcal{C}_\Gamma$ is a stable curve (in the sense of Deligne and Mumford) such that its special fibre $\mathcal{C} \otimes_{\mathcal{O}_K} k$ is k-split degenerate and whose dual graph is the quotient graph $\Gamma\backslash\mathcal{T}_\Gamma$ (cf. [Mum72, Definition 3.2 and Theorem 3.3]). Finally Mumford also proved that the correspondence $\Gamma \mapsto \mathcal{C}_\Gamma$ induces a bijection between the set of isomorphy classes of stable curves $\mathcal{C}$ over $\mathcal{O}_K$ with k-split degenerate special fibre and the set of conjugacy classes of Schottky groups $\Gamma \subseteq \mathrm{PGL}_2(K)$.

When $K = \mathbb{Q}_p$ and the Schottky group $\Gamma \subseteq \mathrm{PGL}_2(K)$ is cocompact, we have that $\mathcal{L}_\Gamma = \mathbb{P}^1(\mathbb{Q}_p)$, $\mathcal{H}_\Gamma = \mathcal{H}_p$, and $\mathcal{T}_\Gamma = \mathcal{T}_p$.

Definition 5.4.4. Let $\Gamma \subseteq \mathrm{PGL}_2(\mathbb{Q}_p)$ be a Schottky group of rank g, let $S = \{\gamma_1, \ldots, \gamma_g\}$ be a system of generators for Γ. A *good fundamental domain* for Γ with respect to S is an admissible subdomain of $\mathcal{H}_p$,

$$\mathcal{F}_\Gamma = \mathbb{P}^1(\mathbb{C}_p) \smallsetminus \bigcup_{i=1}^{2g} \mathbb{B}^-(\alpha_i, \rho_i),$$

which satisfies the following conditions:

(i) the centres α_i are in $\mathbb{P}^1(\mathbb{Q}_p)$, for every $1 \leq i \leq 2g$,

(ii) the closed balls $\mathbb{B}_i^+(\alpha_i, \rho_i)$, for $1 \leq i \leq 2g$, are pair-wise disjoint,

(iii) for every $1 \leq i \leq g$,

$$\gamma_i(\mathbb{P}^1(\mathbb{C}_p) \smallsetminus \mathbb{B}^-(\alpha_i, \rho_i)) = \mathbb{B}^+(\alpha_{i+g}, \rho_{i+g}),$$

$$\gamma_i(\mathbb{P}^1(\mathbb{C}_p) \smallsetminus \mathbb{B}^+(\alpha_i, \rho_i)) = \mathbb{B}^-(\alpha_{i+g}, \rho_{i+g}).$$

Remark 5.4.5. The fact that the domain $\mathcal{F}_\Gamma$ defined above is a fundamental domain (in the usual sense) for the action of Γ is proved in [GvdP80, Proposition 4.1]. Nevertheless, as observed by Gerritzen in [Ger74], it is possible to construct an admissible subdomain $\mathcal{F} \subseteq \mathbb{P}^1(\mathbb{C}_p)$ satisfying Proposition [GvdP80, Proposition 4.1] and which is not a *good* fundamental domain with respect to any system of generators of the group Γ considered.

In [Ger74] and [GvdP80, Ch. I] the existence of good fundamental domains for every Schottky group is proved, making use of the non-archimedean analog of Ford's method of isometry circles.

The following theorem is the p-adic analog of a well-known result about discrete subgroups of $\mathrm{PSL}_2(\mathbb{R})$, and more in general about discrete subgroups of $\mathrm{PGL}_2(\mathbb{C})$, which was first proved by Selberg in [Sel60, Lemma 8]. This is one of the key steps in the proof of the theorem of Čerednik-Drinfel'd, since it allows us to reduce to the case of Mumford curves through a finite cover. By this result we find that the curve $X_{p,+}$ of Theorem 5.3.3 is a finite quotient of a Mumford curve. Therefore the p-adic Shimura curve is a quadratic twist of a finite quotient of a Mumford curve. Since this result is also at the base of the method that we are going to present in Chapter 7 for finding Mumford curves covering certain p-adic Shimura curves, we sketch here a proof.

Theorem 5.4.6. *Let $\Gamma \subseteq \mathrm{PGL}_2(\mathbb{Q}_p)$ be a discontinuous and finitely generated group. Then there exists a normal subgroup Γ^{Sch} of finite index which is torsion-free. In particular Γ^{Sch} is a p-adic Schottky group.*

Proof. Let S be a subset of elements of finite order in Γ such that every element of finite order in Γ is conjugated to an element in S. It is easy to prove that the set S can be taken to be finite (cf. for example [GvdP80, Lemma 3.3.2]). Since Γ is finitely generated, we can find a ring $R \subseteq \mathbb{Q}_p$ which is finitely generated over $\mathbb{Z}_p$ and such that $\Gamma \subseteq \mathrm{PGL}_2(R) \subseteq \mathrm{PGL}_2(\mathbb{Q}_p)$. Since S is finite, there exists a maximal ideal $\mathfrak{m} \subseteq R$ such that, for every $\sigma \in S$, $\sigma \neq \mathrm{I}_2$, we have $\sigma - \mathrm{I}_2 \notin \mathfrak{m}$. Therefore, the group

$$\Gamma^{Sch} := \Gamma(\mathfrak{m}) := \{\gamma \in \Gamma \mid \gamma - \mathrm{I}_2 \in \mathfrak{m}\}$$

is a normal subgroup of Γ of finite index (since $R/\mathfrak{m}$ is a finite field) and from the fact that $\Gamma(\mathfrak{m})$ is normal it follows that $\Gamma(\mathfrak{m})$ does not contain any of the elements of finite order in the group Γ. □

Chapter 6

Modular arithmetic in definite quaternion algebras

The aim of this chapter is to prove a unique factorisation result (Theorem 6.3.4) for Eichler orders inside a definite quaternion algebra with one-sided ideal class number $h(D, N)$ equal to 1, which generalises the *Zerlegungssatz* for the Hurwitz quaternions in [Hur96]. In order to do this, we need to introduce the notion of *ξ-primary quaternion*, which extends the notion of primary quaternions introduced in [Hur96] for the order of Hurwitz quaternions.

In the first section we briefly recall the theory of arithmetic in definite quaternion algebras. In section 6.2 we develop some tools on the modular arithmetic of Eichler orders $\mathcal{O}$ over $\mathbb{Z}$ with $h(D, N) = 1$. We are particularly interested in abelian quotient groups of the form $\mathcal{O}/\xi\mathcal{O}$, where $\xi\mathcal{O}$ is an integral principal ideal. Consider the natural projection $\lambda_r : \mathcal{O}/\mathrm{Nm}(\xi) \twoheadrightarrow \mathcal{O}/\xi\mathcal{O}$ and denote by $(\mathcal{O}/\xi\mathcal{O})_r^\times$ the image of the unit group $(\mathcal{O}/\mathrm{Nm}(\xi))^\times$ under λ_r. Suppose that $\mathcal{O}^\times$ acts freely on $(\mathcal{O}/\xi\mathcal{O})_r^\times$, where the action is just right-multiplication. Then we call a system of representatives $\mathcal{P}$ in $(\mathcal{O}/\xi\mathcal{O})_r^\times$ for the orbits of this action a *ξ-primary class set* for $\mathcal{O}$. It turns out that if one is able to find a ξ-primary class set for an Eichler order $\mathcal{O}$ with $h(D, N) = 1$, then it is possible to have a unique factorisation result in $\mathcal{O}$, as we will show in Theorem 6.3.4.

A particularly interesting situation appears when $2 \in \xi\mathcal{O}$ and $\#\mathcal{P} = 1$. In this case, we will see that there is a one-to-one correspondence between $(\mathcal{O}/\xi\mathcal{O})_r^\times$ and $\mathcal{O}^\times/\mathbb{Z}^\times$, and this is what allows us to compute generators for the Schottky groups arising from the p-adic uniformisation of Shimura curves coming from these orders. We list in Table 6.1 all the definite Eichler orders (up to conjugation) for which such an element ξ exists.

Finally in section 6.3 we state and prove the *Zerlegungssatz*, a unique factorisation result for Eichler orders with $h(D, N) = 1$ and such that there exists an element $\xi \in \mathcal{O}$ such that group $\mathcal{O}/\xi\mathcal{O}$ contains a ξ-primary class set.

6.1 Arithmetic of quaternion algebras

In this section we introduce the basic notions regarding the arithmetic of quaternion algebras that we need for the rest of the chapter.

A *quaternion algebra* over a number field K is central simple algebra which has dimension 4 over K. A quaternion algebra H with basis $\{1, i, j, k\}$ will be denoted by $H = \left(\frac{a,b}{K}\right)$ with $a, b \in K^\times$ such that

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

Every quaternion algebra over K is provided with a K-endomorphism, which is an involution, called *conjugation*:

$$h = x + yi + zj + tk \quad \mapsto \quad \overline{h} = x - yi - zj - tk.$$

The *reduced trace* and the *reduced norm* of a quaternion are given by

$$\mathrm{Tr}(x + yi + zj + tk) = h + \overline{h} = 2x \quad \text{and} \quad \mathrm{Nm}(x + yi + zj + tk) = h\overline{h} = x^2 - ay^2 - bz^2 + abt^2.$$

A quaternion $h \in H$ is said to be *pure* if $\mathrm{Tr}(h) = 0$.

For each place p of K, let K_p denote its completion at p. Then $H_p := H \otimes K_p$ is a quaternion K_p-algebra. If H_p is a division algebra (a skew field), then H is said to be *ramified at* p. Otherwise, if H_p is the matrix algebra over K_p, then H is said to be *non-ramified* or *split at* p. Let $\mathcal{O}_K$ and $\mathcal{O}_{K_p}$ denote the ring of integers of K and K_p, respectively. The *reduced discriminant* D_H of H is the integral ideal of $\mathcal{O}_K$ equal to the product of all prime ideals of $\mathcal{O}_K$ that ramify in H.

We will work over $\mathbb{Q}$ from now on. Let H be a definite quaternion algebra over $\mathbb{Q}$ and fix a place ℓ of $\mathbb{Q}$. A $\mathbb{Z}[1/\ell]$-*ideal* $\mathfrak{a}$ of H is a $\mathbb{Z}[1/\ell]$-module of rank 4. An *order* $\mathcal{O}$ over $\mathbb{Z}[1/\ell]$ in H is a $\mathbb{Z}[1/\ell]$-ideal that is also a ring; equivalently, it is a ring whose elements are integral, contains $\mathbb{Z}[1/\ell]$ and $\mathbb{Q} \otimes_{\mathbb{R}} \mathcal{O} = H$. An *Eichler order* in H is the intersection of two maximal orders over $\mathbb{Z}[1/\ell]$.

Let H be a definite quaternion algebra over $\mathbb{Q}$ of discriminant D and let $\mathcal{O} \subset H$ denote an Eichler order over $\mathbb{Z}$ of level N. Fix a a place ℓ of $\mathbb{Q}$ and let $\mathcal{O}[1/\ell] := \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}[1/\ell]$ denote the corresponding order over $\mathbb{Z}[1/\ell]$. In particular note that, when $\ell = \infty$, then $\mathbb{Z}[1/\ell] = \mathbb{Z}$. Let $\mathfrak{a} \subseteq H$ be a $\mathbb{Z}[1/\ell]$-ideal. We denote by

$$\mathcal{O}_l(\mathfrak{a}) := \{\alpha \in H \mid \alpha\mathfrak{a} \subseteq \mathfrak{a}\} \quad \text{and} \quad \mathcal{O}_r(\mathfrak{a}) := \{\alpha \in H \mid \mathfrak{a}\alpha \subseteq \mathfrak{a}\}$$

its left and right orders, respectively. These are clearly orders over $\mathbb{Z}[1/\ell]$. Then $\mathfrak{a}$ is said to be a *left ideal* of $\mathcal{O}_l(\mathfrak{a})$ and a *right ideal* of $\mathcal{O}_r(\mathfrak{a})$. Moreover we can also say that $\mathfrak{a}$ is a *one-sided* ideal of $\mathcal{O}_l(\mathfrak{a})$ and a one-sided ideal of $\mathcal{O}_r(\mathfrak{a})$, without specifying the side by which the multiplication is stable. The one-sided ideal $\mathfrak{a}$ is said to be an *integral ideal* if it is contained both in $\mathcal{O}_l(\mathfrak{a})$ and $\mathcal{O}_r(\mathfrak{a})$, and is said to be a *two-sided ideal* if $\mathcal{O}_l(\mathfrak{a}) = \mathcal{O}_r(\mathfrak{a})$. Finally, we say that $\mathfrak{a}$ is a *principal ideal* if there exists $\alpha \in H$ such that $\mathfrak{a} = \mathcal{O}_l(\mathfrak{a})\alpha = \alpha\mathcal{O}_r(\mathfrak{a})$.

Two $\mathbb{Z}[1/\ell]$-ideals $\mathfrak{a}, \mathfrak{b}$ of H are equivalent on the left (resp. on the right) if there exists $\alpha \in H^\times$ such that $\mathfrak{a} = \alpha\mathfrak{b}$ (resp. $\mathfrak{a} = \mathfrak{b}\alpha$). It is immediate to see that if two $\mathbb{Z}[1/\ell]$-ideals $\mathfrak{a}, \mathfrak{b}$ are equivalent on the left, then they have the same right order $\mathcal{O}[1/\ell]$, and the set of classes of right ideals of $\mathcal{O}[1/\ell]$, with respect to this equivalence relation, is called the *set of right ideal classes* of the order $\mathcal{O}[1/\ell]$. Analogously, we can define the *set of left ideal classes* of the order $\mathcal{O}[1/\ell]$. The set of left

ideal classes and that of right ideal classes are in bijection, and the associated cardinality is called the *one-sided ideal class number* of the order $\mathcal{O}[1/\ell]$. Moreover this class number does not depend on the conjugacy class of the Eichler order $\mathcal{O}[1/\ell]$ inside H, and so it is denoted by $h(D,N)$.

Note that, even if the notation we used for it depends only on D and N, the number $h(D,N)$ of $\mathcal{O}[1/\ell]$ also depends on the base ring $\mathbb{Z}[1/\ell]$. Actually, when the order $\mathcal{O}[1/\ell]$ satisfies Eichler's condition (i.e. when the algebra H is not ramified at ℓ), then, by the strong approximation Theorem, this number is equal to the strict ideal class number of $\mathbb{Q}$, that is $h(D,N)=1$ (cf. [Eic38a]). On the other side, when $\mathcal{O}[1/\ell]$ does not satisfy Eichler's condition (which is the case, for example, for $\ell=\infty$, since the algebra H is supposed to be definite), then there is a different formula to compute the number $h(D,N)$ (cf. [Eic38b] for the case $N=1$).

6.2 The ξ-primary quaternions and the right-unit property

In this section we see how the notion of ξ-primary quaternion, as well as the right-unit property, arise naturally in this context, and how they become indispensable for the next chapters.

Let $\mathfrak{a}\subseteq\mathcal{O}$ be an integral right-sided ideal (resp. left-sided) of $\mathcal{O}$, and let $(a):=\mathfrak{a}\cap\mathbb{Z}$. Then the quotient $\mathcal{O}/\mathfrak{a}$ is a finitely generated right-module (resp. left-module) over the ring $\mathbb{Z}/a\mathbb{Z}$. For $\alpha,\beta\in\mathcal{O}$, the quaternion α is said to be *congruent to β modulo* $\mathfrak{a}$, and one writes $\alpha\equiv\beta \bmod \mathfrak{a}$, if $\alpha-\beta\in\mathfrak{a}$. In particular, if $\mathfrak{a}$ is a two-sided integral ideal of $\mathcal{O}$, then $\mathcal{O}/\mathfrak{a}$ is a (possibly) non-commutative ring, which is called the *ring of quaternion classes modulo* $\mathfrak{a}$.

Notation 6.2.1. Let $\mathfrak{a}=\gamma\mathcal{O}$ be an integral ideal and consider the natural projection

$$\lambda_r : \mathcal{O}/\mathrm{Nm}(\gamma)\mathcal{O} \twoheadrightarrow \mathcal{O}/\gamma\mathcal{O}.$$

We will denote by $(\mathcal{O}/\gamma\mathcal{O})_r^\times$ the image of $(\mathcal{O}/\mathrm{Nm}(\gamma)\mathcal{O})^\times$ under the map λ_r. Analogously, if $\mathfrak{a}=\mathcal{O}\gamma$, we denote by λ_ℓ the associated projection and $(\mathcal{O}/\mathcal{O}\gamma)_\ell^\times := \mathrm{Im}(\lambda_\ell)$.

Remark 6.2.2. Note that when $\gamma=m\in\mathbb{Z}$, then $m\mathcal{O}=\mathcal{O}m$, and the set $(\mathcal{O}/m\mathcal{O})_r^\times=(\mathcal{O}/\mathcal{O}m)_\ell^\times$ coincides with the group of units $(\mathcal{O}/m\mathcal{O})^\times$ of the quotient ring $\mathcal{O}/m\mathcal{O}$, since the projection of rings $\lambda:\mathcal{O}/m^2\mathcal{O}\to\mathcal{O}/m\mathcal{O}$ restricts to a projection on the associated unit groups.

If we take an integral basis $\{1,\theta_1,\theta_2,\theta_3\}$ for $\mathcal{O}$ over $\mathbb{Z}$ we can see that the ring

$$\mathcal{O}/m\mathcal{O}=\{[\alpha]=a_0+a_1\theta_1+a_2\theta_2+a_3\theta_3 \mid a_i\in\mathbb{Z}/m\mathbb{Z}\}$$

is a $\mathbb{Z}/m\mathbb{Z}$-module of rank 4, and its group of units is

$$(\mathcal{O}/m\mathcal{O})^\times=\{[\alpha]\in\mathcal{O}/m\mathcal{O} \mid (\mathrm{Nm}(\alpha),m)=1\}.$$

In particular, if m is not divisible by any ramified prime, then one has that $\mathcal{O}/m\mathcal{O}\simeq \mathrm{M}_2(\mathbb{Z}/m\mathbb{Z})$ and $(\mathcal{O}/m\mathcal{O})^\times\simeq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$.

Let $\xi\in\mathcal{O}$. The group $\mathcal{O}^\times$ acts on $(\mathcal{O}/\xi\mathcal{O})_r^\times$ by right-multiplication: take $\alpha+\xi\mathcal{O}\in(\mathcal{O}/\xi\mathcal{O})_r^\times$ and $\varepsilon\in\mathcal{O}^\times$. Then we define

$$(\alpha+\xi\mathcal{O})\varepsilon := \alpha\varepsilon+\xi\mathcal{O}=\lambda_r(\alpha\varepsilon+\mathrm{Nm}(\xi)\mathcal{O})\in(\mathcal{O}/\xi\mathcal{O})_r^\times.$$

Two elements $\alpha+\xi\mathcal{O}$ and $\beta+\xi\mathcal{O}$ are equivalent if there exists $\varepsilon \in \mathcal{O}^\times$ such that $(\alpha+\xi\mathcal{O})\varepsilon = \beta+\xi\mathcal{O}$, and we denote by $[\alpha]$ the class of $\alpha + \xi\mathcal{O}$.

The following definition of ξ-*primary quaternion* generalises the one of Hurwitz [Hur96] for a maximal order over $\mathbb{Z}$ inside the definite quaternion algebra of discriminant 2. In what follows, we take $\mathcal{O} = \mathcal{O}_H(N) \subseteq H$ to be an Eichler order over $\mathbb{Z}$ of level N, with $h(D, N) = 1$.

Definition 6.2.3. Take a quaternion $\xi \in \mathcal{O}$, and let $\mathcal{P} = \{[\alpha_1], \ldots, [\alpha_r]\} \subseteq (\mathcal{O}/\xi\mathcal{O})_r^\times$ be a system of representatives of $(\mathcal{O}/\xi\mathcal{O})_r^\times$ for the right-multiplication action given by $\mathcal{O}^\times$. Suppose that:

(*i*) $\mathcal{O}^\times$ acts freely on $(\mathcal{O}/\xi\mathcal{O})_r^\times$ if $2 \notin \xi\mathcal{O}$,

(*ii*) $\mathcal{O}^\times/\mathbb{Z}^\times$ acts freely on $(\mathcal{O}/\xi\mathcal{O})_r^\times$ if $2 \in \xi\mathcal{O}$.

Then we call $\mathcal{P}$ a ξ-*primary class set* for $\mathcal{O}$. A quaternion α that belongs to some class in $\mathcal{P}$ is called a ξ-*primary* quaternion with respect to $\mathcal{P}$.

Remark 6.2.4. Assume that $\mathcal{O}$ admits a ξ-primary class set $\mathcal{P} = \{[\alpha_1], \ldots, [\alpha_r]\}$ and take $\alpha \in \mathcal{O}$ such that $[\alpha] = \alpha + \xi\mathcal{O} \in (\mathcal{O}/\xi\mathcal{O})_r^\times$. Then there exists a unique $i \in \{1, \ldots, r\}$ and a unit $\varepsilon \in \mathcal{O}^\times$ such that $[\alpha]\varepsilon = [\alpha_i] \in \mathcal{P}$. Moreover, if $2 \notin \xi\mathcal{O}$, then ε is unique, and if $2 \in \xi\mathcal{O}$, then ε is unique up to sign.

Note that, if in particular $\mathcal{P} = \{[1]\} \subseteq \mathcal{O}/\xi\mathcal{O}$ is a ξ-primary class set for $\mathcal{O}$, then α is ξ-primary with respect to $\{[1]\}$ if and only if $\alpha \equiv 1 \bmod \xi\mathcal{O}$.

The notion of ξ-primary quaternions turns out to be very important if we want to have unique factorisation in definite quaternion orders. It is an interesting open problem to find ξ-primary class sets in a given definite quaternion order with one-sided ideal class number 1. In [Hur96] Hurwitz takes $\xi = 2(1 + i)$ and shows that the (maximal) order of Hurwitz quaternions $\mathcal{O}$ in the definite quaternion algebra of discriminant $D = 2$ admits the $2(1 + i)$-primary class set $\{[1], [1 + 2\rho]\} \subseteq (\mathcal{O}/2(1 + i)\mathcal{O})^\times$ for $\mathcal{O}$. Using this, he proves a unique factorisation result or *Zerlegungssatz* for elements in this Eichler order. Our next goal is to extend the *Zerlegungssatz* of Hurwitz to all definite quaternion orders with $h(D, N) = 1$. Moreover, as we shall see in the next section, we will find a ξ-primary class set for most of these orders.

