Cover Page

Universiteit Leiden

Author: Anni, Samuele
Title: Images of Galois representations
Issue Date: 2013-10-24

Images of Galois representations

Proefschrift

ter verkrijging van
de graad van Doctor aan de Universiteit Leiden
op gezag van Rector Magnificus prof. mr. C.J.J.M. Stolker,
volgens besluit van het College voor Promoties
te verdedigen op donderdag 24 oktober 2013
klokke 11:15 uur

door

Samuele ANNI

geboren te Galliate, Italië
in 1985

Samenstelling van de promotiecommissie:

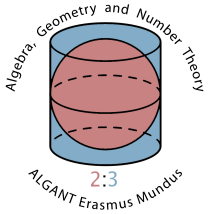
Promotores:

Prof. dr. S. J. Edixhoven
Prof. dr. P. Parent (Université Bordeaux I)

Overige leden:

dr. B. de Smit
Prof. dr. I. Kiming (Universiteit Copenhagen)
Prof. dr. P. Stevenhagen
Prof. dr. G. Wiese (Université de Luxembourg)

This work was funded by Algant-Doc Erasmus Action and was carried out at Universiteit Leiden and Université Bordeaux 1.



THÈSE

présentée à

L'UNIVERSITÉ BORDEAUX I

ÉCOLE DOCTORALE DE MATHÉMATIQUES ET INFORMATIQUE

par Samuele ANNI

POUR OBTENIR LE GRADE DE

DOCTEUR

SPECIALITÉ : Mathématiques Pures

Images des représentations galoisiennes

Directeurs de recherche :

Bas EDIXHOVEN et Pierre PARENT

Soutenue le : 24 Octobre 2013 à Leiden

Devant la commission d'examen formée de :

DE SMIT, Bart	Docteur	Universiteit Leiden	Examinateur
EDIXHOVEN, Bas	Professeur	Universiteit Leiden	Directeur
KIMING, Ian	Professeur	Universiteit Copenhagen	Rapporteur
PARENT, Pierre	Maître de Conférences	Université Bordeaux I	Directeur
PAZUKI, Fabien	Maître de Conférences	Université Bordeaux I	Examinateur
STEVENHAGEN, Peter	Professeur	Universiteit Leiden	Examinateur
WIESE, Gabor	Professeur	Université de Luxembourg	Rapporteur

Images of Galois representations

ABSTRACT (short version)

In this thesis we investigate 2-dimensional, continuous, odd, residual Galois representations and their images. This manuscript consists of two parts.

In the first part of this thesis we analyse a local-global problem for elliptic curves over number fields. Let E be an elliptic curve over a number field K, and let ℓ be a prime number. If E admits an ℓ-isogeny locally at a set of primes with density one then does E admit an ℓ-isogeny over K?

The study of the Galois representation associated to the ℓ-torsion subgroup of E is the crucial ingredient used to solve the problem. We characterize completely the cases where the local-global principle fails, obtaining an upper bound for the possible values of ℓ for which this can happen.

In the second part of this thesis, we outline an algorithm for computing the image of a residual modular 2-dimensional semi-simple Galois representation. This algorithm determines the image as a finite subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$, up to conjugation, as well as certain local properties of the representation and tabulate the result in a database.

In this part of the thesis we show that, in almost all cases, in order to compute the image of such a representation it is sufficient to know the images of the Hecke operators up to the Sturm bound at the given level n. In addition, almost all the computations are performed in positive characteristic.

In order to obtain such an algorithm, we study the local description of the representation at primes dividing the level and the characteristic: this leads to a complete description of the eigenforms in the old-space. Moreover, we investigate the conductor of the twist of a representation by characters and the coefficients of the form of minimal level and weight associated to it in order to optimize the computation of the projective image.

The algorithm is designed using results of Dickson, Khare-Wintenberger and Faber on the classification, up to conjugation, of the finite subgroups of $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$. We characterize each possible case giving a precise description and algorithms to deal with it. In particular, we give a new approach and a construction to deal with irreducible representations with projective image isomorphic to either the symmetric group on 4 elements or the alternating group on 4 or 5 elements.