Definition 6.2.5. Let us take $\xi \in \mathcal{O}$. We say that ξ satisfies the *right-unit property* in $\mathcal{O}$ if the following is satisfied:

(*i*) the map $\varphi : \mathcal{O}^\times \to (\mathcal{O}/\xi\mathcal{O})_r^\times,\ u \mapsto \lambda_r(u + \mathrm{Nm}(\xi)\mathcal{O})$, is a bijection if $2 \notin \xi\mathcal{O}$.

(*ii*) the map $\varphi : \mathcal{O}^\times/\mathbb{Z}^\times \to (\mathcal{O}/\xi\mathcal{O})_r^\times,\ u \mapsto \lambda_r(u + \mathrm{Nm}(\xi)\mathcal{O})$, is a bijection if $2 \in \xi\mathcal{O}$.

Remark 6.2.6. In the second case we have that either $\xi\mathcal{O} = 2\mathcal{O}$, or $\mathrm{Nm}(\xi) = 2$ or $\mathrm{Nm}(\xi) = 1$, so in particular the surjection λ_r is either $\mathcal{O}/4\mathcal{O} \twoheadrightarrow \mathcal{O}/2\mathcal{O}$ or $\mathcal{O}/2\mathcal{O} \twoheadrightarrow \mathcal{O}/\xi\mathcal{O}$ or $\mathcal{O} \twoheadrightarrow \{1\}$.

Remark 6.2.7. If $\xi \in \mathcal{O}$ satisfies the right-unit property in $\mathcal{O}$, then the bijection of the definition induces a multiplicative group structure on the set $(\mathcal{O}/\xi\mathcal{O})_r^\times = \mathrm{Im}(\lambda_r)$.

When $\xi\mathcal{O}$ is a two-sided integral principal ideal, then the map $\lambda_r = \lambda_\ell$ is an epimorphism of rings and $(\mathcal{O}/\xi\mathcal{O})^\times$ is the unit group of the ring $\mathcal{O}/\xi\mathcal{O}$. In the next lemma we show how, in this case, one can relate $(\mathcal{O}/\xi\mathcal{O})_r^\times$ and $(\mathcal{O}/\xi\mathcal{O})^\times$.

Lemma 6.2.8. *Take a two-sided integral principal ideal $\xi\mathcal{O}$ such that the map $\varphi : \mathcal{O}^\times \to (\mathcal{O}/\xi\mathcal{O})^\times$ (resp. $\mathcal{O}^\times/\mathbb{Z}^\times \to (\mathcal{O}/\xi\mathcal{O})^\times$), $\varphi(u) = [u]$ is a well defined group isomorphism if $2 \notin \xi\mathcal{O}$ (resp. if $2 \in \xi\mathcal{O}$). Then $(\mathcal{O}/\xi\mathcal{O})_r^\times = (\mathcal{O}/\xi\mathcal{O})^\times$ and ξ satisfies the right-unit property in $\mathcal{O}$.*

Proof. If $\xi = m \in \mathbb{Z}$ the result is clear (cf. Remark 6.2.2). Suppose that $\xi \notin \mathbb{Z}$ with $\mathrm{Nm}(\xi) = m$, and consider the natural projection of rings $\lambda_r : \mathcal{O}/m\mathcal{O} \twoheadrightarrow \mathcal{O}/\xi\mathcal{O}$, $\alpha + m\mathcal{O} \mapsto \alpha + \xi\mathcal{O}$ which restricts to the unit group, since $m\mathcal{O} \subseteq \xi\mathcal{O}$, so $\mathrm{Im}(\lambda_r) = (\mathcal{O}/\xi\mathcal{O})_r^\times \subseteq (\mathcal{O}/\xi\mathcal{O})^\times$. We want to see that this restriction is still surjective. By assumption, if $2 \notin \xi\mathcal{O}$ (resp. if $2 \in \xi\mathcal{O}$) we have the group isomorphism

$$\varphi : \mathcal{O}^\times \to (\mathcal{O}/\xi\mathcal{O})^\times \quad (\text{resp. } \mathcal{O}^\times/\mathbb{Z}^\times \to (\mathcal{O}/\xi\mathcal{O})^\times) \quad \varphi(u) = [u].$$

Take $[\alpha] \in (\mathcal{O}/\xi\mathcal{O})^\times$. Then there exists $u \in \mathcal{O}^\times$ (resp. $\mathcal{O}^\times/\mathbb{Z}^\times$) such that $\varphi(u) = [u] = [\alpha]$. Moreover, since $\mathrm{Nm}(u) = 1$, we have that $u + m\mathcal{O} \in (\mathcal{O}/m\mathcal{O})^\times$ (cf. Remark 6.2.2), and $\lambda_r(u + m\mathcal{O}) := u+\xi\mathcal{O} = \alpha+\xi\mathcal{O} = [\alpha]$, so $(\mathcal{O}/\xi\mathcal{O})_r^\times = (\mathcal{O}/\xi\mathcal{O})^\times$, and consequently, ξ-satisfies the right-unit property in $\mathcal{O}$. □

Lemma 6.2.9. *Let us take $\xi \in \mathcal{O}$. Then $\mathcal{P} = \{[1]\}$ is a ξ-primary class set for $\mathcal{O}$ if and only if ξ satisfies the right-unit property.*

Proof. We have $\#\mathcal{P} = \#(\mathcal{O}/\xi\mathcal{O})_r^\times/\#\mathcal{O}^\times$ if $2 \notin \xi\mathcal{O}$ and $\#\mathcal{P} = \#(\mathcal{O}/\xi\mathcal{O})_r^\times/\#(\mathcal{O}^\times/\mathbb{Z}^\times)$ otherwise. □

Remark 6.2.10. The right-unit property of Definition 6.2.5 turns out to be a very important and powerful condition, as we will see in what follows. We will be particularly interested in integral ideals $\xi\mathcal{O}$ such that $2 \in \xi\mathcal{O}$, because those are the ones that will be useful to us in Section 3. In this case will see that this is also a *natural* property, since we are able to find such quaternions with the right-unit property in all definite Eichler orders over $\mathbb{Z}$ with one-sided ideal class number 1 (except for two cases, for which such ξ does not exist).

In Table 6.1 we list all definite Eichler orders $\mathcal{O} \subseteq H$ of level N (up to conjugation) with $h(D, N) = 1$ that have an element $\xi \in \mathcal{O}$ satisfying the right-unit property and such that $2 \in \xi\mathcal{O}$. This list coincides with that of all definite Eichler orders over $\mathbb{Z}$ with $h(D, N) = 1$, except for the values $(D, N) = (2, 5)$ and $(7, 1)$ (cf. [KV10, Table 8.2]). In order to do this, we first need to fix a basis for the definite quaternion algebra H containing each order, as well as an integral basis for each order, and then express the element ξ in this basis. Note that, although the quaternion ξ is not unique, the existence of such a ξ does not depend on the integral basis chosen for $\mathcal{O}$.

6.3 The *Zerlegungssatz*

The aim of this section is to prove Theorem 6.3.4, a unique factorisation result that relies on the notion of ξ-primary quaternions introduced in section 6.2.

Definition 6.3.1. Let $\{1, \theta_1, \theta_2, \theta_3\}$ be an integral basis of $\mathcal{O}$. A quaternion $\alpha = a_0 + a_1\theta_1 + a_2\theta_2 + a_3\theta_3 \in \mathcal{O}$ is *primitive* if the ideal generated by its coordinates, $(a_0, a_1, a_2, a_3) \subseteq \mathbb{Z}$, is the entire ring $\mathbb{Z}$. Note that this definition does not depend on the chosen integral basis. A nonzero quaternion $\pi \in \mathcal{O} \setminus \mathcal{O}^\times$ is *irreducible* if, whenever $\pi = \alpha\beta$, then either $\alpha \in \mathcal{O}^\times$ or $\beta \in \mathcal{O}^\times$.

D	H	N	$\mathcal{O}$	$\#(\mathcal{O}^\times/\mathbb{Z}^\times)$	ξ	$\mathrm{Nm}(\xi)$
2	$\left(\frac{-1,-1}{\mathbb{Q}}\right)$	1	$\mathbb{Z}\left[1, i, j, \frac{1}{2}(1+i+j+k)\right]$	12	2	4
		3	$\mathbb{Z}\left[1, 3i, -2i+j, \frac{1}{2}(1-i+j+k)\right]$	3	$(-i+k)$	2
		9	$\mathbb{Z}\left[1, 9i, -4i+j, \frac{1}{2}(1-3i+j+k)\right]$	1	1	1
		11	$\mathbb{Z}\left[1, 11i, -10i+j, \frac{1}{2}(1-3i+j+k)\right]$	1	1	1
3	$\left(\frac{-1,-3}{\mathbb{Q}}\right)$	1	$\mathbb{Z}\left[1, i, \frac{1}{2}(i+j), \frac{1}{2}(1+k)\right]$	6	2	4
		2	$\mathbb{Z}\left[1, 2i, \frac{1}{2}(-i+j), \frac{1}{2}-i+\frac{1}{2}k\right]$	2	$\frac{1}{2}(-1-i-j+k)$	2
		4	$\mathbb{Z}\left[1, 4i, \frac{1}{2}(-5i+j), \frac{1}{2}-3i+\frac{1}{2}k\right]$	1	1	1
5	$\left(\frac{-2,-5}{\mathbb{Q}}\right)$	1	$\mathbb{Z}\left[1, \frac{1}{2}(1+i+j), j, \frac{1}{4}(2+i+k)\right]$	3	$\frac{1}{2}(-1+i-j)$	2
		2	$\mathbb{Z}\left[1, 1+i+j, \frac{1}{2}(-1-i+j), \frac{1}{4}(-i-2j+k)\right]$	1	1	1
13	$\left(\frac{-2,-13}{\mathbb{Q}}\right)$	1	$\mathbb{Z}\left[1, \frac{1}{2}(1+i+j), j, \frac{1}{4}(2+i+k)\right]$	1	1	1

Table 6.1: Definite Eichler orders $\mathcal{O}$ with an element $\xi \in \mathcal{O}$ satisfying the right-unit property.

In total analogy to the number fields situation, one can easily prove the following statement characterising irreducible quaternions (cf. also [Hur96]).

Lemma 6.3.2. *Let $\mathcal{O} \subseteq H$ be an Eichler order of level N with $h(D,N) = 1$. A primitive quaternion $\pi \in \mathcal{O}$ is irreducible if and only if its norm is a prime integer.*

Proof. If $\mathrm{Nm}(\pi)$ is prime then it is obvious that π has to be irreducible. Reciprocally, let us assume the $\pi \in \mathcal{O}$ is irreducible and that $p \mid \mathrm{Nm}(\pi)$ is a prime factor of the norm. We are going to show that, when π is primitive, we have strict inclusions

$$p\mathcal{O} \subsetneq p\mathcal{O} + \pi\mathcal{O} \subsetneq \mathcal{O}.$$

If the first inclusion were an equality, then $p \mid \pi$ and, since π is irreducible, $p \in \mathcal{O}^\times$ or $\pi\mathcal{O} = p\mathcal{O}$. Both options lead to a contradiction, since p is prime (of norm $\mathrm{Nm}(p) = p^2$) and π is assumed to be primitive. If the second inclusion were an equality then it is an easy computation to see that $p \mid \mathrm{Nm}(x)$, for every $x \in p\mathcal{O} + \pi\mathcal{O} = \mathcal{O}$, a contradiction. Since the order $\mathcal{O}$ has one-sided ideal class number equal to 1, then $p\mathcal{O} + \pi\mathcal{O} = \alpha\mathcal{O}$, for some $\alpha \in \mathcal{O} \setminus \mathcal{O}^\times$ and then $\pi = \alpha\beta$ for some $\beta \in \mathcal{O}$. Moreover $\beta \in \mathcal{O}^\times$ since π is irreducible. Hence $p \in p\mathcal{O} + \pi\mathcal{O} = \alpha\mathcal{O} = \pi\mathcal{O}$, i.e., $\pi \mid p$ and $\mathrm{Nm}(\pi) \mid \mathrm{Nm}(p) = p^2$. Since π is irreducible its norm $\mathrm{Nm}(\pi)$ cannot be equal to 1 and, since π is primitive, cannot be $\mathrm{Nm}(\pi) = p^2$ either. Actually $\mathrm{Nm}(\pi) = p^2$ implies $p = \pi\varepsilon$ for a unit $\varepsilon \in \mathcal{O}^\times$ and so $\pi = p\varepsilon^{-1}$. Finally the only possible option is $\mathrm{Nm}(\pi) = p$. □

Lemma 6.3.3. *Let $\mathcal{O}$ be an Eichler order with $h(D,N) = 1$, and take $\alpha, \beta, \gamma \in \mathcal{O}$, where $\mathrm{Nm}(\beta) = p$ is prime. If $p \mid \alpha\beta\gamma$ and $p \nmid \alpha\beta$, then $p \mid \beta\gamma$.*

Proof. Consider the ideal $\overline{\beta}\mathcal{O} + \gamma\mathcal{O} = \delta\mathcal{O}$, which is principal by assumption. Then $\mathrm{Nm}(\delta)$ divides $\mathrm{Nm}(\overline{\beta}) = p$, which gives $\mathrm{Nm}(\delta) = 1$ or p. If $\mathrm{Nm}(\delta) = 1$ then $\delta \in \mathcal{O}^\times$, so there exist $x, y \in \mathcal{O}$ such that $1 = \overline{\beta}x + \gamma y$. This implies that $\alpha\beta = \alpha\beta(\overline{\beta}x + \gamma y) = \alpha\beta\overline{\beta}x + \alpha\beta\gamma y = \alpha p x + \alpha\beta\gamma y$, so $p \mid \alpha\beta$, which is a contradiction. Thus $\delta = \overline{\beta}\varepsilon$, for some $\varepsilon \in \mathcal{O}^\times$. Since $\delta\mathcal{O} = \overline{\beta}\mathcal{O} + \gamma\mathcal{O}$, this gives that $\gamma = \overline{\beta}z$, for some $z \in \mathcal{O}$. Finally, we obtain that $p \mid \beta\overline{\beta}z = \beta\gamma$. □

Theorem 6.3.4 (Zerlegungssatz)**.** *Let H be a definite quaternion algebra of discriminant D and let $\mathcal{O}$ be an Eichler order over $\mathbb{Z}$ of level N with $h(D, N) = 1$. Let $\xi \in \mathcal{O}$ be an integral quaternion such that $\mathcal{O}/\xi\mathcal{O}$ contains a ξ-primary class set $\mathcal{P}$.*

Let us take $\alpha \in \mathcal{O}$ a primitive and ξ-primary quaternion with respect to $\mathcal{P}$ such that its norm has a decomposition in prime factors

$$\mathrm{Nm}(\alpha) = p_1 \cdot \ldots \cdot p_s.$$

Then α admits a decomposition in primitive irreducible and ξ-primary quaternions with respect to $\mathcal{P}$:

$$\alpha = \pi_1 \cdot \ldots \cdot \pi_s$$

with $\mathrm{Nm}(\pi_i) = p_i$, for every $1 \leq i \leq s$. Moreover, if $2 \notin \xi\mathcal{O}$ this decomposition is unique, and if $2 \in \xi\mathcal{O}$, the decomposition is unique up to sign.

Proof. First consider the integral right ideal $p_1\mathcal{O} + \alpha\mathcal{O} \subseteq \mathcal{O}$ of $\mathcal{O}$, which is principal by assumption, so $p_1\mathcal{O} + \alpha\mathcal{O} = \pi_1\mathcal{O}$, for some $\pi_1 \in \mathcal{O}$ uniquely determined up to right multiplication by a unit. Let us see that π_1 is then irreducible and $\mathrm{Nm}(\pi_1) = p_1$. Since $p_1\mathcal{O} \subseteq \pi_1\mathcal{O}$, we have that $\pi_1 \mid p_1$, and then $\mathrm{Nm}(\pi_1) \mid \mathrm{Nm}(p_1) = p_1^2$. If $\mathrm{Nm}(\pi_1) = 1$, then $p_1\mathcal{O} + \alpha\mathcal{O} = \mathcal{O}$, and since every $x \in p_1\mathcal{O} + \alpha\mathcal{O}$ has norm such that $p_1 \mid \mathrm{Nm}(x)$ one obtains a contradiction. If $\mathrm{Nm}(\pi_1) = p_1^2 = \mathrm{Nm}(p_1)$ then, since we also have $\pi_1 \mid p_1$, we conclude that $\pi_1 = p_1\varepsilon$, for some $\varepsilon \in \mathcal{O}^\times$. But then $p_1\mathcal{O} + \alpha\mathcal{O} = p_1\mathcal{O}$, so $p_1 \mid \alpha$, which contradicts the primitivity of α. Thus we have shown that $\mathrm{Nm}(\pi_1) = p_1$, so it is primitive, and then we know by Lemma 6.3.2 that π_1 is irreducible. Moreover, since by assumption we have a ξ-primary class set $\mathcal{P} \subseteq \mathcal{O}/\xi\mathcal{O}$, there exists a unit $\varepsilon_1 \in \mathcal{O}^\times$ such that $\pi_1\varepsilon_1$ is ξ-primary, and this unit is unique if $2 \notin \xi\mathcal{O}$ and is unique up to sign if $2 \in \xi\mathcal{O}$. Thus we obtain a decomposition $\alpha = \pi_1\varepsilon_1\varepsilon_1^{-1}\alpha_1$, for some $\alpha_1 \in \mathcal{O}$, where $\pi_1\varepsilon_1$ is primitive, ξ-primary and irreducible. Moreover since both α and $\pi_1\varepsilon_1$ are primitive, $\varepsilon_1^{-1}\alpha_1$ is also a primitive quaternion.

Next we apply the same argument to $\varepsilon_1^{-1}\alpha_1 \in \mathcal{O}$, whose norm is $\mathrm{Nm}(\varepsilon_1^{-1}\alpha_1) = p_2 \ldots p_s$, and we obtain $\varepsilon_1^{-1}\alpha_1 = \pi_2\varepsilon_2\varepsilon_2^{-1}\alpha_2$ with $\pi_2\varepsilon_2$ primitive, ξ-primary and irreducible. Iterating the process we find primitive and irreducible quaternions $\pi_1\varepsilon_1, \ldots, \pi_s\varepsilon_s$ in $\mathcal{O}$ with $\mathrm{Nm}(\pi_i) = p_i$, such that $\alpha = \pi_1\varepsilon_1 \ldots \pi_s\varepsilon_s$, and these determine a factorisation of α of the form

$$\alpha = \pi_1\varepsilon_1 \cdot \ldots \cdot \pi_s\varepsilon_s,$$

where $\pi_1\varepsilon_1, \ldots, \pi_s\varepsilon_s$ are primitive and ξ-primary quaternions with $\mathrm{Nm}(\pi_i) = p_i$, and every $\varepsilon_i \in \mathcal{O}^\times$ in the decomposition is uniquely determined by each π_i (up to sign if $2 \in \xi\mathcal{O}$).

Finally, let us see that this factorisation is unique (up to sign if $2 \in \xi\mathcal{O}$). Suppose that we have two factorisations of α in primitive ξ-primary irreducible quaternions:

$$\alpha = \pi_1 \cdot \ldots \cdot \pi_s = \sigma_1 \cdot \ldots \cdot \sigma_s, \quad \text{for } s \geq 2,$$

with $\mathrm{Nm}(\pi_i) = \mathrm{Nm}(\sigma_i) = p_i$, for $1 \leq i \leq s$. Then $\pi_1 \dots \pi_s \overline{\pi}_s = \sigma_1 \dots \sigma_s \overline{\pi}_s$, so $p_s \mid \sigma_1 \dots \sigma_s \overline{\pi}_s = (\sigma_1 \dots \sigma_{s-1})\sigma_s \overline{\pi}_s$. Since we are assuming that α is primitive, $p_s \nmid (\sigma_1 \dots \sigma_{s-1})\sigma_s$. Thus, by Lemma 6.3.3, we have that $p_s \mid \sigma_s \overline{\pi}_s$. Now $\sigma_s \overline{\pi}_s = \varepsilon p_s = \varepsilon \pi_s \overline{\pi}_s$, for some $\varepsilon \in \mathcal{O}$, so $\sigma_s = \varepsilon \pi_s$ and ε is a unit. Since both π_s and σ_s are primitive and ξ-primary, we obtain that $\varepsilon = 1$ if $2 \notin \xi\mathcal{O}$, and $\varepsilon = \pm 1$ otherwise. $\square$

Chapter 7

A method for finding Mumford curves covering Shimura curves

In this chapter we state and prove the main result of the second part of this thesis (Theorem 7.1.5). This result gives a concrete way to find generators for certain Schottky groups which are subgroups of the p-adic quaternion groups uniformising p-adic Shimura curves.

In section 7.1 we describe a method to compute explicitly these generators. The section is divided in three parts. In the first part, using the *Zerlegungssatz* of section 6.3 we prove a unique factorisation result for the elements of the group $\mathcal{O}[1/p]^\times$. This result turns out to be very useful, as we are interested in computing a system of generators for congruence subgroups of the group

$$\Gamma_p := \Phi_p(\mathcal{O}[1/p]^\times)/\mathbb{Z}[1/p]^\times$$

introduced in chapter 5, since these are the groups that one has to consider in the p-adic uniformisation of a Shimura curve of discriminant Dp. Note that here $\mathbb{Z}[1/p]^\times$ is the unit group of the centre of $\mathcal{O}[1/p]^\times$. In the second part, we prove the main theorem, which, under certain assumptions on the Eichler order $\mathcal{O}$, gives a system of generators for the congruence subgroup

$$\Gamma_p(\xi) := \Phi_p(\{\alpha \in \mathcal{O}[1/p]^\times \mid \alpha \equiv 1 \bmod \xi\mathcal{O}\})/\mathbb{Z}[1/p]^\times,$$

where $\Phi_p : H \hookrightarrow \mathrm{M}_2(\mathbb{Q}_p)$ denotes a p-adic matrix immersion. Moreover, we give conditions under which the group $\Gamma_p(\xi)$ is a Schottky group. Finally in the third part we compute the rank of $\Gamma_p(\xi)$ (when this is a Schottky group). This is done in Theorem 7.1.6, a theorem that generalises a fundamental result of [Hur96] concerning the number of representations of a prime number p by certain quadratic forms.

In section 7.2 we describe how to compute good fundamental domains for the Mumford curves associated to the Schottky groups treated previously. The knowledge of explicit generators for these groups is extremely useful, and it allows us to describe the stable reduction-graph of these Mumford curves, which are coverings of p-adic Shimura curves. This is done in Theorem 7.2.2.

7.1 Computation of systems of generators for arithmetic Schottky groups

Let H be a definite quaternion algebra over $\mathbb{Q}$ of discriminant D and let $p \nmid D$ be an odd prime. Let $\mathcal{O} = \mathcal{O}_H(N) \subseteq H$ be an Eichler order of level N coprime with p. Let us denote by $\mathcal{O}[1/p] := \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}[1/p]$ the corresponding Eichler order over $\mathbb{Z}[1/p]$, which is unique up to conjugation, and by $\mathcal{O}[1/p]^\times$ its group of units, which is the group of quaternions in $\mathcal{O}[1/p]$ with norm equal to some integral power of p. Finally, let us denote by $\mathcal{O}[1/p]^\times_+$ the corresponding group of *positive* units, i.e.

$$\mathcal{O}[1/p]^\times_+ := \{\alpha \in \mathcal{O}[1/p]^\times \mid v_p(\mathrm{Nm}(\alpha)) \equiv 0 \bmod 2\}.$$

This is an index 2 subgroup of $\mathcal{O}[1/p]^\times$. A system of representatives for the quotient group $\mathcal{O}[1/p]^\times_+/\mathbb{Z}[1/p]^\times$ is given by the group of quaternions $\alpha \in \mathcal{O}[1/p]^\times$ with norm equal to 1, in analogy with the archimedean case.

7.1.1 Unique factorisation in $\mathcal{O}[1/p]^\times$

In the following result we apply the *Zerlegungssatz*, valid for the Eichler order $\mathcal{O}$ when its one-sided ideal class number is $h(D, N) = 1$, in order to give a certain unique factorisation of the elements in the group $\mathcal{O}[1/p]^\times$.

Theorem 7.1.1. *Assume that $\mathcal{O}$ has one-sided ideal class number $h(D, N) = 1$, and let $\xi \in \mathcal{O}$ be an integral quaternion such that $\mathcal{O}/\xi\mathcal{O}$ contains a primary class set $\mathcal{P}$. Then every $\alpha \in \mathcal{O}[1/p]^\times$ can be decomposed as a product*

$$\alpha = p^n \cdot \prod_{i=1}^{r} \beta_i \cdot \varepsilon,$$

for $\varepsilon \in \mathcal{O}^\times$ unique (up to sign if $2 \in \xi\mathcal{O}$), unique $n \in \mathbb{Z}$ and for unique $\beta_1, \ldots, \beta_r \in \mathcal{O}$ primitive ξ-primary quaternions with respect to $\mathcal{P}$ with $\mathrm{Nm}(\beta_i) = p$, for every $1 \leq i \leq r$, and such that no factor of the form $\beta_i \cdot \beta_{i+1} = p$ appears in the product.

Proof. Let us take $\alpha \in \mathcal{O}[1/p]^\times$. Since the norm maps $\mathcal{O}[1/p]^\times$ into $\mathbb{Z}[1/p]^\times$ and the order $\mathcal{O}$ is definite, then $\mathrm{Nm}(\alpha) = p^s$, for some $s \in \mathbb{Z}$. Let $l \geq 0$ be the smallest non-negative integer such that $p^l\alpha \in \mathcal{O}$. Let $m \geq 1$ be the greatest common divisor of the integral coordinates of $p^l\alpha$ in some integral basis of $\mathcal{O}$, and put $\beta := \frac{p^l\alpha}{m}$. Then $\mathrm{Nm}(\beta) = \frac{p^{2l+s}}{m^2} \in \mathbb{Z}$, so m is a power of p, say $m = p^t$, and $\alpha = p^{t-l}\beta$. Now $\beta \in \mathcal{O}$ is a primitive quaternion with $\mathrm{Nm}(\beta) = p^{2l+s-2t}$, and since by assumption $\mathcal{O}$ contains a ξ-primary class set, there exists a unique $\varepsilon \in \mathcal{O}^\times$ (up to sign if $2 \in \xi\mathcal{O}$) such that $\beta' := \beta\varepsilon^{-1}$ is a primitive and ξ-primary quaternion having the same norm as β. Therefore we can apply Theorem 6.3.4 to β' and obtain the result with $n := t - l$. □

Since $p \nmid D$, we can take a p-adic matrix immersion $\Phi_p : H \hookrightarrow \mathrm{M}_2(\mathbb{Q}_p)$. We now consider the following groups introduced in chapter 5:

$$\Gamma_p := \Phi_p(\mathcal{O}[1/p]^\times)/\mathbb{Z}[1/p]^\times \quad \text{and} \quad \Gamma_{p,+} := \Phi_p(\mathcal{O}[1/p]^\times_+)/\mathbb{Z}[1/p]^\times.$$

These are the important groups arising in the p-adic uniformisation of a Shimura curve of discriminant Dp. We will show that, under certain assumptions on H and $\mathcal{O}$, we can find a Schottky group

$\Gamma^{\mathrm{Sch}} \subseteq \Gamma_p$ together with a finite system of generators for Γ^{Sch}. As predicted by Theorem 5.4.6, we can look for this Schottky group among the *principal congruence subgroups* of Γ_p.

Take $\xi \in \mathcal{O}$ satisfying the right-unit property in $\mathcal{O}$ (cf. Definition 6.2.5). From now on we will assume that $2 \in \xi\mathcal{O}$. We then distinguish two non-trivial cases: either $\xi = 2$ or $\mathrm{Nm}(\xi) = 2$ (cf. Remark 6.2.6). In the first case, we consider the following group homomorphism:

$$\begin{array}{rccc} \pi: & \mathcal{O}[1/p]^\times & \to & (\mathcal{O}/2\mathcal{O})^\times = (\mathcal{O}/2\mathcal{O})_r^\times \\ & \alpha & \mapsto & \alpha + 2\mathcal{O} \end{array}$$

(cf. Remark 6.2.2 for the equality). If $\mathrm{Nm}(\xi) = 2$, we consider the following group homomorphism:

$$\begin{array}{rccccc} \pi: & \mathcal{O}[1/p]^\times & \stackrel{\pi'}{\to} & (\mathcal{O}/2\mathcal{O})^\times & \stackrel{\lambda_r}{\twoheadrightarrow} & (\mathcal{O}/\xi\mathcal{O})_r^\times \\ & \alpha & \mapsto & \alpha + 2\mathcal{O} & \mapsto & \alpha + \xi\mathcal{O}, \end{array}$$

where $(\mathcal{O}/\xi\mathcal{O})_r^\times$ has the structure of multiplicative group induced by the bijection $\mathcal{O}^\times/\mathbb{Z}^\times \simeq (\mathcal{O}/\xi\mathcal{O})_r^\times$ (cf. Remark 6.2.7). Note that, since p is odd, any $\alpha \in \mathcal{O}[1/p]^\times$ has norm $\mathrm{Nm}(\alpha) \equiv 1 \bmod 2$, and the map π is well-defined. Moreover, π factors via $\mathbb{Z}[1/p]^\times$, since $\alpha = \pm p^n\beta$ implies that $\alpha \equiv \beta \bmod 2\mathcal{O}$. This induces the short exact sequence described in the following lemma.

Lemma 7.1.2. *Let $\xi \in \mathcal{O}$ be an integral quaternion satisfying the right-unit property in $\mathcal{O}$ with $2 \in \xi\mathcal{O}$, and let p be an odd prime. Then the map π is surjective and there is a split short exact sequence of groups*

$$1 \to \{\alpha \in \mathcal{O}[1/p]^\times \mid \alpha \equiv 1 \bmod \xi\mathcal{O}\}/\mathbb{Z}[1/p]^\times \to \mathcal{O}[1/p]^\times/\mathbb{Z}[1/p]^\times \stackrel{\pi}{\to} (\mathcal{O}/\xi\mathcal{O})_r^\times \to 1.$$

Proof. Since the order $\mathcal{O}[1/p] \subseteq H$ satisfies Eichler's condition, we can apply the Strong Approximation Theorem (cf. [Vig80, Ch III, Théorème 4.3] and [Rap13, Lemma 1.1]) in order to show that the map π is surjective. Finally, since we have a bijection

$$\varphi : \mathcal{O}^\times/\mathbb{Z}^\times \to (\mathcal{O}/\xi\mathcal{O})_r^\times,\ \varphi(u) = [u],$$

there is a split given by $(\mathcal{O}/\xi\mathcal{O})_r^\times \simeq \mathcal{O}^\times/\mathbb{Z}^\times \hookrightarrow \mathcal{O}[1/p]^\times/\mathbb{Z}[1/p]^\times$. □

For any $\xi \in \mathcal{O}$ satisfying the right-unit property in $\mathcal{O}$ with $2 \in \xi\mathcal{O}$, we define the following congruence subgroups:

$$\widetilde{\Gamma}_p(\xi) := \Phi_p(\{\alpha \in \mathcal{O}[1/p]^\times \mid \alpha \equiv 1 \bmod \xi\mathcal{O}\}) \subseteq \mathrm{GL}_2(\mathbb{Q}_p),$$

$$\Gamma_p(\xi) := \widetilde{\Gamma}_p(\xi)/\mathbb{Z}[1/p]^\times \subseteq \mathrm{PGL}_2(\mathbb{Q}_p).$$

Note that $\Gamma_p(\xi)$ is a normal subgroup of Γ_p of finite index, which can be referred to as the *principal congruence subgroup* of Γ_p of level $\xi\mathcal{O}$.

7.1.2 The main theorem

In what follows we will see that, under certain assumptions, the group $\Gamma_p(\xi)$ is a Schottky group and we will find a finite and free system of generators for it. With this aim, let us define the following finite set:

$$\widetilde{S} := \Phi_p(\{\alpha \in \mathcal{O} \mid \mathrm{Nm}(\alpha) = p, \alpha \equiv 1 \bmod \xi\mathcal{O}\}) \subseteq \widetilde{\Gamma}_p(\xi),$$

and we denote by S the image of $\widetilde{S}$ in $\Gamma_p(\xi)$ under the natural projection $\widetilde{\Gamma}_p(\xi) \twoheadrightarrow \Gamma_p(\xi)$.

Remark 7.1.3. Let us take $\alpha = a_0 + a_1\theta_1 + a_2\theta_2 + a_3\theta_3 \in \mathcal{O}$, where $\{1, \theta_1, \theta_2, \theta_3\}$ is an integral basis of $\mathcal{O}$. Suppose that $\Phi_p(\alpha) \in \widetilde{S}$. Then $\alpha = (a_0, a_1, a_2, a_3) \equiv (1, 0, 0, 0) \bmod \xi\mathcal{O}$, so $-\alpha = (-a_0, -a_1, -a_2, -a_3) \equiv (1, 0, 0, 0) \bmod \xi\mathcal{O}$ and $\overline{\alpha} = (a_0, -a_1, -a_2, -a_3) \equiv (1, 0, 0, 0) \bmod \xi\mathcal{O}$. This is because we are assuming that $2 \in \xi\mathcal{O}$. Thus, if $\Phi_p(\alpha) \in \widetilde{S}$, then $\Phi_p(\pm\alpha), \Phi_p(\pm\overline{\alpha}) \in \widetilde{S}$.

Following the same idea as in [GvdP80, Ch. IX], we start by splitting $\widetilde{S}$ into two disjoint sets depending on the trace of their quaternions, namely

$$\widetilde{S} = \Phi_p(\{\pm\alpha_1, \ldots, \pm\alpha_s, \pm\overline{\alpha}_1, \ldots, \pm\overline{\alpha}_s\}) \cup \Phi_p(\{\pm\beta_1, \ldots, \pm\beta_t\}),$$

where $\pm\alpha_i, \pm\overline{\alpha}_i \in \mathcal{O}$, for $1 \leq i \leq s$, are the *impure* quaternions in $\widetilde{S}$ (i.e. $\mathrm{Tr}(\alpha_i) \neq 0$), and $\pm\beta_j$, for $1 \leq j \leq t$, are the *pure* quaternions in $\widetilde{S}$ (i.e. $\mathrm{Tr}(\beta_i) = 0$). We then have:

$$S = \{[\Phi_p(\alpha_1)], \ldots, [\Phi_p(\alpha_s)], [\Phi_p(\beta_1)], \ldots, [\Phi_p(\beta_t)]\},$$

where $[\Phi_p(\alpha_i)], [\Phi_p(\beta_j)]$ denote the classes of the matrices $\Phi_p(\alpha_i)$, $\Phi_p(\beta_j)$ inside $\mathrm{PGL}_2(\mathbb{Q}_p)$. From now on s and t denote the integers such that $\#\widetilde{S} = 4s + 2t$ and $\#S = s + t$.

Definition 7.1.4. For every odd prime $p \nmid DN$, we define the following integer:

$$t_\xi(p) := \#\{\alpha \in \mathcal{O} \mid \mathrm{Nm}(\alpha) = p,\ \alpha \equiv 1 \bmod \xi\mathcal{O},\ \mathrm{Tr}(\alpha) = 0\}.$$

Therefore, $t_\xi(p) = 0$ if and only if there is no transformation $\gamma \in S$ with $\mathrm{Tr}(\gamma) = 0$. In this case, we will say that p satisfies the *null-trace condition* with respect to $\xi\mathcal{O}$.

Theorem 7.1.5. *Let H be a definite quaternion algebra of discriminant D and let $\mathcal{O} = \mathcal{O}_H(N) \subseteq H$ be an Eichler order of level N with $h(D, N) = 1$. Let $p \nmid DN$ be an odd prime. Consider*

$$S = \{[\Phi_p(\alpha_1)], \ldots, [\Phi_p(\alpha_s)], [\Phi_p(\beta_1)], \ldots, [\Phi_p(\beta_t)]\} \subseteq \mathrm{PGL}_2(\mathbb{Q}_p),$$

where $\alpha_1, \ldots, \alpha_s \in \mathcal{O}$ are the impure quaternions in $\mathcal{O}$ with norm p (up to sign and conjugation) and $\beta_1, \ldots, \beta_t$ are the pure quaternions in $\mathcal{O}$ with norm p (up to sign). Then for every $\xi \in \mathcal{O}$ with $2 \in \xi\mathcal{O}$ that satisfies the right-unit property in $\mathcal{O}$, the principal congruence subgroup $\Gamma_p(\xi)$ has S as a system of generators and the only relations among these are the following ones:

$$[\Phi_p(\beta_i)]^2 = 1, \text{ for } 1 \leq i \leq t.$$

In particular, if p satisfies the null-trace condition with respect to $\xi\mathcal{O}$, then $\Gamma_p(\xi)$ is a Schottky group of rank s.

Proof. On the one hand, the split short exact sequence described in Lemma 7.1.2 gives an isomorphism of groups

$$\Gamma_p \simeq \Gamma_p(\xi) \rtimes (\mathcal{O}/\xi\mathcal{O})_r^\times.$$

On the other hand, since we are in the hypothesis of Lemma 6.2.9 we have that $\mathcal{P} = \{[1]\}$ is a ξ-primary class set for $\mathcal{O}$. By Theorem 7.1.1, every element $\alpha \in \mathcal{O}[1/p]^\times$ can be written uniquely up to sign as $\alpha = p^n \prod_{i=1}^r \beta_i \cdot \varepsilon$, for $n \in \mathbb{Z}$, $\varepsilon \in \mathcal{O}^\times$ and $\beta_1, \ldots, \beta_r \in \mathcal{O}$ primitive ξ-primary quaternions with respect to $\mathcal{P}$ with $\mathrm{Nm}(\beta_i) = p$ and such that no factor of the form $\beta_i \cdot \beta_{i+1} = p$ appears in the product. This gives us the following split short exact sequence:

$$\begin{array}{ccccccccc} 1 & \to & \langle\{\alpha \in \mathcal{O} \mid \mathrm{Nm}(\alpha) = p,\, \alpha \equiv 1 \bmod \xi\mathcal{O}\}\rangle/\mathbb{Z}^\times & \to & \mathcal{O}[1/p]^\times/\mathbb{Z}^\times & \to & \mathcal{O}^\times/\mathbb{Z}^\times & \to & 1, \\ & & & & \alpha & & \varepsilon & & \end{array}$$

since

$$\{\alpha = p^n \prod_{i=1}^r \beta_i \mid \mathrm{Nm}(\beta_i) = p,\, \beta_i \equiv 1 \bmod \xi\mathcal{O}\} = \langle\{\alpha \in \mathcal{O} \mid \mathrm{Nm}(\alpha) = p,\, \alpha \equiv 1 \bmod \xi\mathcal{O}\}\rangle.$$

Hence, we obtain the following semidirect product:

$$\mathcal{O}[1/p]^\times/\mathbb{Z}^\times \simeq \langle\{\alpha \in \mathcal{O} \mid \mathrm{Nm}(\alpha) = p,\, \alpha \equiv 1 \bmod \xi\mathcal{O}\}\rangle/\mathbb{Z}^\times \rtimes \mathcal{O}^\times/\mathbb{Z}^\times.$$

After taking the quotient by its centre we obtain

$$\Gamma_p = \langle S\rangle \rtimes \mathcal{O}^\times/\mathbb{Z}^\times.$$

Since ξ satisfies the right-unit property in $\mathcal{O}$, the natural map $\varphi : \mathcal{O}^\times/\mathbb{Z}^\times \to (\mathcal{O}/\xi\mathcal{O})_r^\times$ is an isomorphism of groups (cf. Definition 6.2.5). Thus the following diagram commutes:

$$\begin{array}{ccccccccc} 1 & \to & \Gamma_p(\xi) & \to & \Gamma_p & \to & \mathcal{O}^\times/\mathbb{Z}^\times & \to & 1 \\ & & \uparrow & & \| & & \wr\downarrow & & \\ 1 & \to & \langle S\rangle & \to & \Gamma_p & \to & (\mathcal{O}/\xi\mathcal{O})_r^\times & \to & 1 \end{array}$$

and we obtain that

$$\Gamma_p(\xi) = \langle S\rangle.$$

With this we have found a finite system of generators for the group $\Gamma_p(\xi)$.

Let us look now at the possible relations among these generators. First of all, observe that $[\Phi_p(\beta_i)]^2 = 1$, for $i = 1, \ldots, t$, are relations in S, because $\beta_i\overline{\beta}_i = -\beta_i^2 = p$, which is a unit in $\mathbb{Z}[1/p]$. We are going to prove that actually these are the only possible relations. Since $\mathrm{Nm}(\alpha_i) = p$ for every $1 \le i \le s$, we observe that if there is a relation among the generators $[\Phi_p(\alpha_i)]$, this must have an even number of elements (since the valuation at p of the determinant of this relation has to be even). Suppose then that we have $[\Phi_p(\alpha_1)] \cdot \ldots \cdot [\Phi_p(\alpha_{2k})] = [1]$, for some positive integer k. This means that $\alpha := \alpha_1 \cdot \ldots \cdot \alpha_{2k} = \pm p^m$, for some $m \ge 1$, and taking norms we find that $m = k$. By Theorem 7.1.1, α has a decomposition, unique up to sign, as a product $\alpha = p^n \cdot \varepsilon \cdot \prod_{i=1}^r \beta_i$, with $n \in \mathbb{Z}$, $\varepsilon \in \mathcal{O}^\times$ and

(a) $\beta_1, \ldots, \beta_r \in \mathcal{O}$ primitive and ξ-primary quaternions with respect to $\mathcal{P} = \{[1]\}$,

(b) $\mathrm{Nm}(\beta_i) = p$,

(c) no factor of the form $\beta_i \cdot \beta_{i+1} = p$ appears in the product.

Since $\alpha = \pm p^k$, by the uniqueness of this decomposition, we cannot have a decomposition $\alpha = \alpha_1 \cdot \ldots \cdot \alpha_{2k}$ with the α_i satisfying conditions (a)-(c) simultaneously. Since α_i already satisfy conditions (a) and (b), this means that there are α_i, α_{i+1} such that $\alpha_i \alpha_{i+1} = p$, so $\alpha_i = \overline{\alpha}_{i+1}$, and this is a contradiction because we already excluded these elements in S. □

7.1.3 The number of generators of $\Gamma_p(\xi)$

Finally, when the group $\Gamma_p(\xi)$ is a Schottky group (i.e. when p satisfies that $t_\xi(p) = 0$), we want to know the rank of this group, that is, we would like to compute the cardinality s. Before showing how to do so, we will introduce some notations.

Once we have fixed a presentation $H = \left(\frac{a,b}{\mathbb{Q}}\right)$ for the quaternion algebra and a basis for the Eichler order $\mathcal{O}$, let $\mathrm{N}_{(a,b),4}(X,Y,Z,T) := X^2 - aY^2 - bZ^2 + abT^2$ denote the quaternary normic form associated to H with respect to the basis $\{1, i, j, ij\}$, and let $\mathrm{N}_{\mathcal{O},4}(X,Y,Z,T)$ denote the quaternary normic form associated to $\mathcal{O}$ with respect to the chosen basis. For every prime p, we consider the number of representations of p by these normic forms:

$$r(\mathrm{N}_{(a,b),4}, p; \mathbb{Z}) := \#\{(x,y,z,t) \in \mathbb{Z}^4 \mid \mathrm{N}_{(a,b),4}(x,y,z,t) = p\},$$

$$r(\mathrm{N}_{\mathcal{O},4}, p; \mathbb{Z}) := \#\{(x,y,z,t) \in \mathbb{Z}^4 \mid \mathrm{N}_{\mathcal{O},4}(x,y,z,t) = p\}.$$

Note that $r(\mathrm{N}_{\mathcal{O},4}, p; \mathbb{Z})$ does not depend on the presentation of the algebra nor on the chosen basis of $\mathcal{O}$ (cf. [AB04] Prop. 3.86), while $r(\mathrm{N}_{(a,b),4}, p; \mathbb{Z})$ does depend on the presentation of H. Given $\xi \in \mathcal{O}$ we also define the following integer:

$$r(\mathrm{N}_{\mathcal{O},4}, p; \xi) := \#\{\alpha \in \mathcal{O} \mid \mathrm{Nm}(\alpha) = p,\ \alpha \equiv 1 \bmod \xi\mathcal{O}\}.$$

Note that, when $\xi = 2$, then

$$r(\mathrm{N}_{\mathcal{O},4}, p; 2) = \#\{(x,y,z,t) \in \mathbb{Z}^4 \mid \mathrm{N}_{\mathcal{O},4}(x,y,z,t) = p,\ (x,y,z,t) \equiv (1,0,0,0) \bmod 2\},$$

and when $\xi = 1$,

$$r(\mathrm{N}_{\mathcal{O},4}, p; 1) = r(\mathrm{N}_{\mathcal{O},4}, p; \mathbb{Z}).$$

The following is a fundamental result concerning the numbers of representations of a prime p by certain quaternary quadratic forms that generalises a result of [Hur96].