Beelden van Galoisrepresentaties

Samenvatting (beknopte versie)

In dit proefschrift doen wij onderzoek naar 2-dimensionale, continue, oneven, residuele Galoisrepresentaties en hun beelden. Dit proefschrift bestaat uit twee delen.

In het eerste deel analyseren wij een lokaal-globaal probleem voor elliptische krommen over getallenlichamen. Zij E een elliptische kromme over een getallenlichaam K, en zij ℓ een priemgetal. Heeft E een ℓ-isogenie over K als deze een lokale ℓ-isogenie heeft voor een verzameling priemen met dichtheid één?

De studie van de Galoisrepresentatie die wordt toegekend aan de ℓ-torsie ondergroep van E vormt een cruciaal ingrediënt om dit probleem op te lossen. We karakteriseren alle gevallen waarin het lokaal-globaal principe niet op gaat, en we verkrijgen een bovengrens voor de waardes van ℓ waarvoor dit kan gebeuren.

In het tweede deel van dit proefschrift beschrijven we een algoritme dat de beelden van residuele 2-dimensionale Galoisrepresentaties komend van modulaire vormen uitrekent. Dit algoritme bepaalt het beeld als een eindige ondergroep van $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$, op conjugatie na, alsmede bepaalde lokale eigenschappen van de representaties en tabuleert de resultaten in een database.

In dit deel van het proefschrift tonen we aan dat het, in bijna alle gevallen, voor het uitrekenen van het beeld van zo'n representatie voldoende is om de beelden van de Hecke-operatoren tot aan de Sturmgrens te weten op een gegeven niveau n. Bovendien worden bijna alle berekeningen in positieve karakteristiek gedaan.

Om zo'n algoritme te verkrijgen, bestuderen we de lokale beschrijving van de representatie bij priemen die het niveau en de karakteristiek delen: dit geeft een volledige beschrijving van de eigenvormen in de oude ruimte. Daarnaast bestuderen we de conductor van de twists van de representatie met karakters en de coëfficiënten van de vorm van minimaal niveau en gewicht daarmee geassocieerd om de berekeningen van het projectieve beeld te optimaliseren.

Het algoritme is gebaseerd op resultaten van Dickson, Khare-Wintenberger en Faber over de classificatie van eindige ondergroepen van $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$, op conjugatie na. We karakterisen alle mogelijke gevallen door een precieze beschrijving en algoritmes te geven die ze afhandelen. In het bijzonder geven we een nieuwe benadering en een constructie die irreducibele representaties afhandelt waarvan het projectieve beeld isomorf met de symmetrische groep op 4 letters of de alternerende groep op 4 of 5 letters.

Images des représentations galoisiennes

Résumé (version brève)

Dans cette thèse, on étudie les représentations 2-dimensionnelles continues du groupe de Galois absolu d'une clôture algébrique fixée de $\mathbb{Q}$ sur les corps finis qui sont modulaires et leurs images. Ce manuscrit se compose de deux parties.

Dans la première partie, on étudie un problème local-global pour les courbes elliptiques sur les corps de nombres. Soit E une courbe elliptique sur un corps de nombres K, et soit ℓ un nombre premier. Si E admet une ℓ-isogénie localement sur un ensemble de nombres premiers de densité 1 alors est-ce que E admet une ℓ-isogénie sur K ?

L'étude de la représentation galoisienne associée à la ℓ-torsion de E est l'ingrédient essentiel utilisé pour résoudre ce problème. On caractérise complètement les cas où le principe local-global n'est pas vérifié, et on obtient une borne supérieure pour les valeurs possibles de ℓ pour lesquelles ce cas peut se produire.

La deuxième partie a un but algorithmique : donner un algorithme pour calculer les images des représentations galoisiennes 2-dimensionnelles sur les corps finis attachées aux formes modulaires.

L'un des résultats principaux est que l'algorithme n'utilise que des opérateurs de Hecke jusqu'à la borne de Sturm au niveau donné n dans presque tous les cas. En outre, presque tous les calculs sont effectués en caractéristique positive.

On étudie la description locale de la représentation aux nombres premiers divisant le niveau et la caractéristique. En particulier, on obtient une caractérisation précise des formes propres dans l'espace des formes anciennes en caractéristique positive.

On étudie aussi le conducteur de la tordue d'une représentation par un caractère et les coefficients de la forme de niveau et poids minimaux associée.