Theorem 7.1.6. *Let H be a definite quaternion algebra of discriminant D and let $\mathcal{O} \subseteq H$ be an Eichler order of level N with $h(D,N) = 1$. Let $p \nmid DN$ be a prime, and let $\xi \in \mathcal{O}$ be an integral quaternion such that $\mathcal{O}/\xi\mathcal{O}$ contains a ξ-primary class set. Then the cardinality of the finite set*

$$\{\pi \in \mathcal{O} \mid \mathrm{Nm}(\pi) = p,\ \pi \text{ is } \xi\text{-primary}\}$$

is equal to:

(a) $p + 1$, *when* $2 \notin \xi\mathcal{O}$,

(b) $2(p+1)$, *when* $2 \in \xi\mathcal{O}$.

Proof. Let $c := \#\{\pi \in \mathcal{O} \text{ } \xi\text{-primary} \mid \mathrm{Nm}(\pi) = p\}$. Since $p \nmid DN$ we have an isomorphism of algebras $\mathcal{O}/p\mathcal{O} \simeq \mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$. Therefore the set

$$A_p := \{[\alpha] \in \mathcal{O}/p\mathcal{O} \mid \alpha \notin p\mathcal{O},\ \mathrm{Nm}(\alpha) \equiv 0 \bmod p\}$$

has $(p^2-1)(p+1)$ elements, since

$$\#A_p = \#\mathrm{M}_2(\mathbb{Z}/p\mathbb{Z}) - \#\mathrm{GL}_2(\mathbb{F}_p) - 1 = p^4 - (p^2-1)(p^2-p) - 1 = p^3 + p^2 - p - 1 = (p^2-1)(p+1).$$

We now distinguish two cases depending on whether $2 \in \xi\mathcal{O}$ or not.

(*a*) When $2 \notin \xi\mathcal{O}$, we can define the map

$$\Sigma : A_p \to \{\pi \in \mathcal{O} \mid \mathrm{Nm}(\pi) = p,\ \xi\text{-primary}\},$$

assigning to $[\alpha] \in A_p$ the unique quaternion $\pi_{[\alpha]}$ which is ξ-primary and such that $\alpha\mathcal{O} + p\mathcal{O} = \pi_{[\alpha]}\mathcal{O}$.

(*b*) When $2 \in \xi\mathcal{O}$, the primary quaternion $\pi_{[\alpha]}$ defined above is unique only up to sign, so this same assignment gives a well defined map

$$\Sigma : A_p \to \{\pi \in \mathcal{O} \mid \mathrm{Nm}(\pi) = p,\ \xi\text{-primary}\}/\{\pm 1\},$$

where the quotient by $\{\pm 1\}$ denotes the equivalence relation that identifies π and $-\pi$.

Finally, we will show that:

(*a*) if $2 \notin \xi\mathcal{O}$, then $c = \#A_p/(p^2-1) = p+1$,

(*b*) if $2 \in \xi\mathcal{O}$, then $c = 2(\#A_p/(p^2-1)) = 2(p+1)$.

Indeed, the map Σ is, in both cases, a 1 to p^2-1 correspondence. To prove this, let us see that $\#\Sigma^{-1}(\Sigma([\alpha])) = p^2 - 1$. First we observe that

$$\Sigma^{-1}(\pi_{[\alpha]}) = \{[\alpha]\lambda \in A_p \mid \lambda \in \mathcal{O}/p\mathcal{O}\},$$

and then we find that this set has cardinality

$$\#(\mathcal{O}/p\mathcal{O})/\#\{[x] \in \mathcal{O}/p\mathcal{O} \mid \alpha x \equiv 0 \bmod \xi\mathcal{O}\} - 1 = p^4/p^2 - 1 = p^2 - 1.$$

□

Remark 7.1.7. In particular, when the data $D, N, H, \mathcal{O}$ and $\xi \in \mathcal{O}$ are taken as in Table 6.1 this result says that the number of representations $r(\mathrm{N}_{\mathcal{O},4}, p; \xi)$ is equal to $2(p+1)$.

Corollary 7.1.8. *Let H be a definite quaternion algebra of discriminant D, let $\mathcal{O} = \mathcal{O}_H(N) \subseteq H$ be an Eichler order of level N, and let $p \nmid DN$ be an odd prime. Assume that the following conditions are satisfied:*

(*i*) $h(D, N) = 1$,

(*ii*) *there exists a quaternion $\xi \in \mathcal{O}$ which satisfies the right-unit property in $\mathcal{O}$ with $2 \in \xi\mathcal{O}$ (cf. Table 6.1),*

(*iii*) *the prime p satisfies the null-trace condition with respect to $\xi\mathcal{O}$ (cf. Definition* 7.1.4).

Then $\Gamma_p(\xi)$ is a Schottky group of rank

$$\operatorname{rank}\Gamma_p(\xi) = \frac{p+1}{2}.$$

Proof. After Theorem 7.1.5, since p satisfies the null-trace condition with respect to $\xi\mathcal{O}$, we have that $\Gamma_p(\xi)$ is a Schottky group of rank $\#S = s$. Hence we need to compute $s = \frac{1}{4}r(\mathrm{N}_{\mathcal{O},4}, p; \xi)$ and by Theorem 7.1.6 we find $s = (p+1)/2$. □

7.2 p-adic fundamental domains and their reduction-graphs

In this section we describe how to construct good fundamental domains for Mumford curves uniformised by the Schottky groups of the previous section.

By [Ger74, Satz 1] we know that we can always find a system of generators $S = \{\gamma_1, \dots, \gamma_g\}$ for a Schottky group Γ such that there exists a good fundamental domain for Γ with respect to S (cf. Definition 5.4.4). We also say that such a system of generators is *in good position*. The problem to find generators in good position for a given Schottky group is an important problem, which is computationally solved in [MR15].

In the following proposition we give sufficient conditions for a system of generators of a Schottky group to be in good position. In particular, this applies to the generators arising from Theorem 7.1.5 and it will allow us to describe the stable reduction-graph of Mumford curves covering p-adic Shimura curves.

Proposition 7.2.1. *Let $\Gamma \subseteq \mathrm{PGL}_2(\mathbb{Q}_p)$ be a cocompact Schottky group of rank g, and let $S = \{\gamma_1, \dots, \gamma_g\}$ be a system of generators. Assume that:*

(*a*) *the rank of Γ is $g = (p+1)/2$,*

(*b*) $\det(\gamma_i) = p\mathbb{Q}_p^{\times 2}$ *for every $i = 1, \dots, g$.*

Then a good fundamental domain for the action of Γ with respect to S is

$$\mathbb{P}^1(\mathbb{C}_p) \smallsetminus \left(\bigcup_{a=0}^{p-1} \mathbb{B}^-(a, 1/\sqrt{p}) \cup \mathbb{B}^-(\infty, 1/\sqrt{p}) \right).$$

Proof. For every $i = 1, \dots, g$, let us denote by $\alpha_i, \alpha_{i+g} \in \mathbb{P}^1(\mathbb{Q}_p)$ the two fixed points of the transformations γ_i, γ_i^{-1}, and define the following admissible subdomain of $\mathcal{H}_p$:

$$\mathcal{F}_\Gamma := \mathbb{P}^1(\mathbb{C}_p) \smallsetminus \bigcup_{i=1}^{2g} \mathbb{B}^- \left(\alpha_i, 1/\sqrt{p}\right).$$

Condition (*i*) of Definition 5.4.4 is clearly satisfied, since the transformations γ_i are hyperbolic, so their fixed points are in $\mathbb{P}^1(\mathbb{Q}_p)$. Moreover, since these fixed points by definition satisfy that $\alpha_i = \lim_{n\to\infty}(\gamma_i^n \cdot v^0)$ and $\alpha_{i+g} = \lim_{n\to\infty}(\gamma_i^{-n} \cdot v^0)$, then we find that

$$\gamma_i \cdot e^{(1)}_{\widetilde{\alpha}_i} = -e^{(1)}_{\widetilde{\alpha}_{i+g}},$$

and applying the reduction map of Theorem 5.2.6 we find that condition (iii) of Definition 5.4.4 is satisfied. Therefore we only need to check condition (ii).

So let us suppose that there exist $i, j \in \{1, \dots, (p+1)/2\}, i \neq j$, such that

$$\mathbb{B}^+(\alpha_i, 1/\sqrt{p}) \cap \mathbb{B}^+(\alpha_j, 1/\sqrt{p}) \neq \emptyset.$$

In fact, since these two balls have the same radius we obtain $\mathbb{B}^+(\alpha_i, 1/\sqrt{p}) = \mathbb{B}^+(\alpha_j, 1/\sqrt{p})$. Let $\widetilde{\alpha}_i, \widetilde{\alpha}_j \in \mathbb{P}^1(\mathbb{F}_p)$ be the corresponding reductions mod p of α_i, α_j. Applying the reduction map of Theorem 5.2.6 and the fact that this is equivariant with respect to the action of $\mathrm{PGL}_2(\mathbb{Q}_p)$, we find that

$$\gamma_i \cdot e^{(1)}_{\widetilde{\alpha}_i} = -e^{(1)}_{\widetilde{\alpha}_{i+g}} \text{ and } \gamma_j \cdot e^{(1)}_{\widetilde{\alpha}_j} = -e^{(1)}_{\widetilde{\alpha}_{j+g}}.$$

Therefore $\gamma_i\gamma_j^{-1} \cdot (-e^{(1)}_{\widetilde{\alpha}_{j+g}}) = -e^{(1)}_{\widetilde{\alpha}_{i+g}}$, and the transformation $\gamma_i\gamma_j^{-1}$ fixes a vertex of $\mathcal{T}_p$, which is a contradiction since the group Γ_p is torsion-free.

Finally the subdomain $\mathcal{F}_\Gamma$ is a good fundamental domain for Γ with respect to the system of generators S and, by Lemma 5.1.3 (b), we have that

$$\mathcal{F}_\Gamma = \mathbb{P}^1(\mathbb{C}_p) \smallsetminus \left(\bigcup_{a=0}^{p-1} \mathbb{B}^-(a, 1/\sqrt{p}) \cup \mathbb{B}^-(\infty, 1/\sqrt{p}) \right).$$

□

Theorem 7.2.2. *Let H be a definite quaternion algebra of discriminant D, let $\mathcal{O} = \mathcal{O}_H(N) \subseteq H$ be an Eichler order of level N, and let $p \nmid DN$ be an odd prime. Assume that the following conditions are satisfied:*

- (i) *$h(D, N) = 1$,*
- (ii) *there exists a quaternion $\xi \in \mathcal{O}$ which satisfies the right-unit property in $\mathcal{O}$ with $2 \in \xi\mathcal{O}$,*
- (iii) *the prime p satisfies the null-trace condition with respect to $\xi\mathcal{O}$.*

Then it follows that

- (a) *The group $\Gamma_p(\xi)$ is a Schottky group of rank $(p+1)/2$ generated by the transformations in $\mathrm{PGL}_2(\mathbb{Q}_p)$ represented by the matrices in*

$$\widetilde{S} := \Phi_p(\{\alpha \in \mathcal{O} \mid \mathrm{Nm}(\alpha) = p, \alpha \equiv 1 \bmod \xi\mathcal{O}\}).$$

- (b) *A good fundamental domain for the action of $\Gamma_p(\xi)$ with respect to the system of generators $\widetilde{S}$ is the admissible subdomain of $\mathcal{H}_p$*

$$\mathcal{F}_p(\xi) := \mathbb{P}^{1,rig}(\mathbb{C}_p) \smallsetminus \bigcup_{a \in \{0,\dots,p-1,\infty\}} \mathbb{B}^-(a, 1/\sqrt{p}).$$

- (c) *If $X_p(\xi)$ denotes the Mumford curve associated to $\Gamma_p(\xi)$, then the rigid analytic curve $X_p(\xi)^{rig}$ is obtained from the fundamental domain $\mathcal{F}_p(\xi)$ with the following pair-wise identifications: for every $\gamma \in \widetilde{S}$,*

$$\gamma\left(\mathbb{P}^1(\mathbb{C}_p) \smallsetminus \mathbb{B}^-(\tilde{\alpha}_\gamma, 1/\sqrt{p})\right) = \mathbb{B}^+(\tilde{\alpha}_{\gamma^{-1}}, 1/\sqrt{p}),$$

$$\gamma\left(\mathbb{P}^1(\mathbb{C}_p)\smallsetminus\mathbb{B}^+(\tilde{\alpha}_\gamma,1/\sqrt{p})\right)=\mathbb{B}^-(\tilde{\alpha}_{\gamma^{-1}},1/\sqrt{p}),$$

where $\widetilde{\alpha}_\gamma$ *and* $\widetilde{\alpha}_{\gamma^{-1}}$ *are defined as the reduction in* $\mathbb{P}^1(\mathbb{F}_p)$ *of the fixed points of the transformations* $\{\gamma,\gamma^{-1}\}$.

(*d*) *The stable reduction-graph of* $X_p(\xi)$ *is the quotient of the open subtree* $\mathcal{T}_p^{(1)}\smallsetminus\{v_0^{(1)},\dots,v_{p-1}^{(1)},v_\infty^{(1)}\}$ *of* $\mathcal{T}_p$ *via the pair-wise identifications of the* $p+1$ *oriented edges given by* $\gamma e_{\widetilde{\alpha}_\gamma}=-e_{\widetilde{\alpha}_{\gamma^{-1}}}$, *for every* $\gamma\in\widetilde{S}$.

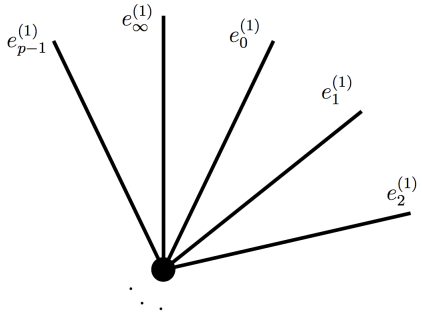


Figure 7.1: Open subtree $\mathcal{T}_p^{(1)}\smallsetminus\{v_0^{(1)},\dots,v_{p-1}^{(1)},v_\infty^{(1)}\}$ of $\mathcal{T}_p$ before pair-wise identification

Proof. After Theorem 7.1.5 we know that $\Gamma_p(\xi)$ is a Schottky group and by Corollary 7.1.8 it has rank $(p+1)/2$. Therefore (a) follows. Now we are in the hypothesis of Proposition 7.2.1 and (*b*) follows. By the theory of Mumford curves recalled in chapter 5, there exists a projective curve $X_p(\xi)$ over $\mathbb{Q}_p$ such that its rigidification is

$$\Gamma_p(\xi)\backslash\mathcal{F}_p(\xi)\simeq\Gamma_p(\xi)\backslash\mathcal{H}_p\simeq X_p(\xi)^{rig},$$

and by the definition of good fundamental domain (cf. Definition 5.4.4 (*iii*)) this gives the identifications of (*c*).

Finally applying the equivariant reduction map of Theorem 5.2.6 we find that the fundamental domain $\mathcal{F}_p(\xi)$ together with its identifications reduce to the rose-graph with $(p+1)/2$ petals, as described in (*d*) (see Figure 7.2). □

Corollary 7.2.3. *Consider the Shimura curve* $X(Dp,N)$ *of discriminant* Dp, *with* $(D,N)=1$ *and* $p\nmid DN$, *associated to an Eichler order of level* N *in the indefinite quaternion algebra of discriminant* Dp. *Let* H *be the definite quaternion algebra of discriminant* D *and let* $\mathcal{O}=\mathcal{O}_H(N)\subset H$ *be an Eichler order of level* N.

If $\mathcal{O}$ *satisfies the conditions of Theorem* 7.2.2, *then there exists a Mumford curve of genus* $(p+1)/2$ *covering the p-adic rigid Shimura curve* $(X(Dp,N)\otimes_{\mathbb{Q}}\mathbb{Q}_p)^{rig}$ *and the degree of the cover is equal to the order of the group* $\mathcal{O}^\times/\mathbb{Z}^\times$.

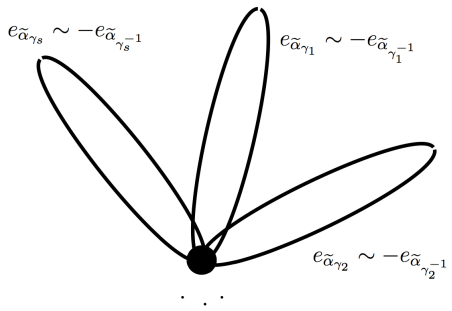


Figure 7.2: Stable reduction-graph of the Mumford curve $X_p(\xi)$

Proof. After applying Theorem 7.1.5 we find a Schottky group $\Gamma_p(\xi)$ which is a normal subgroup of Γ_p of index $\#\Gamma_p/\Gamma_p(\xi) = \#\mathcal{O}^\times/\mathbb{Z}^\times$. Therefore, there exists a rigid analytic curve isomorphic to $\Gamma_p\backslash\mathcal{H}_p$ which is a finite quotient of the rigidification of the Mumford curve $X_p(\xi)$ described in Theorem 7.2.2.

Moreover, by Theorem 5.3.1 we have that $(X(D,N)\otimes_{\mathbb{Q}}\mathbb{Q}_p)^{rig} \simeq \Gamma_p\backslash(\mathcal{H}_p\otimes_{\mathbb{Q}_p}\mathbb{Q}_{p^2})$, so the statement of this corollary follows. □

Remarks 7.2.4 (About the conditions of Theorem 7.2.2)**.**

(1) Condition (*ii*) of Theorem 7.2.2 is satisfied by all the definite Eichler orders $\mathcal{O}_H(N)$ in Table 6.1.

(2) If one wants to do explicit computations, condition (*iii*) of Theorem 7.2.2 is easy to check in each case once p is fixed. Actually, once the finite set of generators for the group $\Gamma_p(\xi)$ is computed, one only needs to check whether any of them has null trace.

(3) Note that when condition (*iii*) of Theorem 7.2.2 is not satisfied, it is still possible to find a Schottky group $\Gamma_p(\xi)^\star \subseteq \Gamma_p(\xi)$, avoiding the 2-torsion, together with an explicit system of generators. This is shown in [GvdP80, Ch. IX] in the case $D = 2, N = 1$ and can be extended to all the cases considered in the present work. Using Magma, we also computed generators for the group $\Gamma_p(\xi)^\star$ for primes $p \leq 2000$ in all the cases of Table 6.1, and checked that its rank is always p. Therefore we would find a Mumford curve of genus p covering the p-adic Shimura curve.

Chapter 8

Application of the method to bad reduction of Shimura curves

As explained in the introduction, in [FM14] the authors develop an algorithm which computes the reduction-graphs with lengths at p of Shimura curves $X(Dp, N)$ associated to any Eichler order of level N contained in an indefinite quaternion algebra of discriminant Dp. Thus this problem is completely solved for all Shimura curves. Nevertheless in this chapter we give general formulas describing the reduction-graphs with lengths for those families of Shimura curves satisfying Corollary 7.2.3, that is, families of Shimura curves $X(Dp, N)$ such that the one-sided ideal class number $h(D, N)$ is equal to 1, except for the families of Shimura curves $X(2p, 5)$ and $X(7p, 1)$ (for which the quaternion ξ required in Theorem 7.2.2 does not exist).

In section 8.1 we show how to recover these formulas, after Theorem 7.2.2, using the explicit knowledge of the Mumford curves covering the p-adic Shimura curves considered. We are led to study the two following coverings:

(i) $\Gamma_p(\xi)\backslash\mathcal{T}_p \twoheadrightarrow \Gamma_p\backslash\mathcal{T}_p$ of degree $\#\mathcal{O}^\times/\mathbb{Z}^\times$.

(ii) $\Gamma_{p,+}\backslash\mathcal{T}_p \twoheadrightarrow \Gamma_p\backslash\mathcal{T}_p$ of degree 2.

The reduction-graph with lengths $\Gamma_p\backslash\mathcal{T}_p$ is, by the way, the reduction-graph of an integral model of the Atkin-Lehner quotient of $X(Dp, N)$ associated to the involution of norm p.

In section 8.2 we see how the methods used so far are also useful to easily obtain genus formulas for these quotients of Shimura curves and for certain Atkin-Lehner quotients. Finally in section 8.3 we show how one can make more explicit some conditions about the generators of the Schottky groups considered before, by exploring what we call the *null-trace* condition.

8.1 Reduction-graphs with lengths

For the definitions of *admissible curve* and *reduction-graph with lengths* we refer the reader to Jordan and Livné's article [JL84]. The Drinfel'd model $\mathcal{X}(Dp, N)$ over $\mathbb{Z}_p$ of the Shimura curve $X(Dp, N)$, as defined in chapter 5, is then an admissible curve, and its reduction-graph $\Gamma_{p,+}\backslash\mathcal{T}_p$ is

a graph with lengths.

We start by giving some basic definitions and results.

Definition 8.1.1. Let $\mathcal{G}$ be a graph and let Γ be a group acting by the left on $\mathcal{G}$. We define the *length* of a vertex $[v] \in \mathrm{Ver}(\Gamma\backslash\mathcal{G})$ (resp. an edge $[e] \in \mathrm{Ed}(\Gamma\backslash\mathcal{G})$) as the cardinality of the stabiliser Γ_v of a representative $v \in \mathrm{Ver}(\mathcal{G})$ (resp. the stabiliser Γ_e of a representative $e \in \mathrm{Ed}(\mathcal{G})$) inside the group Γ. We denote it by $\ell([v])$ (resp. $\ell([e])$).

For every $n \geq 1$, we define the integer

$$c_n := \#\{[e] \in \mathrm{Ed}(\Gamma\backslash\mathcal{G}) \mid \ell([e]) = n\}.$$

Finally, given a graph $\mathcal{G}$ and a vertex $v \in \mathrm{Ver}(\mathcal{G})$, we denote by $\mathrm{Star}(v)$ the subset of oriented edges $e \in \mathrm{Ed}(\mathcal{G})$ with origin in v.

If Γ is a group acting by the left on a graph $\mathcal{G}$, then there is a natural surjective map $\mathrm{Star}(v) \to \mathrm{Star}([v])$. Therefore, applying the orbit-stabiliser theorem, is easy to prove the following lemma.

Lemma 8.1.2. *Let $\mathcal{G}$ be a graph and let Γ be a group acting by the left on $\mathcal{G}$. Take $v \in \mathrm{Ver}(\mathcal{G})$ and $e \in \mathrm{Star}(v)$. Then $\ell([e])$ divides $\ell([v])$ and the following formula holds:*

$$\#\mathrm{Star}(v) = \sum_{[e]\in\mathrm{Star}([v])} \frac{\ell([v])}{\ell([e])}.$$

For the sake of exposition, we fix from now on a presentation of the definite quaternion algebra $H = \left(\frac{a,b}{\mathbb{Q}}\right)$. We shall consider in each case the one considered in Table 6.1. Then for every prime integer p such that $\left(\frac{a}{p}\right) = 1$, we can take the following p-adic matrix immersion

$$\begin{aligned} \Phi_p : \qquad H = \left(\frac{a,b}{\mathbb{Q}}\right) \qquad &\longrightarrow \qquad \mathrm{M}_2(\mathbb{Q}_p(\sqrt{a})) = \mathrm{M}_2(\mathbb{Q}_p) \\ x_0 + x_1 i + x_2 j + x_3 k \quad &\longmapsto \quad \begin{pmatrix} x_0 + x_1\sqrt{a} & x_2 + x_3\sqrt{a} \\ b(x_2 - x_3\sqrt{a}) & x_0 - x_1\sqrt{a} \end{pmatrix}. \end{aligned}$$

Remark 8.1.3. More generally, once a matrix immersion $\Phi_p : H \to \mathrm{M}_2(\mathbb{Q}_p(\sqrt{a}))$ is fixed, we can always change the presentation of H in order to have $\Phi_p(H) \subseteq \mathrm{M}_2(\mathbb{Q}_p)$, that is, we can always choose integers a, b such that the Hilbert symbol is $(a,b)_\ell = -1$ for every $\ell \mid D$ and $(a,b)_\ell = 1$ for every $\ell \nmid D$, and such that $\left(\frac{a}{p}\right) = 1$ (cf. [Ser70]).

Proposition 8.1.4. *Let B be an indefinite quaternion algebra of discriminant Dp and let $\mathcal{O}_B(N) \subseteq B$ be an Eichler order of level N. Let $X(Dp, N)$ be the Shimura curve associated to B and $\mathcal{O}_B(N)$. Let H be the definite quaternion algebra of discriminant D and let $\mathcal{O} = \mathcal{O}_H(N) \subseteq H$ be an Eichler order of level N. Assume that $\mathcal{O}$ satisfies the hypothesis of Theorem 7.2.2. Then the reduction-graph with lengths $\Gamma_p\backslash\mathcal{T}_p$ has one vertex of length $\#\mathcal{O}^\times/\mathbb{Z}^\times$, and the number of edges is described in Table 8.1.*

D	N	c_1	c_2	c_3
2	1	$\frac{1}{12}\left(p-9-4\left(\frac{3}{p}\right)\right)$	1	$1+\left(\frac{3}{p}\right)$
	3	$\frac{1}{3}\left(p-\left(\frac{3}{p}\right)\right)$	0	$1+\left(\frac{3}{p}\right)$
	9	$p+1$	0	0
	11	$p+1$	0	0
3	1	$\frac{1}{6}\left(p-6-\left(\frac{3}{p}\right)\right)$	2	$\frac{1}{2}\left(1+\left(\frac{3}{p}\right)\right)$
	2	$\frac{1}{2}(p-1)$	2	0
	4	$p+1$	0	0
5	1	$\frac{1}{3}\left(p-\left(\frac{-3}{p}\right)\right)$	0	$1+\left(\frac{-3}{p}\right)$
	2	$p+1$	0	0
13	1	$p+1$	0	0

Table 8.1: Number of edges with lengths of the graph $\Gamma_p\backslash\mathcal{T}_p$

Proof. Since the graph $\Gamma_p(\xi)\backslash\mathcal{T}_p$ has 1 vertex of length 1 (cf. Theorem 7.2.2), we have that the quotient graph

$$\Gamma_p\backslash\mathcal{T}_p \simeq (\Gamma_p(\xi)\backslash\mathcal{T}_p)/(\Gamma_p/\Gamma_p(\xi))$$

has only 1 vertex $[v^0]$ of length $\ell([v^0]) = \#\Gamma_p/\Gamma_p(\xi) = \#\mathcal{O}^\times/\mathbb{Z}^\times$. After Theorem 7.2.2 (d), we know that the reduction-graph $\Gamma_p(\xi)\backslash\mathcal{T}_p$ consists of $p+1$ oriented edges pair-wise identified.

Now we only need to describe the action of $\mathcal{O}^\times/\mathbb{Z}^\times \simeq \Gamma_p/\Gamma_p(\xi)$ on this graph. Note that the fundamental domain for the action of $\Gamma_p(\xi)$ in $\mathcal{T}_p$ (which is by definition the reduction of a good fundamental domain in $\mathcal{H}_p$) is the open tree

$$\mathcal{T}_p^{(1)} \smallsetminus \{v_a^{(1)} \mid a \in \mathbb{P}^1(\mathbb{F}_p)\} \simeq \mathrm{Star}(v^0),$$

so we can identify each of its open edges with the $\mathbb{F}_p$-rational points of $\mathbb{P}^1_{\mathbb{F}_p}$ by fixing a bijection $\delta : \mathrm{Star}(v^0) \simeq \mathbb{P}^1(\mathbb{F}_p)$. This gives rise to the following action on the edges:

$$\begin{array}{rcl} \mathrm{PGL}_2(\mathbb{Z}_p) \times \mathrm{Star}(v^0) & \to & \mathrm{Star}(v^0) \\ (\gamma, e) & \mapsto & \mathrm{red}(\gamma)\cdot\delta(e) \end{array}$$

where $\mathrm{red} : \mathrm{PGL}_2(\mathbb{Z}_p) \twoheadrightarrow \mathrm{PGL}_2(\mathbb{F}_p) = \mathrm{Aut}(\mathbb{P}^1(\mathbb{F}_p))$ is the natural projection. Now, since $\Phi_p(\mathcal{O}^\times)/\mathbb{Z}^\times \subseteq \mathrm{PGL}_2(\mathbb{Z}_p)$, in order to study the action of $\Phi_p(\mathcal{O}^\times)/\mathbb{Z}^\times$ on $\Gamma_p(\xi)\backslash\mathcal{T}_p$ we need to study the fixed points in $\mathbb{P}^1(\mathbb{F}_p)$ of these finite order transformations.

Since, by Lemma 8.1.2 the length $\ell([e])$ of an edge $[e] \in \mathrm{Ed}(\Gamma_p\backslash\mathcal{T}_p)$ has to divide $\ell([v^0]) = \#\mathcal{O}^\times/\mathbb{Z}^\times$, by Table 6.1 we know that $\ell([e]) \in \{1,2,3,4,6,12\}$. Here we need to separate cases:

(*i*) $(D,N) = (2,9), (2,11), (3,4), (5,2)$ and $(13,1)$. In these cases we have that $\#\mathcal{O}^\times/\mathbb{Z}^\times = 1$, so $\Gamma_p\backslash\mathcal{T}_p$ is the stable reduction-graph $\Gamma_p(\xi)\backslash\mathcal{T}_p$ with $(p+1)/2$ edges of length 1.

(*ii*) $D = 2, N = 1$. In this case we have

$$\mathcal{O}^\times/\mathbb{Z}^\times = \left\{1, i, j, k, \frac{1 \pm i \pm j \pm k}{2}\right\}$$

and there are transformations of order 2 and of order 3. The order 2 transformations are

$$\Phi_p(i) = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & \sqrt{-1} \end{pmatrix}, \quad \Phi_p(j) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \Phi_p(k) = \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix},$$

and the order 3 transformations are

$$\Phi_p\left(\frac{1 \pm i + j + k}{2}\right) = \frac{1}{2}\begin{pmatrix} 1 \pm \sqrt{-1} & 1 + \sqrt{-1} \\ -1 + \sqrt{-1} & 1 \mp \sqrt{-1} \end{pmatrix},$$

$$\Phi_p\left(\frac{1 + i \pm j + k}{2}\right) = \frac{1}{2}\begin{pmatrix} 1 + \sqrt{-1} & \pm 1 + \sqrt{-1} \\ \mp 1 + \sqrt{-1} & 1 - \sqrt{-1} \end{pmatrix},$$

$$\Phi_p\left(\frac{1 + i + j \pm k}{2}\right) = \frac{1}{2}\begin{pmatrix} 1 + \sqrt{-1} & 1 \pm \sqrt{-1} \\ -1 \mp \sqrt{-1} & 1 - \sqrt{-1} \end{pmatrix},$$

$$\Phi_p\left(\frac{1 \pm i - j \mp k}{2}\right) = \frac{1}{2}\begin{pmatrix} 1 \pm \sqrt{-1} & -1 \mp \sqrt{-1} \\ 1 \mp \sqrt{-1} & 1 \mp \sqrt{-1} \end{pmatrix}.$$

Studying the fixed points of each transformation in $\mathbb{P}^1(\mathbb{F}_p)$ one can see that, under the restriction that $\left(\frac{-1}{p}\right) = 1$ (which is given by the chosen presentation for the algebra), each order 2 transformation has always 2 fixed points in $\mathbb{P}^1(\mathbb{F}_p)$, and that an order 3 transformation has 2 fixed points in $\mathbb{P}^1(\mathbb{F}_p)$ if $p \equiv 1 \bmod 3$ and 0 fixed points if $p \equiv 2 \bmod 3$. One also checks that there is no point fixed at the same time by an order 2 transformation and an order 3 transformation. From this we conclude that $c_3 = 2$ if $p \equiv 1 \bmod 3$ and $c_3 = 0$ if $p \equiv 2 \bmod 3$. Next, one can see that the three unoriented edges of $\Gamma_p(2)\backslash\mathcal{T}_p$ corresponding to the 6 fixed points of order 2 transformations are all identified by the transformations of order 3. Thus we are left with only one edge $[y]$ of length 2. Since c_2 counts the number of oriented edges of order 2, we now could have either $c_2 = 2$ (if $[e] \neq [\overline{e}]$) or $c_2 = 1$ (if $[e] = [\overline{e}]$). An easy computation shows that we are in the second case. Thus $c_2 = 1$. Finally, by Lemma 8.1.2, we obtain $p + 1 = 12c_1 + 6c_2 + 4c_3$. So we have that if $c_3 = 2$ then $c_1 = \frac{p-13}{12}$ and if $c_3 = 0$ then $c_1 = \frac{p-5}{12}$.

(*iii*) $D = 2, N = 3$. In this case, since $\#\mathcal{O}^\times/\mathbb{Z}^\times = 3$, we have $c_2 = 0$. Lemma 8.1.2 gives $p + 1 = 3c_1 + c_3$. Again, after studying the order 3 transformations we can see that $c_3 = 2$ if $p \equiv 1 \bmod 3$ and $c_3 = 0$ if $p \equiv 2 \bmod 3$. Thus $c_1 = \frac{p-1}{3}$ if $p \equiv 1 \bmod 3$ and $c_3 = \frac{p+1}{3}$ if $p \equiv 2 \bmod 3$.

(*iv*) $D = 3, N = 1$. In this case $\#\mathcal{O}^\times/\mathbb{Z}^\times = 6$. As before, one can see that the points fixed by order 2 transformations are never fixed by order 3 transformations. Lemma 8.1.2 gives $p+1 = 6c_1+3c_2+2c_1$. The order 3 transformations give $c_3 = 1$ when $p \equiv 1 \bmod 3$ and $c_3 = 0$ when $p \equiv 2 \bmod 3$ and the order 2 transformations give again some unoriented edges that the order 3 transformations take to the same class $[e] \in \mathrm{Ed}(\Gamma_p(2)\backslash\mathcal{T}_p)$. In this case $c_2 = 2$, because $[e] \neq [\overline{e}]$.

(v) $D = 3, N = 2$. In this case, $\#\mathcal{O}^\times/\mathbb{Z}^\times = 2$, so $c_3 = 0$. The order 2 transformation gives two oriented edges that are not in the same class, so $c_2 = 2$. Finally, Lemma 8.1.2 gives $p + 1 = 2c_1 + c_2$, so $c_1 = \frac{p-1}{2}$.

(vi) $D = 5, N = 1$. In this case $\#\mathcal{O}^\times/\mathbb{Z}^\times = 3$, so $c_2 = 0$. Similar computations as in the previous cases give $c_3 = 2$ and $c_1 = (p-1)/3$ when $p \equiv 1 \bmod 3$ and $c_3 = 0$ and $c_1 = (p+1)/3$ when $p \equiv 2 \bmod 3$.

□

Remark 8.1.5. We have already noted that we have restricted ourselves to some (infinite) set of primes p such that $\left(\frac{a}{p}\right) = 1$, with $a = -1$ when $D = 2, 3$, or $a = -2$ when $D = 5, 13$. This means that we are assuming that $p \equiv 1 \bmod 4$ when $D = 2, 3$ and $p \equiv 1, 3 \bmod 8$ when $D = 5, 13$. In Section 8.3 we will show that, at least in the cases $(D, N) = (2, 1), (3, 1)$ the condition $p \equiv 1 \bmod 4$ is not restrictive, since the primes satisfying this also satisfy that

$$t_\xi(p) := \#\{\alpha \in \mathcal{O} \mid \mathrm{Tr}(\alpha) = 0,\ \mathrm{Nm}(\alpha) = p,\ \alpha \equiv 1 \bmod \xi\mathcal{O}\} = 0,$$

which is the null-trace condition of Theorem 7.2.2.

Remark 8.1.6. In the cases with $N = 1$, the formulas in Table 8.1 coincide with the ones obtained by Kurihara in [Kur79], even though the method for proving them is substantially different.

8.2 Genus formulas

After Corollary 7.2.3 we have constructed, for the orders $\mathcal{O}$ together with the quaternions ξ of Table 6.1, and for prime integers p satisfying the null-trace condition of Definition 7.1.4, a covering $\Gamma_p(\xi)\backslash\mathcal{H}_p \twoheadrightarrow \Gamma_p\backslash\mathcal{H}_p$ of degree $\mathcal{O}^\times/\mathbb{Z}^\times$, where the quotient $\Gamma_p(\xi)\backslash\mathcal{H}_p$ is algebraisable and has genus $(p+1)/2$. Therefore, following [GvdP80] we can apply the Riemann-Hurwitz formula in order to compute the genus of the algebraic curve $\Gamma_p\backslash\mathcal{H}_p$:

$$p - 1 = \#(\mathcal{O}^\times/\mathbb{Z}^\times)(2g - 2) + \sum_{d \mid \#(\mathcal{O}^\times/\mathbb{Z}^\times)} w_d,$$

where w_d is the number of points on $\Gamma_p\backslash\mathcal{H}_p$ which are fixed by some transformation in Γ_p of order $d > 1$.

The formulas we obtain in the following result generalise those computed in [GvdP80] relative to the family of Shimura curves $X(2p, 1)$, with $p \equiv 1 \bmod 4$. We refer the reader also to [vdP92], in which the author explains the explicit relations of these computations with the family of Shimura curves $X(2p, 1)$.

Proposition 8.2.1. *Under the assumptions of Theorem* 7.2.2*, the genus of the graph* $\Gamma_p\backslash\mathcal{T}_p$ *is expressed in Table* 8.2*, where*

(i) $\delta_p(2, 1) := w_2^{(1)} + w_2^{(2)} + w_2^{(3)}$*, with*

$$w_2^{(i)} := \frac{1}{2}\#\{(\alpha = (a_0, a_1, a_2, a_3)_H \in \mathcal{O} \mid \mathrm{Nm}(\alpha) = p,\ \alpha \equiv 1 \bmod 2\mathcal{O},\ a_i = 0\},\ i = 1, 2, 3.$$

(*ii*) $\delta_p(3,1) := w_2^{(1)} + w_2^{(2)} + w_2^{(3)}$, *with*

$$w_2^{(1)} := \frac{1}{2}\#\{\alpha = (a_0,a_1,a_2,a_3)_H \in \mathcal{O} \mid \mathrm{Nm}(\alpha) = p, \alpha \equiv 1 \bmod 2\mathcal{O},\ a_1 = 0\},$$

$$w_2^{(2)} := \frac{1}{2}\#\{\alpha = (a_0,a_1,a_2,a_3)_H \in \mathcal{O} \mid \mathrm{Nm}(\alpha) = p, \alpha \equiv 1 \bmod 2\mathcal{O},\ a_1 + 3a_2 = 0\},$$

$$w_2^{(3)} := \frac{1}{2}\#\{\alpha = (a_0,a_1,a_2,a_3)_H \in \mathcal{O} \mid \mathrm{Nm}(\alpha) = p, \alpha \equiv 1 \bmod 2\mathcal{O},\ a_1 - 3a_2 = 0\}.$$

(*iii*) $\delta_p(3,2) := \frac{1}{2}\#\{\alpha = (a_0,a_1,a_2,a_3)_H \in \mathcal{O} \mid \mathrm{Nm}(\alpha) = p,\ \alpha \equiv 1 \bmod \xi\mathcal{O},\ a_1 - 3a_2 = 0\}.$

D	N	genus
2	1	$\frac{1}{24}\left(p+23-\delta_p(2,1)-8\left(1-\left(\frac{3}{p}\right)\right)\right)$
	3	$\frac{1}{6}\left(p+5-2\left(1-\left(\frac{-3}{p}\right)\right)\right)$
	9	$(p+1)/2$
	11	$(p+1)/2$
3	1	$\frac{1}{12}\left(p+11-\delta_p(3,1)-2\left(1-\left(\frac{3}{p}\right)\right)\right)$
	2	$\frac{1}{4}\left(p+3-\delta_p(3,2)\right)$
	4	$(p+1)/2$
5	1	$\frac{1}{6}\left(p+5-2\left(1-\left(\frac{-3}{p}\right)\right)\right)$
	2	$(p+1)/2$
13	1	$(p+1)/2$

Table 8.2: Genus of $\Gamma_p\backslash\mathcal{T}_p$

Proof. For the case $D = 2$, $N = 1$, we refer the reader to [GvdP80, Ch. IX]. We will prove here another case, since all cases are computed in a similar way. We consider the case $D = 3$, and $N = 1$. That is the one for which the group $\Phi_p(\mathcal{O}^\times)/\mathbb{Z}^\times$ is the biggest among the ones we are considering. For each order 2 transformation $u_2^{(i)} \in \Phi_p(\mathcal{O}^\times)/\mathbb{Z}^\times$, we have to compute the cardinality

$$w_2^{(i)} := \#\{[z] \in \Gamma_p\backslash\mathcal{T}_p \mid\ u_2^{(i)} z = \gamma z,\ \gamma \in \Gamma_p(2)\}.$$

Let us study each unit of order 2 separately.

- $u_2^{(1)} = \left(\begin{smallmatrix}\sqrt{-1} & 0\\ 0 & \sqrt{-1}\end{smallmatrix}\right)$. The equation $uz = \gamma z$, with $\gamma = \left(\begin{smallmatrix}A & B\\ C & D\end{smallmatrix}\right) \in \Gamma_p(2)$ gives

$$z = -\frac{A+D}{2C} \pm \frac{\sqrt{(\frac{A+D}{2})^2 - BC}}{C},$$

so $(\frac{A+D}{2})^2 - BC = a_0 + 3(a_2^2 + a_3^2) = p - a_1^2$, which does not belong to $\mathbb{Q}_p^{\times 2}$ if and only if $a_1 = 0$. Therefore in this case we obtain that $w_2^{(1)}$ is equal to 2 times the number of generators α of $\Gamma_p(\xi)$ such that the coordinates $(a_0, a_1, a_2, a_3)_H$ in the basis of $H = \left(\frac{-1,-3}{\mathbb{Q}}\right)$ have $a_1 = 0$, and this is equal to

$$\frac{1}{4} \cdot 2 \cdot \#\{\alpha = (a_0, a_1, a_2, a_3)_H \in \mathcal{O} \mid \mathrm{Nm}(\alpha) = p, \alpha \equiv 1 \bmod 2\mathcal{O},\ a_1 = 0\},$$

since we have to exclude for each quaternion α in this set, its conjugated $\overline{\alpha}$, its opposite $-\alpha$ and the opposite of its conjugated $-\overline{\alpha}$.

- $u_2^{(2)} = \begin{pmatrix} \frac{1}{2}\sqrt{-1} & \frac{1}{2} \\ -\frac{3}{2} & -\frac{1}{2}\sqrt{-1} \end{pmatrix}$. Analogous arguments show that the number $w_2^{(2)}$ is equal to 2 times the number of generators $\alpha = (a_0, a_1, a_2, a_3)_H$ of $\Gamma_p(\xi)$ with $a_1 + 3a_2 = 0$.
- $u_2^{(3)} = \begin{pmatrix} \frac{1}{2}\sqrt{-1} & -\frac{1}{2} \\ \frac{3}{2} & -\frac{1}{2}\sqrt{-1} \end{pmatrix}$. Similar computations in this case give that $w_2^{(3)}$ is equal to 2 times the number of generators $\alpha = (a_0, a_1, a_2, a_3)_H$ of $\Gamma_p(\xi)$ with $a_1 - 3a_2 = 0$.