L'algorithme est conçu à partir des résultats de Dickson, Khare-Wintenberger et Faber sur la classification, à conjugaison près, des sous-groupes finis de $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$. On caractérise chaque cas en donnant une description et des algorithmes pour le vérifier.

En particulier, on donne une nouvelle approche pour les représentations irréductibles avec image projective isomorphe soit au groupe symétrique sur 4 éléments ou au groupe alterné sur 4 ou 5 éléments.

Preface

Let $\overline{\mathbb{Q}}$ be an algebraic closure of the field of rational numbers $\mathbb{Q}$, and let $G_{\mathbb{Q}}$ be the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, the automorphism group of the field $\overline{\mathbb{Q}}$.

The main objects of study in this thesis are the images of 2-dimensional continuous odd representations of the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ over finite fields, i.e. residual representations. These mathematical objects appear naturally in number theory, arithmetic geometry and representation theory.

Class field theory provides us a precise understanding of representations of degree one, or characters. By the Kronecker-Weber Theorem, a continuous character χ from $G_{\mathbb{Q}}$ to $\mathbb{C}^*$ is a Dirichlet character:

$$G_{\mathbb{Q}} \longrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \mathbb{C}^*,$$
$$\chi$$

for some integer $n \geq 1$, where ζ_n is an n-root of unity.

In this thesis we investigate 2-dimensional, continuous, odd, residual Galois representations and their images. This manuscript consists of two parts in which two different topics are studied. In each part is provided a short introduction to the problem treated. Therefore, here we underline the main new results obtained and the links between the two parts.

In the first part, we analyse a question where the study of the image of a certain 2-dimensional Galois representation is the key element to solve the problem. The second part of this thesis has a computational purpose: to give an algorithm for computing the images of 2-dimensional, continuous, odd, residual Galois representations.

The first part of this thesis is committed to analyse a local-global problem for elliptic curves over number fields. Let E be an elliptic curve over a number field K, and let ℓ be a prime number. If E admits an ℓ-isogeny locally at a set of primes with density one then does E admit an ℓ-isogeny over K?

The definition of local isogeny, for primes of good reduction and not dividing ℓ, is the natural one, and it is recalled in Definition 1.1.1. This research is motivated by a recent article of Sutherland, see [Sut12].

The study of the Galois representation associated to the ℓ-torsion subgroup of E is the crucial ingredient used to solve the problem.

Let K be a number field and E an elliptic curve over K. Assume that the j-invariant of E is different from 0 and 1728. A pair $(\ell, j(E))$ is said to be

exceptional for K if E/K admits an ℓ-isogeny locally for a set of density one of primes of K but not globally over K. In this part of the thesis we give a complete description of the set of exceptional pairs for a number field K. Part I of the thesis appears as preprint on arXiv, see [Ann13].

We also obtain an upper bound for the possible values of ℓ occurring in such pairs in terms of d, the degree of K over $\mathbb{Q}$, and Δ, the discriminant of K:

$$\ell \leq \max\{\Delta, 6d{+}1\}.$$

The main theorem of the first part of this thesis is the following:

Main Theorem. *Let K be a number field of degree d over $\mathbb{Q}$ and discriminant Δ, and let $\ell_K := \max\{\Delta, 6d{+}1\}$. The following holds:*

(1) *if $(\ell, j(E))$ is an exceptional pair for the number field K then $\ell \leq \ell_K$;*

(2) *there are only finitely many exceptional pairs for K with $7 < \ell \leq \ell_K$;*

(3) *the number of exceptional pairs for K with $\ell = 7$ is finite or infinite, according to the rank of Elkies-Sutherland's elliptic curve:*

$$y^2 = x^3 - 1715x + 33614$$

being zero or positive over K;

(4) *there exists no exceptional pair for K with $\ell = 2$ and with $\ell = 3$;*

(5) *there exist exceptional pairs for K with $\ell = 5$ if and only if $\sqrt{5}$ belongs to K. Moreover, if $\sqrt{5}$ belongs to K then there are infinitely many exceptional pairs for K with $\ell = 5$.*

Part I of this thesis is organized as follows.

For the convenience of the reader, in Chapter 1 we introduce the topic and recall the results obtained by Sutherland in [Sut12, Section 2].