For the order 3 transformations $u_3^{(i)} \in \Phi_p(\mathcal{O}^\times)/\mathbb{Z}^\times$, $i = 1, 2$, we have to compute the value

$$w_3^{(i)} := \{[z] \in \Gamma_p \backslash \mathcal{T}_p \mid uz = z\}$$

in a similar way. This is $1 - \left(\frac{3}{p}\right)$ in each case, and the formula is then completed for this case. □

Corollary 8.2.2. *Under the assumptions of Theorem* 7.2.2*, the reduction-graph with lengths* $\Gamma_{p,+} \backslash \mathcal{T}_p$ *is described by the following properties:*

(*a*) *It consists of two vertices and* $c_1 + c_2 + c_3$ *unoriented edges joining them, with the values* c_1, c_2, c_3 *given in Table* 8.1*.*

(*b*) *Its genus is* $g_+ = c_1 + c_2 + c_3 - 1$*.*

(*c*) *The number of edges with lengths is obtained by multiplying by* 2*, in each case, the formulas of Table* 8.1*.*

Proof. The curve $\Gamma_{p,+} \backslash \mathcal{H}_p$ is a degree 2 covering of $\Gamma_p \backslash \mathcal{H}_p$, so it is immediate to see that

$$g_+ = \#\{e \in \mathrm{Ed}(\Gamma_p \backslash \mathcal{T}_p) \mid -e \neq e\} - 1 + \#\{e \in \mathrm{Ed}(\Gamma_p \backslash \mathcal{T}_p) \mid -e = e\} = c_1 + c_2 + c_3 - 1.$$

The rest of the statement is then also clear. □

Remark 8.2.3. The genus g_+ is actually the genus of the special fibre of the Drinfel'd model $\mathcal{X}(Dp, N)$ of the considered Shimura curves. Indeed, the reader can check that this coincides with the usual genus formula for the Shimura curve $X(Dp, N)$, i.e.

$$g(X(Dp, N)) = 1 + \frac{N}{12} \prod_{\ell | Dp} (\ell - 1) \prod_{\ell | N} \left(\frac{\ell + 1}{\ell}\right) - \frac{1}{4} e_2(D, N) - \frac{1}{3} e_3(D, N),$$

where

$$e_2(Dp,N) := \begin{cases} \prod_{\ell|Dp}\left(1-\left(\frac{-4}{\ell}\right)\right)\prod_{\ell|N}\left(1+\left(\frac{-4}{\ell}\right)\right) & \text{if } 4\nmid N, \\ 0 & \text{if } 4\mid N, \end{cases}$$

$$e_3(Dp,N) := \begin{cases} \prod_{\ell|Dp}\left(1-\left(\frac{-3}{\ell}\right)\right)\prod_{\ell|N}\left(1+\left(\frac{-3}{\ell}\right)\right) & \text{if } 9\nmid N, \\ 0 & \text{if } 9\mid N. \end{cases}$$

(cf. [Shi70]).

8.3 The null-trace condition

Here we show how one can make more explicit some conditions about the considered generators of the Schottky groups. We will take a close look to the case $D = 3$ and $N = 1$, and we will rewrite the null-trace condition (cf. condition (iii) of Theorem 7.2.2) in a more amenable and arithmetic way.

Lemma 8.3.1. *A quaternion $\alpha = a_0 + a_1 i + a_2 j + a_3 k \in H = \left(\frac{-1,-3}{\mathbb{Q}}\right)$ belongs to the finite set*

$$A := \{\alpha \in \mathcal{O} \mid \alpha \equiv 1 \bmod 2\mathcal{O},\ \mathrm{Nm}(\alpha) = p\}$$

if and only if it satisfies the following conditions:

(i) $a_i \in \mathbb{Z}$ *for every* $0 \le i \le 3$,

(ii) $a_0^2 + a_1^2 + 3a_2^2 + 3a_3^2 = p$,

(iii) $a_0 + a_3 \equiv 1 \bmod 2$, $a_1 + a_2 \equiv 0 \bmod 2$.

Proof. Let $H = \left(\frac{-1,-3}{\mathbb{Q}}\right)$ be the definite quaternion algebra of discriminant $D = 3$ and let us consider the maximal order $\mathcal{O} \subseteq H$ with basis $\{1, i, \lambda, \mu\}$, where $\lambda := (i+j)/2$ and $\mu := (1+k)/2$. If we take $\alpha = a_0 + a_1 i + a_2 j + a_3 k \in A$ and we express it in the integral basis of $\mathcal{O}$, namely $\alpha = x + yi + z\lambda + t\mu$, we obtain the following relations:

$$a_0 = x + t/2, \quad a_1 = y + z/2, \quad a_2 = z/2, \quad a_3 = t/2.$$

The condition $\alpha \equiv 1 \bmod 2$ tells us that $z \equiv t \equiv 0 \bmod 2$, so $a_i \in \mathbb{Z}$ for every $0 \le i \le 3$. Moreover we also have $a_0 + a_3 = x + t \equiv 1 \bmod 2$ and $a_1 + a_2 = y + z \equiv 0 \bmod 2$, so we find the conditions of the statement on the coefficients a_i. The converse is clearly true. □

Proposition 8.3.2. *Let H be the definite quaternion algebra of discriminant $D = 3$ and let $\mathcal{O} \subseteq H$ be a maximal order. With the notations as in Theorem 7.1.5 we have that, if $p \equiv 1 \bmod 4$, then*

$$t_2(p) := \#\{\alpha \in \mathcal{O} \mid \alpha \equiv 1 \bmod 2\mathcal{O},\ \mathrm{Nm}(\alpha) = p,\ \mathrm{Tr}(\alpha) = 0\} = 0.$$

Proof. Suppose that there exists a pure quaternion $\alpha \in \mathcal{O}$ of norm p such that $\alpha \equiv 1 \bmod 2\mathcal{O}$. Then the previous conditions on the coefficients $a_i \in \mathbb{Z}$ translate into

$$a_3 \equiv 1 \bmod 2, \quad a_1 + a_2 \equiv 0 \bmod 2, \quad a_1^2 + 3a_2^2 + 3a_3^2 = p.$$

If we now reduce modulo 4 we obtain

$$p = a_1^2 + 3a_2^2 + 3a_3^2 \equiv 4a_2^2 + 3 \equiv 3 \bmod 4.$$

□

In an analogous way one can prove also the following proposition for the order of Hurwitz quaternions (cf. [GvdP80, Ch. IX]).

Proposition 8.3.3. *Let H be the definite quaternion algebra of discriminant $D = 2$ and let $\mathcal{O}$ be a maximal order in H. If $p \equiv 1 \bmod 4$, then $t_2(p) = 0$.*

Remark 8.3.4. After Lemma 8.3.1 we can rewrite the quantity $\delta_p(3,1)$ arising in the genus formula of Proposition 8.2.1 as $\delta_p(3,1) := w_2^{(1)} + w_2^{(2)} + w_2^{(3)}$, with

$$\begin{aligned}
w_2^{(1)} &:= \frac{1}{2}\#\{(a_0,a_2,a_3) \in \mathbb{Z}^3 \mid a_0^2 + 3(a_2^2 + a_3^2) = p, \\
&\qquad\qquad a_0 + a_3 \equiv 1 \bmod 2,\ a_2 \equiv 0 \bmod 2\}, \\
w_2^{(2)} &:= \frac{1}{2}\#\{(a_0,a_1,a_2,a_3) \in \mathbb{Z}^4 \mid a_0^2 + a_1^2 + 3(a_2^2 + a_3^2) = p, \\
&\qquad\qquad a_0 + a_3 \equiv 1 \bmod 2,\ a_1 + a_2 \equiv 0 \bmod 2,\ a_1 + 3a_2 = 0\}, \\
w_2^{(3)} &:= \frac{1}{2}\#\{(a_0,a_1,a_2,a_3) \in \mathbb{Z}^4 \mid a_0^2 + a_1^2 + 3(a_2^2 + a_3^2) = p, \\
&\qquad\qquad a_0 + a_3 \equiv 1 (\bmod 2),\ a_1 + a_2 \equiv 0 \bmod 2,\ a_1 - 3a_2 = 0\}.
\end{aligned}$$

The same approach works also for the case $D = 2$ and $N = 1$ (as worked out in [GvdP80, Ch. IX]). Actually $\delta_p(2,1) := w_2^{(1)} + w_2^{(2)} + w_2^{(3)}$, with

$$\begin{aligned}
w_2^{(1)} &:= \frac{1}{2}\#\{(a_0,a_2,a_3) \in \mathbb{Z}^3 \mid a_0^2 + a_2^2 + a_3^2 = p,\ a_0 \equiv 1; \bmod 2,\ a_2 \equiv a_3 \equiv 0 \bmod 2\}, \\
w_2^{(2)} &:= \frac{1}{2}\#\{(a_0,a_1,a_3) \in \mathbb{Z}^3 \mid a_0^2 + a_1^2 + a_3^2 = p,\ a_0 \equiv 1; \bmod 2,\ a_1 \equiv a_3 \equiv 0 \bmod 2\}, \\
w_2^{(3)} &:= \frac{1}{2}\#\{(a_0,a_1,a_2) \in \mathbb{Z}^3 \mid a_0^2 + a_1^2 + a_2^2 = p,\ a_0 \equiv 1; \bmod 2,\ a_1 \equiv a_2 \equiv 0 \bmod 2\}.
\end{aligned}$$

Chapter 9

Computation of reduction-graphs

In the this chapter we describe an algorithm, that we have implemented in Magma [BCP97], in order to obtain explicit examples illustrating our method.

In section 9.1 we give a detailed example of how one can use our algorithm to compute:

(1) a quaternion $\xi \in \mathcal{O}$ such that the group $\Gamma_p(\xi)$ is a Schottky group using Theorem 7.1.5,

(2) a free system of generators for this Schottky group as in Theorem 7.1.5,

(3) a p-adic good fundamental domain in the p-adic upper half-plane $\mathcal{H}_p$ for the action of the Schottky group, as in Theorem 7.2.2

(4) the stable reduction-graph of this fundamental domain, as explained in Theorem 7.2.2.

In section 9.2 we give a description of the functions that we use in our algorithm.

9.1 Examples

We will consider, as a concrete example, the family of Shimura curves of discriminant $D_B = 3p$ and level $N = 2$.

First we need to compute the definite quaternion algebra $H = \left(\frac{-1,-3}{\mathbb{Q}}\right)$ of discriminant $D = 3$, an integral basis for an Eichler order $\mathcal{O} \subseteq H$ of level $N = 2$, and an element $\xi \in \mathcal{O}$ satisfying the right-unit property in $\mathcal{O}$, as requested by Theorem 7.1.5.

```
> D := 3; N:=2;
> H, O := Data(D,N);
> NmH, NmO := Normic_form(H,O);
> xi := choose_xi(O);
> xi;
-1/2 - 1/2*I - 1/2*J + 1/2*K
```

We fix then the prime $p = 13$. We now see that this prime satisfies the null-trace condition with respect to the chosen ξ. Therefore, by Theorem 7.2.2, we know that $\Gamma_{13}(-\frac{1}{2} - \frac{1}{2}i - \frac{1}{2}j + \frac{1}{2}ij)$ is

a Schottky group and that the stable reduction-graph of the associated Mumford curve will be a graph obtained via pair-wise identification of the boundary edges of a graph, consisting of one vertex and $p+1 = 14$ edges (see Figure 9.1).

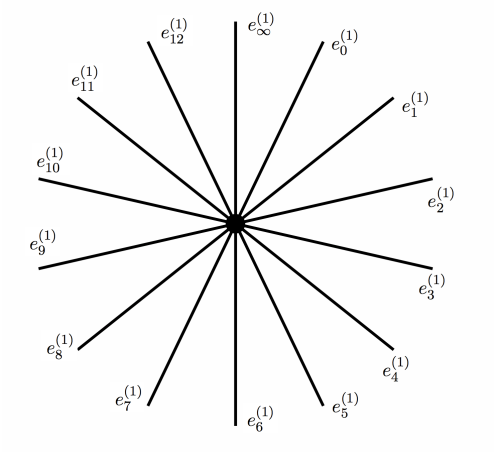


Figure 9.1: Reduction of the fundamental domain $\mathcal{F}_{13}(-\frac{1}{2} - \frac{1}{2}i - \frac{1}{2}j + \frac{1}{2}ij)$

In order to compute these identifications, as described in Theorem 7.2.2, we first need to compute a system of generators for the Schottky group $\Gamma_p(\xi)$. These are first computed as quaternions of H and then as p-adic matrices in $\mathrm{GL}_2(\mathbb{Q}_p)$. Note that there are $(p+1)/2 = 7$ of them, as predicted by Proposition 7.1.8. The symbol `i` appearing in the matrix description below is the 13-adic number $\sqrt{-1}$.

```
> p := 13;
> gens_xi, gens_Schottky := generators_Gammas(H,O,p,xi);
> gens_xi;
[ -3 + 1/2*I - 1/2*J + K, -3 - 1/2*I + 1/2*J + K, -3 + I - J,
-1 + 2*K, -1 + 3/2*I - 3/2*J + K, -1 - 3/2*I + 3/2*J + K, -1 - 3*I - J ]
> gens_Schottky;
[
    [  1/2*(i - 6) 1/2*(2*i - 1)]
    [1/2*(6*i + 3)  1/2*(-i - 6)],

    [ 1/2*(-i - 6) 1/2*(2*i + 1)]
    [1/2*(6*i - 3)   1/2*(i - 6)],

    [ i - 3     -1]
    [     3 -i - 3],

    [ -1 2*i]
    [6*i  -1],
```

```
    [ 1/2*(3*i - 2)  1/2*(2*i - 3)]
    [ 1/2*(6*i + 9) 1/2*(-3*i - 2)],

    [1/2*(-3*i - 2)  1/2*(2*i + 3)]
    [ 1/2*(6*i - 9)  1/2*(3*i - 2)],

    [-3*i - 1       -1]
    [       3  3*i - 1]
]
```

We can now compute the fundamental domain $\mathcal{F}_p(\xi) \subseteq \mathcal{H}_p$ for the action of $\Gamma_p(\xi)$. The next function `fundamental_domain` gives as output the radii $1/\sqrt{p}$ of the balls constituting the boundary of the fundamental domain, as well as the pair-wise identification of the boundary of these balls (cf. Theorem 7.2.2). This is done by reducing modulo p the fixed points of the transformations γ, γ^{-1} for all the generators γ previously computed. In the output of this function, each ball is identified by the coordinates of its center, which is a point in $\mathbb{P}^1(\mathbb{Q}_p)$.

```
> radius, pairing := fundamental_domain(H,O,p,xi,gens_xi);
> radius;
0.27735009811261456100917086672 8
> pairing;
[
    <( 9  1), (11  1)>,
    <( 1  1), ( 2  1)>,
    <( 5  1), ( 7  1)>,
    <( 3  1), (10  1)>,
    <( 8  1), ( 1  0)>,
    <( 0  1), ( 6  1)>,
    <( 4  1), (12  1)>
]
```

In figure 9.2 we represent this p-adic fundamental domain, where one has to read the labels of the balls as a notation for the pair-wise identifications given in `pairing`: the interior (resp. exterior) of the ball X is identified with the exterior (resp. interior) of the ball X^{-1}. Finally, in figure 9.3, we can see the reduction-graph of the Mumford curve associate to $\Gamma_p(\xi)$, which is obtained by reduction of the rigid analytic variety $\Gamma_p(\xi)\backslash\mathcal{F}_p(\xi)$.

Now we show how we compute the reduction-graph with lengths $\Gamma_p\backslash\mathcal{T}_p$. It is important to remark that, even if one could easily compute this graph with its lengths, thanks to the formulas of Table 8.1 and Table 8.2, we use here an alternative algorithm we designed in order to obtain the desired graph. Indeed, we do it by letting act the Schottky group $\Gamma_p(\xi)$ on the quotient $(\mathcal{O}^\times/\mathbb{Z}^\times)\backslash\mathcal{T}_p = (\Gamma_p/\Gamma_p(\xi))\backslash\mathcal{T}_p$.

Therefore we first need to compute the quotient of the reduction of the fundamental domain $\mathcal{F}_p(\xi)$ (see Figure 9.1) by the action of the finite group $\mathcal{O}^\times/\mathbb{Z}^\times$. This is done by using the following function `UnitsAction`.

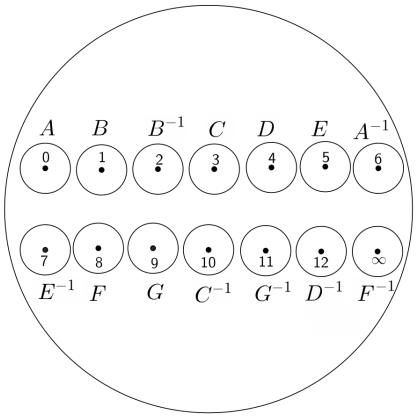


Figure 9.2: Fundamental domain $\mathcal{F}_p(\xi)$ for the action of $\Gamma_p(\xi)$ on $\mathcal{H}_p$

```
classes := UnitsAction(H,O,p);
> classes;
[ { ( 8  1), ( 0  1) },
  { ( 1  1), (11  1) },
  { ( 2  1), ( 9  1) },
  { (10  1), ( 3  1) },
  { (12  1), ( 4  1) },
  { ( 5  1) },
  { ( 6  1), ( 1  0) },
  { ( 7  1) } ]
```

For example, we can see that the oriented edge $e_8^{(1)}$ is identified with $e_0^{(1)}$, and that the edge $e_5^{(1)}$ remains alone in its class (for the moment).

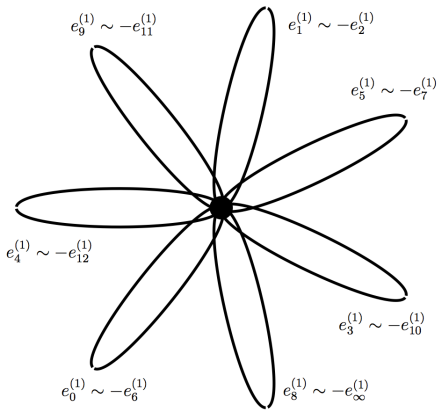


Figure 9.3: Stable reduction-graph of the Mumford curve associated to $\Gamma_{13}(-\frac{1}{2} - \frac{1}{2}i - \frac{1}{2}j + \frac{1}{2}ij)$

Finally, with the function `DescriptionGraph` we compute the reduction-graph with lengths $\Gamma_{13}\backslash\mathcal{T}_{13}$, which corresponds to the special fibre at 13 of the Atkin-Lehner quotient, associated to the prime 13, of the Shimura curve $X(3\cdot 13, 2)$.

```
aller_retour, loops := DescriptionGraph(H,O,p,xi,gens_xi);
> aller_retour;
[
    <{ (10  1),( 3  1) }, 1>,
    <{ (12  1), ( 4  1) }, 1>
]
> loops;
[
    <{ ( 8  1), ( 6  1), ( 0  1), ( 1  0) }, 1>,
    <{ ( 2  1), ( 1  1), (11  1), ( 9  1) }, 1>,
    <{ ( 7  1), ( 5  1) }, 2>
]
```

We can see that this graph has 2 *aller-retour* edges (i.e. edges e such that $-e = e$) of length 1 and 1 *loop* of length 2 (obtained from the identification of $e_5^{(1)}$ with $-e_7^{(1)}$). In figure 9.4 we represent the reduction-graphs $\Gamma_{13}\backslash\mathcal{T}_{13}$ and $\Gamma_{13,+}\backslash\mathcal{T}_{13}$ associated to the Shimura curve $X(3p, 2)$ at the prime $p = 13$.

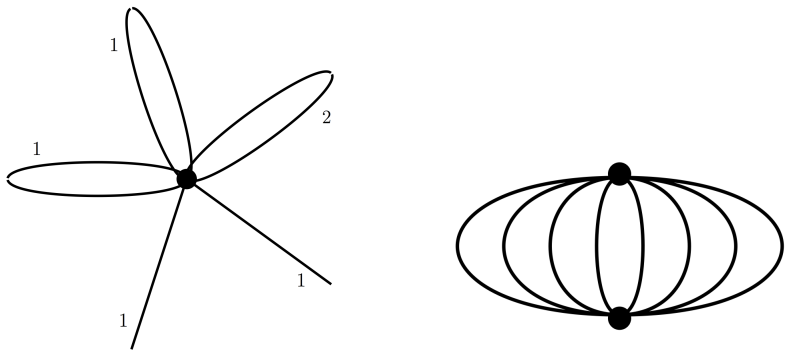


Figure 9.4: Reduction-graphs with lengths $\Gamma_{13}\backslash\mathcal{T}_{13}$ and $\Gamma_{13,+}\backslash\mathcal{T}_{13}$ for $X(3\cdot 13, 2)$

To conclude, we show the final reduction-graphs in another example: in Figure 9.5 the reduction-graphs $\Gamma_p\backslash\mathcal{T}_p$ and $\Gamma_{p,+}\backslash\mathcal{T}_p$ when $D = 3$, $N = 1$ and $p = 61$, are represented.

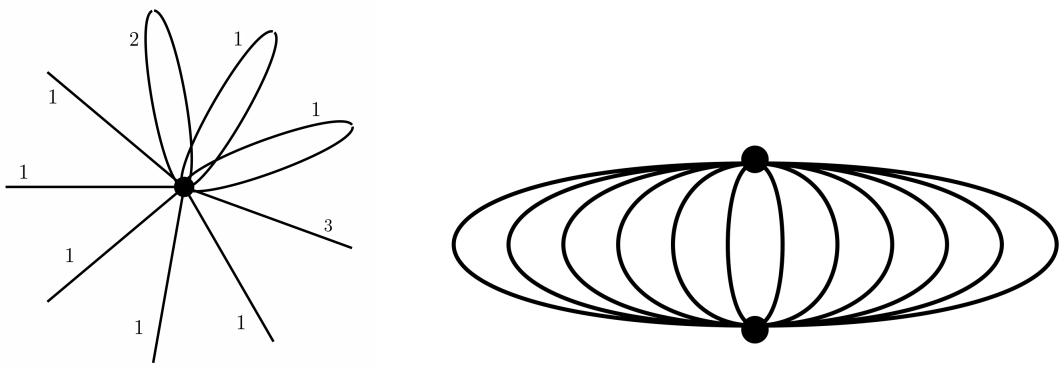


Figure 9.5: Reduction-graphs with lengths $\Gamma_{61}\backslash\mathcal{T}_{61}$ and $\Gamma_{61,+}\backslash\mathcal{T}_{61}$ for $X(3\cdot 61,1)$

9.2 Description of the functions used in the algorithm

Main functions

intrinsic generators_Gamma (H :: AlgQuat, O :: AlgQuatOrd, p :: RngIntElt, xi :: AlgQuatElt) -> SeqEnum, SeqEnum

Given an Eichler order $\mathcal{O}$ inside a definite quaternion algebra H with one-sided ideal class number 1, an odd prime integer p, and a quaternion $\xi \in \mathcal{O}$ satisfying the right-unit property in $\mathcal{O}$, this functions computes a free free system of generators for the Schottky group $\Gamma_p(\xi)^\star \subseteq \Gamma_p(\xi)$ (cf. Remark 7.2.4). The outputs is:

- The list of generators in quaternionic form, given as elements of H.
- The list of generators in matrix form, given as elements of $\mathrm{GL}_2(\mathbb{Q}_p)$.

When p satisfies the null-trace condition with respect to $\xi\mathcal{O}$, we have $\Gamma_p(\xi)^\star = \Gamma_p(\xi)$ and the output is a free system of generators for the Schottky group $\Gamma_p(\xi)$.

intrinsic fundamental_domain (H :: AlgQuat, O :: AlgQuatOrd, p :: RngIntElt, xi :: AlgQuatElt, gens_xi :: SeqEnum) -> FldReElt, SeqEnum

This function computes a good fundamental domain $\mathcal{F}_p(\xi) \subseteq \mathcal{H}_p$ with respect to the generators of the Schottky group $\Gamma_p(\xi)$ computed by the previous function. The output is:

- The radii $1/\sqrt{p}$ of the p-adic balls constituting the boundary of $\mathcal{F}_p(\xi)$.
- The pair-wise identifications of the boundary of these balls.

Each ball is identified with its center, which is a point in $\mathbb{P}^1(\mathbb{Q}_p)$.

intrinsic DescriptionGraph (H :: AlgQuat, O :: AlgQuatOrd, p :: RngIntElt, xi :: AlgQuatElt, gens_xi :: SeqEnum) -> SeqEnum, SeqEnum

This function computes the reduction-graph with lengths $\Gamma_p\backslash\mathcal{T}_p$. The output is:

- The list of *aller-retour* edges, together with their lengths.

- The list of loops, together with their lengths.

Each loop and each *aller-retour* edge is presented as a class of edges of the quotient graph $(\Gamma_p/\Gamma_p(\xi))/\mathcal{T}_p$.

Auxiliar functions

intrinsic Data (D :: RngIntElt, N :: RngIntElt) -> AlgQuat, AlgQuatOrd

This function determines a basis for the definite quaternion algebra H of discriminant D and a basis for an Eichler order $\mathcal{O} \subseteq H$ of level N.

intrinsic choose_xi (O :: AlgQuatOrd) -> AlgQuatElt

Given a definite Eichler order with ideal class number 1, this function finds a quaternion $\xi \in \mathcal{O}$ such that $2 \in \xi\mathcal{O}$, and which satisfies the right-unit property in $\mathcal{O}$.

intrinsic Normic_form (H :: AlgQuat, O :: AlgQuatOrd) -> RngMPolElt, RngMPolElt

This function computes the normic forms associated to a given definite quaternion algebra H and an Eichler order $\mathcal{O} \subseteq H$, respectively.

intrinsic UnitsAction (H :: AlgQuat, O :: AlgQuatOrd, p :: RngIntElt) -> SeqEnum, SeqEnum

This function computes the action of the unit group $\mathcal{O}^\times/\mathbb{Z}^\times$ on the fundamental domain computed by the function `fundamental_domain`. That is, it computes the quotient $(\Gamma_p/\Gamma_p(\xi))\backslash\mathcal{T}_p$.

Resum

El programa de Langlands es una xarxa de conjectures inmensa, de caràcter unificador, que connecta el món de les representacions automorfes de grups algebraics reductius amb el món de les representacions de Galois. Aquestes conjectures associen una representació automorfa d'un grup algebraic reductiu a cada representació de dimensió n d'un grup de Galois i, de manera recíproca, associen una representació de Galois a cada representació automorfa d'un grup algebraic reductiu. A més a més, aquestes correspondències estan fetes de manera que les funcions L lligades a aquests dos objectes coincideixen.

La teoria de formes modulars és un camp de l'anàlisi complexa la importància de la qual es troba en les seves connexions i aplicacions a la teoria de nombres. En aquesta tesi utilitzarem, d'una banda, les propietats aritmètiques de les formes modulars per estudiar certes representacions de Galois i el seu significat aritmètic. D'altra banda, utilitzarem el significat geometric d'aquestes funcions analítiques complexes per tal d'estudiar una generalització natural de les corbes modulars. Una corba modular és un objecte geomètric que parametritza classes d'isomorfisme de corbes el·líptiques juntament amb una estructura addicional que depèn de cert subgrup modular. La generalització que ens interessarà són les anomenades corbes de Shimura. Concretament ens interessaran els seus models p-àdics.

En aquesta tesi es tracten dos temes diferents, un a cada banda del programa de Langlands. A la banda de les representacions de Galois estem interessats en representacions de Galois que prenen valors en àlgebres de Hecke locals associades a formes modulars amb coeficients en cossos finits. A la banda de les formes automorfes ens interessen les corbes de Shimura: desenvolupem alguns resultats aritmètics en àlgebres de quaternions definides i donem alguns resultats sobre corbes de Mumford que recobreixen corbes de Shimura p-àdiques.

Gràcies a un teorema de Deligne, Deligne-Serre i Shimura, sabem que es pot associar, a tota forma pròpia de Hecke normalitzada $f \in S_2(N, \varepsilon; \overline{\mathbb{F}}_p)$, una representació de Galois contínua, semisimple i senar de dimensió 2 del grup de Galois absolut $G_{\mathbb{Q}}$ del cos de nombres racionals. A més, des que Khare, Wintenberger i altres van demostrar la conjectura de modularitat de Serre ([KW09a], [KW09b]), sabem que el recíproc també és cert, és a dir, les representacions de Galois senars i irreductibles provenen de formes modulars d'una manera molt concreta. Les propietats que gaudeixen els coeficients de les formes modulars han estat explotades des dels temps de Jacobi i Eisenstein, més tard per Ramanujan i ho continuen sent actualment. Hom pot estar interessat en trobar, per exemple, les congruències que poden aparèixer entre elles mòdul alguns nombres primers. Només per donar un exemple, a [Ram16] Ramanujan introdueix la seva *funció tau* τ, la qual descriu descriu els coeficients d'una forma cuspidal de pes 12 i nivell 1, i conjectura que

$\tau(n) \equiv \sigma_{11}(n) \bmod 691$, on $\sigma_k(n)$ denota la suma de les potències k-èssimes dels divisors positius de n. Ramanujan també conjecturà moltes altres congruències que no van ser demostrades fins molts anys després.

És ben sabut que les àlgebres de Hecke mod p governen congruències mod p de formes pròpies de Hecke normalitzades. Un dels objectius d'aquesta tesi és estudiar les representacions de Galois que prenen valors en aquestes àlgebres de Hecke per tal d'entendre millor aquestes congruències. Més concretament, suposem que tenim dues formes pròpies de Hecke diferents $f, g \in \mathrm{S}_k(N;\mathbb{C})$ de pes k, nivell N i caràcter trivial (només per tal de simplificar les notacions), i denotem per $\mathbb{T}_{\mathbb{Z}} \subseteq \mathrm{End}_{\mathbb{C}}(\mathrm{S}_k(N;\mathbb{C}))$ el subanell generat pels operadors T_n amb $(n, Np) = 1$ (i que és un $\mathbb{Z}$-mòdul). Considerem l'àlgebra de Hecke residual $\overline{\mathbb{T}}_{\mathbb{F}_p} := \mathbb{T}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{F}_p$. Aleshores, el fet que l'àlgebra de Hecke $\overline{\mathbb{T}}_{\mathbb{F}_p}$ mod p sigui semisimple pot ser conseqüència de tres fenòmens ([MW11]): congruències entre $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-classes de conjugació de formes noves, ramificació en p dels cossos de coeficients de formes noves i que el p-índex de l'anell de coeficients local en l'anell d'enters del cos local de coeficients sigui més gran que 1. Les conseqüències del primer fenomen seran estudiades profundament en el capítol 3 d'aquesta tesi.

Sigui $f(z) = \sum_{n=0}^{\infty} a_n(f) q^n \in \mathrm{S}_k(N;\mathbb{C})$ una forma pròpia de Hecke normalitzada els coeficients de la qual viuen en cert anell d'enters d'un cos de nombres, i denotem per $\overline{\rho}_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_q)$ la representació de Galois mod p associada i que sabem que és semisimple i únicament determinada pels coeficients de f mod p, per a primers $\ell \nmid Np$, i on $\mathbb{F}_q$ és el cos finit generat pels $a_\ell(f)$ mod p. Posem $\overline{\mathbb{T}}_{\mathbb{F}_q} := \mathbb{T}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{F}_q$. Considerem l'homomorfisme d'anells

$$\begin{array}{rccl} \overline{\lambda}_f : & \overline{\mathbb{T}}_{\mathbb{F}_q} & \to & \mathbb{F}_q \\ & T_n & \mapsto & a_n(f) \bmod p \end{array}$$

i sigui $\mathfrak{m}_f := \ker(\overline{\lambda}_f)$, que és un ideal maximal de $\overline{\mathbb{T}}_{\mathbb{F}_q}$. Denotem per $\overline{\mathbb{T}}_{\mathfrak{m}_f}$ la localització de $\overline{\mathbb{T}}_{\mathbb{F}_q}$ en $\mathfrak{m}_f$. Aleshores $\overline{\mathbb{T}}_{\mathfrak{m}_f}$ és una $\mathbb{F}_q$-àlgebra local, commutativa i de dimensió finita. Si a més suposem que la representació de Galois residual $\overline{\rho}_f$ és absolutament irreductible, pel Teorema 3 de [Car94], tenim una representació de Galois contínua

$$\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{T}}_{\mathfrak{m}_f})$$

tal que $\overline{\rho}_f = \pi \circ \rho_f$, on π estén la projecció natural $\pi : \mathbb{T}_{\mathfrak{m}_f} \to \mathbb{F}_q$. En aquest context, sorgeix l'interès de saber quina és la imatge de ρ_f. En els capítols 2 i 3 veurem com calcular aquesta imatge a partir del coneixement de la imatge de $\overline{\rho}$ i alguna condició addicional.

Una altra aplicació important d'aquestes àlgebres de Hecke mod p és que ens poden donar informació sobre certes extensions abelianes de cossos de nombres. Les representacions de Galois que investiguem es corresponen amb extensions abelianes de cossos de nombres no resolubles molt grans que els mètodes actuals no permeten tractar computacionalment. En el capítol 4 veurem que els mètodes que desenvolupem en els capítols anteriors per tractar les extensions de grups que ens apareixen ens permeten fer aquestes extensions (parcialment) més accessibles.

A l'altra banda del programa de Langlands ens trobem de manera natural amb les corbes de Shimura, una generalització natural de les corbes modulars clàssiques. Aquestes corbes algebraiques i el seu poder aritmètic van ser estudiats per Shimura durant els anys 60, recolzant-se en treballs previs de Fricke, Klein i Poincaré. A la segona part d'aquest manuscrit tractarem corbes de Shimura i les seves uniformitzacions.

De la mateixa manera que les corbes modulars, les corbes de Shimura admeten uniformitzacions complexes i p-àdiques. Encara que la uniformització complexa de corbes de Shimura és més difícil d'enfocar computacionalment degut a la manca de cúspides, varis treballs recents han esquivat aquesta dificultat i han fet aquests càlculs més accessibles (veure, per exemple, [AB04], [BT07], [BT08], [Nua15], [Voi06] i [VW11]). La teoria de la uniformització p-àdica de corbes de Shimura té com a fonaments els teoremes essencials de Čerednik a [Cer76] i de Drinfel'd a [Dri76]. Aquestes uniformitzacions no arquimedianes descriuen models enters p-àdics de corbes de Shimura associades a àlgebres de quaternions indefinides de discriminant Dp, juntament amb la seva fibra especial de mala reducció, utilitzant el llenguatge de la geometria analítica rígida. Hi ha també alguns treballs que prenen un enfocament computacional a la uniformització p-àdica de corbes de Shimura mitjançant el càlcul dels seus punts especials, per exemple [DP06], [Gre06] i [Gre09]. Resultats més recents en aquesta direcció es poden trobar a [FM14], on els autors descriuen un algoritme per calcular el graf de reducció amb longituds d'una corba de Shimura associada a un ordre d'Eichler arbitrari.

A la segona part d'aquesta tesi donarem alguns resultats sobre aquestes uniformitzacions p-àdiques que són vàlides per a algunes famílies infinites de corbes de Shimura i que són abordables des d'un punt de vista computacional. Els nostres resultats sorgeixen de dues fonts d'inspiració. La primera és el treball clàssic de Hurwitz de l'any 1896 ([Hur96]), on l'autor introdueix els quaternions de Hurwitz i prova un resultat de descomposició única anàlog al que hi ha per als enters de Gauß. Utilitzant aquesta unicitat aleshores pot demostrar la coneguda fórmula pel nombre de representacions d'un enter no negatiu com a suma de quatre quadrats. El segon treball és l'article més recent de Gerritzen i van der Put [GvdP80], on estudien corbes de Mumford que recobreixen corbes de Shimura de discriminant $2p$ i nivell $N = 1$. La combinació i generalització d'aquests dos treballs ens porta a l'estudi de la uniformització d'algunes famílies de corbes de Shimura mitjançant l'estudi de certes corbes de Mumford que les recobreixen. Concretament, considerarem corbes de Shimura $X(Dp, N)$ de discriminant Dp i nivell N tals que l'orde d'Eichler de nivell N associat contingut dins l'àlgebra de quaternions definida de discriminant D té nombre de classes d'ideals $h(D, N)$ igual a 1.

Sigui $G \subseteq \mathrm{PGL}_2(\mathbb{Q}_p)$ un grup finitament generat i discontinu. Aleshores és possible trobar un subgrup normal $\Gamma \subseteq G$ d'índex finit que és lliure de torsió. En particular, aquest subgrup Γ és un grup de Schottky p-àdic. La importància dels grups de Schottky p-àdics es troba en el fet ens proporcionen la uniformització p-àdica de corbes de Mumford. Donat un grup de Schottky $\Gamma \subseteq \mathrm{PGL}_2(\mathbb{Q}_p)$, Mumford mostra com associar-hi una corba de Mumford $\mathcal{C}_\Gamma$ (cf. Teorema 3.3 i Corol·lari 4.11 de [Mum72]). La corba $\mathcal{C}_\Gamma$ està determinada de manera única, llevat d'isomorfisme, per la classe de conjugació del grup de Schottky dins $\mathrm{PGL}_2(\mathbb{Q}_p)$. En particular, quan aquest grup és un grup cocompacte, el graf de reducció estable de $\mathcal{C}_\Gamma$ respecte del model estable associat a Γ és el graf finit $\Gamma \setminus \mathcal{T}_p$, on $\mathcal{T}_p$ denota l'arbre de Bruhat-Tits associat a $\mathrm{PGL}_2(\mathbb{Q}_p)$.

El teorema de Čerednik-Drinfel'd proporciona una manera de descriure el conjunt de $\mathbb{Q}_{p^2}$-punts de la corba algebraica $X(Dp, N)$ com a quocient del semiplà superior p-àdic $\mathcal{H}_p$ per l'acció d'un subgrup cocompacte discret $\Gamma_{p,+} \subseteq \mathrm{PGL}_2(\mathbb{Q}_{p^2})$. A més, el graf de reducció de la fibra especial del model integral de Drinfel'd és el graf quocient $\Gamma_{p,+} \setminus \mathcal{T}_p$. Per tant, la teoria de la uniformització p-àdica de corbes de Shimura ens porta a considerar certs subgrups de $\mathrm{PGL}_2(\mathbb{Q}_p)$ cocompactes i discrets. El problema és que, en general, aquests grups ja no són lliures de torsió. No obstant, com hem dit abans, és possible trobar un subgrup normal que sigui lliure de torsió. A més, pel Teorema

1 de [Ger74], sabem que sempre es pot trobar un sistema de generadors per a un grup de Schottky Γ de manera que existeixi un domini fonamental *bo* per a Γ respecte aquest sistema. A [MR15] mostren com trobar, computacionalment, generadors en *bona posició* per a un grup de Schottky qualsevol. El principal objectiu de la segona part d'aquesta tesi és presentar un resultat en aquest context que mostra, de manera molt concreta, com trobar generadors de manera explícita per a aquests grups de Schottky. Per fer-ho, utilitzarem aritmètica modular en l'àlgebra de quaternions definida associada a la corba de Shimura en qüestió. A més, ho fem de manera que ens permetrà descriure fàcilment el graf de reducció estable de la corba de Mumford que recobreix la corba de Shimura p-àdica.

A continuació fem un resum de la tesi i resumim els resultats importants.

A la primera part del document veurem com un estudi detallat de les àlgebres de Hecke mod p ens permet obtenir resultats sobre la imatge de certes representacions de Galois que prenen valors en àlgebres de Hecke locals mod p. Això ens portara a deduir l'existència d'extensions abelianes p-elementals de cossos de nombres grans que no són accessibles computacionalment en l'actualitat.

El capítol 1 és un capítol introductori per a la primera part de la tesi. Està dividit en tres seccions. Comencem per donar una breu introducció a la teoria d'àlgebres de Hecke mod p i de formes modulars mod p. Després expliquem com, gràcies a un resultat de Carayol a [Car94] podem associar una representació de Galois ρ_f a una àlgebra de Hecke local $\mathbb{T}_f$ mod p sobre un cos finit $\mathbb{F}_q$ de característica p, sota la hipòtesi que la representació de Galois residual $\overline{\rho}_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_q)$ sigui absolutament irreductible. Finalment, com que estem interessats en calcular la imatge de ρ_f, incloem una secció sobre imatges de representacions de Galois residuals.

Al capítol 2 estenem un resultat de J. Manoharmayum (cf. [Man15]) a subgrups de $\mathrm{GL}_n(A)$, on A denota un anell noetherià local i complet amb cos residual k. Més concretament, sigui $W(k)$ l'anell de vectors de Witt d'un cos finit k de característica p. Denotem per $T : k \hookrightarrow W(k)$ l'alçament de Teichmüller i denotem per $W(k)_A$ la imatge de l'homomorfisme local natural $\iota : W(k) \to A$. Per a un subgrup $D \subseteq \mathbb{F}_q^\times$ considerem els grups següents:

$$\mathrm{GL}_n^D(W(k)_A) := \{g \in \mathrm{GL}_n(W(k)_A) \mid \det(g) \in \iota(T(D))\},$$

$$\mathrm{GL}_n^D(\mathbb{F}_q) := \{g \in \mathrm{GL}_n(\mathbb{F}_q) \mid \det(g) \in D\}.$$

Utilitzant tècniques similars a [Man15], demostrem el resultat següent.

Teorema. *Sigui $(A, \mathfrak{m}_A)$ un anell noetherià local complet amb ideal maximal $\mathfrak{m}_A$ i cos residual $A/\mathfrak{m}_A$ finit de característica p. Denotem per $\pi : A \to A/\mathfrak{m}_A$ la projecció natural. Suposem que tenim donat un subcòs k de $A/\mathfrak{m}_A$ i un subgrup tancat G de $\mathrm{GL}_n(A)$. Suposem que el cos k té com a mínim 4 elements i que $k \neq \mathbb{F}_5$ si $n = 2$ i $k \neq \mathbb{F}_4$ si $n = 3$. Suposem que $\pi(G) \supseteq \mathrm{GL}_n^D(k)$. Aleshores G conté un conjugat de $\mathrm{GL}_n^D(W(k)_A)$.*

Aquest resultat resulta ser de molta utilitat per als nostres propòsits, ja que com a conseqüència obtenim el corol·lari següent, que utilitzem fortament en el capítol 3.

Corol·lari. *Sigui k un cos finit de característica p i cardinalitat com a mínim 4, $k \neq \mathbb{F}_5$ si $n = 2$ i $k \neq \mathbb{F}_4$ si $n = 3$. Sigui $(A, \mathfrak{m}_A)$ una k-algebra local i commutativa de dimensió finita amb cos residual k i $\mathfrak{m}_A^2 = 0$. Sigui $G \subseteq \mathrm{GL}_n^D(A)$ un subgrup. Suposem que $G \mod \mathfrak{m}_A = \mathrm{GL}_n^D(k)$.*

Aleshores existeix un $\mathbb{F}_p[\mathrm{GL}_n^D(k)]$-submòdul $M \subseteq \mathrm{M}_n^0(\mathfrak{m}_A)$ tal que G és, llevat de conjugació per un element $u \in \mathrm{GL}_n(A)$ amb $\pi(u) = 1$, un producte semi-directe (no torçat) de la forma

$$G \simeq M \rtimes \mathrm{GL}_n^D(k).$$

En el capítol 3 estudiem representacions de Galois contínues

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T})$$

on $(\mathbb{T}, \mathfrak{m})$ denota una àlgebra commutativa local de dimension finita sobre un cos de nombres $\mathbb{F}_q$ de característica p, equipat amb la topologia discreta i amb $\mathbb{F}_q$ com a cos residual. Les representacions residuals $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ d'aquestes representacions de Galois són ben conegudes, i després del teorema de modularitat de Serre podem associar, a les que són irreductibles, una forma pròpia normalitzada de nivell, pes i caràcter prescrits. També es pot calcular explícitament la imatge d'aquestes representacions residuals (veure per exemple [Ann13]). Estarem particularment interessats en el cas $\mathrm{Im}(\overline{\rho}) = \mathrm{GL}_2^D(\mathbb{F}_q)$, on $D \subseteq \mathbb{F}_q^\times$ indica la imatge del determinant de $\overline{\rho}$. Denotem per $\mathrm{M}_2^0(\mathbb{F}_q)$ el grup de matrius amb coeficients a $\mathbb{F}_q$ i traça 0. En aquesta situació, demostrem el resultat següent.

Teorema. *Denotem per $\mathbb{F}_q$ un cos finit de característica p i $q = p^d$ elements, i suposem que $q \neq 2, 3, 5$. Sigui $(\mathbb{T}, \mathfrak{m}_{\mathbb{T}})$ una $\mathbb{F}_q$-àlgebra commutativa local de dimensió finita equipada amb la topologia discreta, i amb cos residual $\mathbb{T}/\mathfrak{m} \simeq \mathbb{F}_q$. Suposem que $\mathfrak{m}^2 = 0$. Sigui Γ un grup profinit i sigui $\rho : \Gamma \to \mathrm{GL}_2(\mathbb{T})$ una representació contínua tal que*

(a) $\mathrm{Im}(\rho) \subseteq \mathrm{GL}_2^D(\mathbb{T})$, *on $D \subseteq \mathbb{F}_q^\times$ és un subgrup.*

(b) $\mathrm{Im}(\overline{\rho}) = \mathrm{GL}_2^D(\mathbb{F}_q)$, *on $\overline{\rho}$ denota la reducció $\rho \bmod \mathfrak{m}$.*

(c) *$\mathbb{T}$ està generada com a $\mathbb{F}_q$-àlgebra pel conjunt de traces de ρ.*

Sigui $m := \dim_{\mathbb{F}_q} \mathfrak{m}$ i sigui t el nombre de traces diferents de $\mathrm{Im}(\rho)$.