In Chapter 2, we study exceptional pairs over arbitrary number fields. First we deduce the effective version of Sutherland's result, then we describe how to tackle the case not treated by Sutherland and we prove the statement (4) of the Main Theorem, see Proposition 2.1.9. Chapter 2 ends with the proof of the bound given in (1) of the Main Theorem (Corollary 2.3.5).

In Chapter 3 we prove finiteness results for the set of exceptional pairs for a number field K and we prove statements (2), (5) and (3) of the Main Theorem, see respectively Theorem 3.1.1, Corollary 3.2.2 and Proposition 3.3.1. These results are obtained studying particular modular curves and their genus, for more details see Theorem 3.1.1, Proposition 3.2.1 and Proposition 3.3.1.

In Part II of this thesis we outline an algorithm for computing the image of a residual modular 2-dimensional semi-simple Galois representation. This

means that the algorithm will determine the image as a finite subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$, up to conjugation, as well as certain local properties of the representation and tabulate the result in a database.

Let n be a positive integer, the congruence subgroup $\Gamma_1(n)$ is the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ given by

$$\Gamma_1(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : a \equiv d \equiv 1\,,\, c \equiv 0 \bmod n \right\}.$$

Let n and k be positive integers, we will denote by $S(n,k)_{\mathbb{C}}$ the complex vector space of weight k cusp forms on $\Gamma_1(n)$, see [DS05] or [DS74], and by $\mathbb{T}(n,k)$ the associated Hecke algebra, i.e. the $\mathbb{Z}$-subalgebra of $\mathrm{End}_{\mathbb{C}}(S(n,k)_{\mathbb{C}})$ generated by the Hecke operators T_p for every prime p and the diamond operators $\langle d \rangle$ for every $d \in (\mathbb{Z}/n\mathbb{Z})^*$. The Hecke algebra $\mathbb{T}(n,k)$ is finitely generated as a $\mathbb{Z}$-module, for further details see [EC11, Theorem 2.5.11] or [DS05, p.234].

The aforementioned algorithm is developed for residual modular 2-dimensional semi-simple Galois representations:

Theorem (Shimura, Deligne [DS74, Théorème 6.7]). *Let n and k be positive integers. Let $\mathbb{F}$ be a finite field, ℓ its characteristic, and $f : \mathbb{T}(n,k) \to \mathbb{F}$ a morphism of rings from the cuspidal Hecke algebra of level n and weight k to $\mathbb{F}$. Then there is a continuous semi-simple representation $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F})$ that is unramified outside $n\ell$ such that for all primes p not dividing $n\ell$ we have:*

$$\mathrm{Trace}(\rho_f(\mathrm{Frob}_p)) = f(T_p) \quad \textit{and} \quad det(\rho_f(\mathrm{Frob}_p)) = f(\langle p \rangle)p^{k-1} \quad \textit{in } \mathbb{F}.$$

Such a ρ_f is unique up to isomorphism.

One of the purposes of this research is to minimize the number of Hecke operators of which the image through the ring morphism f, as in the previous theorem, has to be computed in order to describe the image. Indeed, we focus on using as few coefficients of the underlying modular form as possible.

Let ℓ be a prime, to check equality between mod ℓ modular eigenforms of the same level and weight it is enough to compute the prime-indexed coefficients up to a certain bound which is the Sturm bound.

Two different mod ℓ modular forms can give rise to the same Galois representation: the coefficients indexed by the primes dividing the level and the characteristic may differ. Hence, either we solve this problem mapping the form to a higher level (or twisting it) and use the Sturm bound at that level, which is greater than the bound at the given level, or we study how to describe the coefficients at primes dividing the level and the characteristic so that we can list all possibilities.

In order to describe these coefficients, it is needed to know local properties of the Galois representation, i.e. the restriction of the representation to the decomposition group at the corresponding primes.

Associated to the algorithm there is a database which stores all the data obtained.

The algorithm is cumulative and built with a bottom-up approach: for any new level n, we will store in the database the system of eigenvalues at levels dividing n and weights smaller than the weight considered, so that there will be no need to re-do the computations if the representation arises from lower level or weight. In particular, the following theorem holds, for a proof and more detailed explanations see Chapter 6 herein, Theorem 6.3.6:

Theorem. *Let n, m and k be positive integers with n a multiple of m. Let ℓ be a prime not dividing n, and such that $2 \leq k \leq \ell + 1$. Let $f : \mathbb{T}(n,k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings and let $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the unique, up to isomorphism, continuous semi-simple representation corresponding to it. Let $g : \mathbb{T}(m,k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings and let $\rho_g : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the corresponding Galois representation. Let us assume that $\mathrm{N}(\rho_g) = m$ and that the weight of ρ_g is minimal. The following holds:*
- *if ρ_f is ramified at ℓ then ρ_f is isomorphic to ρ_g if and only if f is in the subspace of the old-space given by g at level n.*
- *if ρ_f is unramified at ℓ then ρ_f is isomorphic to ρ_g if and only if f is either in the subspace of the old-space given by g at level n or in the subspace of the old-space given by g' at level n, where g' is the form such that $g'(T_p) = g(T_p)$ for all primes p different from ℓ and $g'(T_\ell)$ satisfies:*

$$x^2 - \mathrm{Trace}(\rho_f(\mathrm{Frob}_\ell))x + \det(\rho_f(\mathrm{Frob}_\ell)) = (x - g(T_\ell))(x - g'(T_\ell)).$$

Similarly, if a Galois representation arises as a twist of a representation of lower conductor, the algorithm will detect such data and it will not re-do any computation to determine the projective image of the representation since it is already stored in the database.

On the other hand, once the data at a certain level is computed, the database will fill in all the contribution at higher level coming from degeneracy morphism and twisting, so that the computation at a certain level will be performed only when we are dealing with a new object.

Let us introduce shortly the design of the algorithm, this is done in details in Chapter 11.

The algorithm follows results of Dickson, Khare-Wintenberger and Faber on the classification, up to conjugation, of the finite subgroups of $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$:

Dickson's Theorem ([Dic58]). *Let $\ell \geq 3$ be a prime and H a finite subgroup of $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$. Then a conjugate of H is one of the following groups:*

- *a finite subgroup of the upper triangular matrices;*
- $\mathrm{SL}_2(\mathbb{F}_{\ell^r})/\{\pm 1\}$ *or* $\mathrm{PGL}_2(\mathbb{F}_{\ell^r})$ *for* $r \in \mathbb{Z}_{>0}$*;*
- *a dihedral group* D_{2n} *with* $n \in \mathbb{Z}_{>1}$ *and* $(\ell, n) = 1$*;*
- *a subgroup isomorphic to either* $\mathfrak{S}_4$*, or* $\mathfrak{A}_4$ *or* $\mathfrak{A}_5$*, i.e. to the symmetric group on* 4 *elements or the alternating group on* 4 *or* 5 *elements.*

In the aforementioned algorithm for every data not coming from lower level or weight, we determine if the associate representation is reducible or not. If the representation is irreducible, then we compute the field of definition of the representation, see Proposition 9.1.1.

In order to determine the image up to conjugation, as shown in Chapter 5, it is enough to know the projective image of the representation, up to conjugation, and the set of determinants. Hence, we compute the field of definition of the projective representation, see Proposition 9.2.1, Proposition 9.2.2 and Algorithm 9.2.3.

To decide about the projective image of the representation we perform a list of checks according to Dickson's classification, unless the representation arises from twisting of a representation of lower conductor, in which case the projective image is already stored in the database. In Chapter 10 we show how to verify that a representation has projective image of dihedral type or isomorphic to either $\mathfrak{A}_4$, or $\mathfrak{S}_4$ or $\mathfrak{A}_5$. In the latter case, we relate such projectively exceptional image to data coming from characteristic 2, 3 and 5, for more details see Proposition 10.2.1 and the related section in Chapter 10. Once we have excluded all exceptional cases i.e. all cases in which the image is exceptional, see Definition 5.1.3, the image is "big", meaning that it contains the special linear group of degree 2 of the extension of $\mathbb{F}_\ell$ corresponding to the field of definition of the projective image.

The representation ρ_f can be computed, as explained in [EC11], in time polynomial in n, k and the cardinality of $\mathbb{F}$, where $\mathbb{F}$ is a finite field of characteristic ℓ where the representation is defined, ℓ not dividing n. Due to the current state of technology, we cannot compute such representations for large values of n, k over finite fields of arbitrary order (greater than 41).