(i) *Si $p \neq 2$, aleshores $t = q^{m+1}$ i*

$$\mathrm{Im}(\rho) \simeq \underbrace{(\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q))}_{m} \rtimes \mathrm{GL}_2^D(\mathbb{F}_q) \simeq \mathrm{GL}_2^D(\mathbb{T}).$$

(ii) *Si $p = 2$, aleshores*

$$t = q^\alpha \cdot ((q-1)2^\beta + 1), \text{ per a certs } 0 \leq \alpha \leq m \text{ i } 0 \leq \beta \leq d(m-\alpha) \text{ únics,}$$

i en aquest cas $\mathrm{Im}(\rho) \simeq M \rtimes \mathrm{SL}_2(\mathbb{F}_q)$, on M és un $\mathbb{F}_2[\mathrm{SL}_2(\mathbb{F}_q)]$-submòdul de $\mathrm{M}_2^0(\mathfrak{m})$ de la forma

$$M \simeq \underbrace{\mathrm{M}_2^0(\mathbb{F}_q) \oplus \ldots \oplus \mathrm{M}_2^0(\mathbb{F}_q)}_{\alpha} \oplus \underbrace{C_2 \oplus \cdots \oplus C_2}_{\beta},$$

on $C_2 \subseteq \mathbb{S}$ és un subgrup de 2 elements de les matrius escalars. A més, M està determinat de manera única per t, llevat d'isomorfisme.

Després apliquem aquest teorema a exemples concrets que provenen de formes modulars, i resumim els resultats en vàries taules. Un estudi d'aquestes taules ens permet establir algunes conjectures sobre la imatge de les representacions de Galois $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{T}}_{\mathfrak{m}_f})$ corresponents provinents de formes modulars mod 2.

Al capítol 4 traduïm els resultats anteriors a resultats sobre l'aritmètica de certes extensions abelianes p-elementals de cossos de nombres. La descripció explícita que donem al capítol 3 de la imatge de $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T})$ ens permet calcular certa part de cert cos de classes radials del cos K tallat per $\overline{\rho}$. En particular, si $p \neq 2$ demostrem que K admet una extensió abeliana p-elemental de grau p^{3dm}, on d denota el grau de $\mathbb{F}_q$ i $m = \dim_{\mathbb{F}_q} \mathfrak{m}/\mathfrak{m}^2$. Quan la característica és $p = 2$, provem que K admet una extensió abeliana 2-elemental de grau $2^{3d\alpha+\beta}$, on α i β depenen del nombre de traces diferents de $\mathrm{Im}(\rho)$, tal com explica el teorema anterior.

Finalment, en aquest capítol incloem una secció amb preguntes que sorgeixen de manera natural en aquest context, i que indiquen una possible direcció per a continuar investigant.

La part II es la continuació d'un projecte comú amb Piermarco Milione, que va ser començat a la seva tesi [Mil16], també sota la direcció de la Dra. Pilar Bayer. Una versió adaptada es pot trobar a [AM16]. En aquesta part donem una descripció explícita dels dominis fonamentals associats a la uniformització p-àdica de famílies de corbes de Shimura de discriminant Dp i nivell $N \geq 1$, per als quals $h(D, N) = 1$.

En el capítol 5 introduïm el semiplà superior p-àdic i també l'arbre de Bruhat-Tits, juntament amb l'aplicació de reducció que l'identifica amb la reducció d'aquesta varietat analítica rígida. També resumim els resultats de la teoria de corbes de Mumford que necessitem per als capítols que segueixen i els relacionem amb la uniformització p-àdica de corbes de Shimura.

Al capítol 6 introduïm breument el lector a la teoria de l'aritmètica d'àlgebres de quaternions. Desenvolupem algunes eines en el context de l'aritmètica modular d'ordres d'Eichler $\mathcal{O}$ sobre $\mathbb{Z}$ amb $h(D, N) = 1$ en una àlgebra de quaternions definida H. Ens interessen en particular els quocients de la forma $\mathcal{O}/\xi\mathcal{O}$, on $\xi\mathcal{O}$ és un ideal principal enter a la dreta. Estenem la noció de *quaternions primaris* introduïda a [Hur96] per l'órdre de quaternions de Hurwitz a ordres d'Eichler $\mathcal{O}$ sobre $\mathbb{Z}$ amb $h(D, N) = 1$. Aquesta noció resulta ser crucial per tal de demostrar un resultat de descomposició única en aquests ordres d'Eichler, un resultat que estén el *Zerlegungsatz* pels quaternions de Hurwitz. En efecte, quan fixem un quaternió $\xi \in \mathcal{O}$ que satisfà certa propietat (que anomenem *propietat de les unitats a la dreta*, cf. la Definició 6.2.5), qualsevol quaternió $\alpha \in \mathcal{O}$ és associat a un quaternió ξ-primari (cf. Definició 6.2.3), i.e. existeix una única unitat (llevat de signe si $2 \in \xi\mathcal{O}$) $\varepsilon \in \mathcal{O}^\times$ tal que $\varepsilon\alpha$ és ξ-primari. Aquest fet ens permet centrar-nos només en la descomposició dels quaternions ξ-primaris, i demostrar el resultat següent.

Theorem. *Sigui H una àlgebra de quaternions definida de discriminant D i sigui $\mathcal{O}$ un ordre d'Eichler sobre $\mathbb{Z}$ de nivell N amb $h(D, N) = 1$. Sigui $\xi \in \mathcal{O}$ un quaternió enter tal que el grup quocient abelià $\mathcal{O}/\xi\mathcal{O}$ conté un conjunt de classes ξ-primàries $\mathcal{P}$. Sigui $\alpha \in \mathcal{O}$ un quaternió primitiu i ξ-primari respecte $\mathcal{P}$ tal que la seva norma descompon en factors primers*

$$\mathrm{Nm}(\alpha) = p_1 \cdot \ldots \cdot p_s.$$

Llavors α admet una descomposició en quaternions irreductibles, primitius i ξ-primaris respecte $\mathcal{P}$:

$$\alpha = \pi_1 \cdot \ldots \cdot \pi_s$$

amb $\mathrm{Nm}(\pi_i) = p_i$*, per a cada* $1 \leq i \leq s$*. A més, si* $2 \notin \xi\mathcal{O}$ *aquesta descomposició és única, i si* $2 \in \xi\mathcal{O}$*, la descomposició és única llevat de signe.*

Aquest teorema ens serà molt útil al capítol 7, on trobarem generadors pels grups de Schottky que sorgeixen de la uniformització p-àdica de corbes de Shimura.

En el capítol 7 apliquem els resultats aritmètics obtinguts en el capítol anterior per tal de demostrar el resultat principal d'aquesta part de la tesi. Aquest resultat dóna una manera concreta i explícita per trobar generadors per a certs grups de Shottky que provenen de grups de quaternions p-àdics que uniformitzen corbes de Shimura p-àdiques. Els resultats principals d'aquest capítol (Teorema 7.1.5 i Corol·lari 7.2.3) es poden resumir en el resultat següent.

Teorema. *Sigui* $X(Dp, N)$ *una corba de Shimura associada a un ordre d'Eichler de nivell* N *dins l'àlgebra de quaternions indefinida de discriminant* Dp*, i sigui* $\mathcal{O}$ *un ordre d'Eichler de nivell* N *dins l'àlgebra de quaternions definida de discriminant* Dp*. Suposem que*

(*i*) $h(D, N) = 1$.

(*ii*) *Existeix* $\xi \in \mathcal{O}$ *tal que* $2 \in \xi\mathcal{O}$ *i l'aplicació*

$$\varphi : \mathcal{O}^\times/\mathbb{Z}^\times \to (\mathcal{O}/\xi\mathcal{O})_r^\times, \quad \varphi(u) = \lambda_r(u + \mathrm{Nm}(\xi)\mathcal{O})$$

és una bijecció, on $(\mathcal{O}/\xi\mathcal{O})_r^\times$ *denota la image de* $(\mathcal{O}/\mathrm{Nm}(\xi)\mathcal{O})^\times$ *sota la projecció natural* $\lambda_r : \mathcal{O}/\mathrm{Nm}(\xi)\mathcal{O} \twoheadrightarrow \mathcal{O}/\xi\mathcal{O}$.

(*iii*) *El nombre primer* p *satisfà*

$$t(p) := \#\{\alpha \in \mathcal{O} \mid \mathrm{Nm}(\alpha) = p,\, \alpha - 1 \in \xi\mathcal{O},\, \mathrm{Tr}(\alpha) = 0\} = 0.$$

Aleshores existeix una corba de Mumford C *que recobreix la corba de Shimura* $X(Dp, N) \otimes_{\mathbb{Q}} \mathbb{Q}_p$ p*-àdica tal que:*

(*a*) *la corba* C *té gènere* $(p + 1)/2$,

(*b*) *el grau del recobriment és* $\#\mathcal{O}^\times/\mathbb{Z}^\times$,

(*c*) *un conjunt finit de generadors per al grup de Schottky que uniformitza la corba de Mumford* C *ve donada per la imatge, dins* $\mathrm{PGL}_2(\mathbb{Q}_p)$*, del conjunt de matrius escalars*

$$\widetilde{S} := \Phi_p(\{\alpha \in \mathcal{O} \mid \mathrm{Nm}(\alpha) = p,\, \alpha - 1 \in \xi\mathcal{O}\}) \subseteq \mathrm{GL}_2(\mathbb{Q}_p),$$

on Φ_p *denota una immersió matricial de l'àlgebra de quaternions definida dins* $\mathrm{M}_2(\mathbb{Q}_p)$.

A la taula 6.1 mostrem un quaternió $\xi \in \mathcal{O}$ que satisfà la condició (*ii*) per a cada àlgebra de quaternions definida amb $h(D, N) = 1$, excepte pels casos $(D, N) = (2, 5)$ i $(7, 1)$, per als quals aquest quaternió no existeix.

És interessant remarcar que la condició (*a*) del teorema és conseqüència d'un resultat que provem relacionat amb el nombre de representacions del primer p per una forma quadràtica quaternària amb alguna condició de congruència en els coeficients.

Teorema. *Sigui $\xi \in \mathcal{O}$ un quaternió que satisfà la condició a (ii) del teorema anterior. aleshores el conjunt finit*

$$\{\alpha \in \mathcal{O} \mid \mathrm{Nm}(\alpha) = p,\ \alpha - 1 \in \xi\mathcal{O}\}$$

té cardinalitat $2(p+1)$.

Utilitzant aquests resultats som capaços de construir dominis fonamentals bons per a les corbes de Mumford associades i, com a conseqüència, d'obtenir també els grafs de reducció estable per a aquestes corbes.

En el capítol 8 mostrem com l'estudi detallat que hem fet de la corba de Shimura p-àdica com a varietat analítica rígida ens permet obtenir, fàcilment, fórmules que descriuen els grafs de reducció amb longituds d'aquestes corbes de Shimura, així com també fórmules per als seus gèneres i per al gènere de certs quocients d'Atkin-Lehner.

Finalment, en el capítol 9 describim un algoritme que hem implementat en Magma que calcula el graf de reducció descrit anteriorment, per tal de fer el nostre mètode efectiu. Mostrem com calcular, en exemples concrets, sistemes lliures de generadors per a grups de Schottky com en el teorema anterior, un domini fonamental p-àdic bo per a l'acció del grup de Schottky en $\mathcal{H}_p$ i el seu graf de reducció estable.

Bibliography

[AB04] M. Alsina and P. Bayer, *Quaternion orders, quadratic forms, and Shimura curves*, CRM Monograph Series, vol. 22, AMS, 2004. ↑(document), 7.1.3, 9.2

[AM16] Laia Amorós and Piermarco Milione, *Mumford curves covering p-adic Shimura curves and their fundamental domains*, 2016. http://arxive.org/abs/1608.04891. ↑(document), 9.2

[Ann13] Samuele Anni, *Images of Galois representations*, PhD Thesis, Université Bordeaux I (2013). ↑(document), 1.3, 1.3, 9.2

[BC91] J.-F. Boutot and H. Carayol, *Uniformisation p-adique des courbes de Shimura: les théorèmes de Čerednik et de Drinfeld*, Astérisque **196-197** (1991), 45–158. Courbes modulaires et courbes de Shimura (Orsay, 1987/1988). ↑5.2, 5.2.5, 5.2

[BCP97] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system I: The user language*, J. Symbolic Comput. **24** (1997), 235–265. ↑9

[BGR84] S. Bosch, U. Güntzer, and R. Remmert, *Non-archimedean analysis: a systematic approach to rigid analytic geometry*, Grundlehren der mathematischen Wissenschaften, vol. 261, Springer, 1984. ↑5.1, 5.1

[Bos14] S. Bosch, *Lectures on formal and rigid geometry*, Lectures Notes in Mathematics, vol. 2105, Springer, 2014. ↑5.3

[BT07] P. Bayer and A. Travesa, *Uniformizing functions for certain Shimura curves, in the case $D = 6$*, Acta Arithmetica **126** (2007), 315–339. ↑(document), 9.2

[BT08] ———, *On local constants associated to arithmetical automorphic functions*, Pure and Applied Mathematics Quaterly. Special Issue: In honor of Jean-Pierre Serre **1** (2008), 1107–1132. ↑(document), 9.2

[Car94] Henri Carayol, *Formes modulaires et représentations galoisiennes à valeurs dans un anneau local complet*, Contemporary Mathematics **165** (1994), 213–237. ↑(document), 1, 1.2, 9.2

[Cer76] I. V. Cerednik, *Uniformization of algebraic curves by discrete arithmetic subgroups of $\mathrm{PGL}_2(k_w)$ with compact quotients*, Math. USSR Sbornik **29** (1976), no. 1, 55–78. ↑(document), 5.3, 9.2

[CR00] Charles W. Curtis and Irving Reiner, *Representation theory of finite groups*, AMS Chelsea Publishing, 2000. ↑2.2

[CR81] ———, *Methods of representation theory*, Vol. I, John Wiley & Sons, Inc., 1981. ↑2.2, 3.2

[DDT94] H. Darmon, F. Diamond, and R. Taylor, *Fermat's last theorem*, Current Developments in Mathematics (Cambridge, Mass., 1995), International Press, Cambridge, Mass. (1994), 1–154. ↑1, 1.1

[DI95] Fred Diamond and John Im, *Modular forms and modular curves*, Canadian Mathematical Society **17** (1995), no. 39-133. ↑1

[DP06] H. Darmon and R. Pollack, *The efficient calculation of Stark-Heegner points via overconvergent modular symbols*, Israel J. Math. **153** (2006), 319–354. ↑(document), 9.2

[Dri76] V. G. Drinfeld, *Coverings of p-adic symmetric regions*, Functional Analysis and Its Applications **10** (1976), no. 2, 107–115. ↑(document), 5.3, 9.2

[DS74] Pierre Deligne and Jean-Pierre Serre, *Formes modulaires de poids 1*, Annales scientifiques de l'É.N.S 4^e série **7** (1974), no. 4, 507–530. ↑1.2

[DT07] S. Dasgupta and J. Teitelbaum, *The p-adic upper half-plane*, Chapter in p-adic Geometry, Lectures from the 2007 Arizona WInter School **45** (2007), 65–122. ↑5.2.5

[Eic38a] M. Eichler, *Allgemeine Kongruenzklasseneinteilungen der Ideale einfachen Algebren über algebraischen Zahlkörpen und ihre L-Reihen*, J. Reine Angew. Math. **179** (1938), 227–251. ↑6.1

[Eic38b] ———, *Über die Idealklassenzahl total definiter Quaternionenalgebren*, Math. Z. **43** (1938), no. 1, 102–109. ↑6.1

[Eis95] David Eisenbud, *Commutative algebra*, Springer-Verlag, New York, 1995. ↑3.1, 3.2

[FM14] C. Franc and M. Masdeu, *Computing fundamental domains for the Bruhat-Tits tree for* $\mathrm{GL}_2(\mathbb{Q}_p)$*, p-adic automorphic forms, and the canonical embedding of Shimura curves*, LSM Journal of Computation in Mathematics **17** (2014), no. 01, 1–23. ↑(document), 8, 9.2

[Ger74] L. Gerritzen, *Zur nichtarquimedischen Uniformisierung von Kurven*, Math. Ann. **210** (1974), 321–337. ↑(document), 5.4.5, 7.2, 9.2

[Gre06] M. Greenberg, *Heegner point computations via numerical p-adic integration*, Algorithmic Number Theory (2006), 361–376. ↑(document), 9.2

[Gre09] ———, *Computing Heegner points arising from Shimura curve parametrizations*, Clay Mathematics Proceedings **8** (2009). ↑(document), 9.2

[GvdP80] L. Gerritzen and M. van der Put, *Schottky groups and Mumford curves*, Lecture Notes in Mathematics, vol. 817, Springer, 1980. ↑(document), 5, 5.4.5, 5.4, 7.1.2, 7.2.4, 8.2, 8.2, 8.3, 8.3.4, 9.2

[Hur96] A. Hurwitz, *Über die Zahlentheorie der Quaternionen*, Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse **1896** (1896), 313–340. ↑(document), 6, 6.2, 6.2, 6.3, 7, 7.1.3, 9.2

[JL84] B. W. Jordan and R. A. Livné, *Local diophantine properties of Shimura curves*, Math. Ann. **270** (1984), no. 2, 235–248. ↑5.3, 8.1

[Kur79] A. Kurihara, *On some examples of equations defining Shimura curves and the Mumford uniformization*, J. Fac. Sci. Univ. Tokyo, Sect. IA Math **25** (1979), no. 3, 277–300. ↑5.2.2, 8.1.6

[KV10] M. Kirschmer and J. Voight, *Algorithmic enumeration of ideal classes for quaternion orders*, SIAM J. Comp. **39** (2010), no. 10, 1714–1747. ↑6.2

[KW09a] C. Khare and J.-P. Wintenberger, *Serre's modularity conjecture (i)*, Invent. Math. (2009). ↑(document), 9.2

[KW09b] ———, *Serre's modularity conjecture (ii)*, Invent. Math. (2009). ↑(document), 9.2

[Lan76] Serge Lang, *Introduction to modular forms*, Springer-Verlag, Berlin, 1976. ↑1.3

[LS02] Joan-Carles Lario and René Schoof, *Some computations with Hecke rings and deformation rings*, Experiment. Math. **11** (2002), no. 2, 303–311. ↑1.3

[Man15] Jayanta Manoharmayum, *A structure theorem for subgroups of* GL_n *over complete local noetherian rings with large residual image*, Proceedings of the American Mathematical Society **143** (2015July), no. 7, 2743–2758. ↑(document), 2, 2.1, 2.2, 2.2, 2.3, 2.4, 2.4, 2.4, 2.4, 9.2

[Mat86] Hideyuki Matsumura, *Commutative ring theory*, Cambride University Press, 1986. ↑2.1

[Mil16] P. Milione, *Shimura curves and their p-adic uniformizations*, PhD Thesis, Universitat de Barcelona (2016). ↑(document), 9.2

[MR15] R. Morrison and Q. Ren, *Algorithms for Mumford curves*, Journal of Symbolic Computation **68** (2015), 259–284. ↑(document), 7.2, 9.2

[Mum72] D. Mumford, *An analytic construction of degenerating curves over complete local rings*, Compositio Math. **24** (1972), 129–174. ↑(document), 5, 5.2, 5.4, 9.2

[MW11] M. Mohyla and G. Wiese, *A computational study of the asymptotic behaviour of coefficient fields of modular forms*, Publ. Math. Besancon Algèbre Théorie Nr (2011), 75–89. ↑(document), 9.2

[Nua15] J. Nualart, *On the hyperbolic uniformization of Shimura curves with an Atkin-Lehener quotient of genus* 0, PhD Thesis, Universitat de Barcelona, 2015. ↑(document), 9.2

[Ram16] S. Ramanujan, *On certain arithmetical functions*, Trans. Cambridge Phil. Soc. **22** (1916), 159–184. ↑(document), 9.2

[Rap13] A. S. Rapinchuk, *Strong approximation for algebraic groups*, Thin groups and superstrong approximation, MSRI Publications **61** (2013), 269–298. ↑7.1.1

[Rib83] Kenneth A. Ribet, *Mod p Hecke Operators and Congruences Between Modular Forms*, Inventiones mathematicae **71** (1983), 193–205. ↑1.1

[Sel60] A. Selberg, *On discontinous groups in higher dimensional symmetric spaces*, Contribution to function theory, Tata Institute of Fundamental Research (1960), 147–164. ↑5.4

[Ser70] J.P. Serre, *Cours d'arithmétique*, Collection Sup, Presses Universitaires de France, 1970. ↑8.1.3

[Ser77] J. P. Serre, *Arbres, amalgames,* SL_2, Cours au Collège de France, rédigé avec la collaboration de Hyman Bass, Astérisque, vol. 46, Société Mathèmatique de France, 1977. ↑5.2, 5.2.1

[Shi67] G. Shimura, *Construction of Class Fields and Zeta Functions of Algebraic Curves*, Annals of Mathematics **85** (1967), no. 1, 58–159. ↑5.3

[Shi70] ———, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, vol. 11, Princeton University Press, 1970. ↑5.2.3, 8.2.3

[SS91] P. Schneider and U. Stuhler, *The cohomology of p-adic symmetric domains*, Inv. Math. **105** (1991), no. 1, 47–122. ↑5.1

[vdP92] M. van der Put, *Discrete groups, Mumford curves and Theta functions*, Ann. de la Fac. des Science de Toulouse **1** (1992), no. 3, 399–438. ↑8.2

[Vig80] M. F. Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics, vol. 800, Springer, 1980. ↑5.3.2, 7.1.1

[Voi06] J. Voight, *Computing CM points on Shimura curves arising from cocompact arithmetic triangle groups*, Chapter in Algorithmic Number Theory, Lecture Notes in Computer Science **4076** (2006), 406–420. ↑(document), 9.2

[VW11] J. Voight and J. Willis, *Computing power series expansions of modular forms*, Chapter in Computations with modular forms **6** (2011), 331–361. ↑(document), 9.2

[Wie06] G. Wiese, *Mod p modular forms*, 2006. ↑1, 1.1

[Wie] ———. http://math.uni.lu/∼wiese/. ↑3.3