Anyway, the computation of the image of a residual 2-dimensional odd semi-simple Galois representation is a totally different matter than the computation of the representation itself. In particular, there is no need to know explicitly the representation in order to compute its image.

Moreover, the algorithm, outlined in the second part of this thesis, will record the conductor of the representation and local data on the representation without computing the representation itself.

One of the main results in this part of the thesis is that the algorithm takes as input only Hecke operators up to the Sturm bound at level n in almost

all cases, i.e. the bound on the number of operators needed is of the order:

$$\frac{k}{12} \cdot n \log\log n,$$

and, in the cases where a greater number of operators is needed, the bound increases, in the worst case, of a factor q^2, where q is the smallest odd prime not dividing n. In addition, almost all the computations are performed in positive characteristic: only in Chapter 10 in the construction related to projectively exceptional images some computations in characteristic zero are needed. Moreover, no pre-computed list of number fields with specific Galois groups is needed in order to compute the projective image.

Part II of this thesis is organized as follows.

In Chapter 4 we introduce the idea of the aforementioned algorithm. In particular, we present the necessary preliminaries on Katz modular forms and on Khare-Wintenberger Theorem.

In Chapter 5 we explain how the image will be described and we prove that any finite subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ occurring as image of an irreducible odd representation is determined, up to conjugation in $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$, by its projective image and its set of determinants. This is done through a case-by-case analysis using Dickson's classification.

In Chapter 6 we prove that working with coefficients up to the Sturm bound is enough to check isomorphism between residual modular semi-simple 2-dimensional Galois representations coming from forms of the same level and weight. In particular, see Theorem 6.3.5 and Theorem 6.3.6 in which we deal with the coefficients indexed by the primes dividing the level and the characteristic.

In Chapter 7 we deal with reducible representations. The main idea of this chapter is to check equalities between mod ℓ modular forms and the reduction modulo ℓ of certain Eisenstein series, see Theorem 7.2.3.

Twisting a representation by a character is a basic operation in representation theory. In order to describe the projective image of the representation we are studying, we investigate the conductor of the twist and the local description of the representation at primes dividing the conductor. We show that it is possible to determine whether the representation restricted to the decomposition group at a ramified prime is irreducible or reducible, and in the latter case we study its splitting. Since the twist of a modular residual Galois representation is modular, we also investigate the coefficients of the form of minimal level and weight associated to the given twist. The problem of twisting a representation by a character is studied in Chapter 8, where several useful results are collected about the conductor of the twist, see Proposition 8.2.1, Proposition 8.2.4 and Proposition 8.2.6. Moreover, we

outline an algorithm which returns the local description of the representation at the primes dividing the level and the characteristic, see Algorithm 8.2.9.

In Chapter 9, results about the field of definition of the representation and of the projective representation are presented, see Proposition 9.1.1, Proposition 9.2.1 and Proposition 9.2.2. In particular, we prove that, if the representation is irreducible and does not arise from lower level or weight, then the coefficients up to the Sturm bound are enough to determine the field of definition of the linear representation. In the case of the field of definition of the projective representation, we give a characterization and an algorithm to compute it, see Algorithm 9.2.3.

In Chapter 10 we deal with irreducible representations with projective image of dihedral type or projectively exceptional type, i.e. projectively isomorphic to the symmetric group on 4 elements or the alternating group on 4 or 5 elements. In the projective dihedral case we show the existence of a twist for the representation and we describe the character for which such a twist occurs, see Proposition 10.1.1 and Corollary 10.1.2. When the image is projectively exceptional, we give a new approach and a construction for these kinds of representations, using representation theory and the Khare-Wintenberger Theorem.

The outlined algorithm is summarized in Chapter 11, where also an explanation of the associate database is given.

In the appendix, we analyse degeneracy maps between modular curves and we deduce results about residual modular Galois representations and their level of realization, see Theorem A.3.1. These results are not used in the algorithm.

Contents

Contents

Part I

A local-global principle for isogenies of prime degree over number fields

Chapter 1

Introduction

Let E be an elliptic curve over a number field K, and let ℓ be a prime number. If we know residual information on E, i.e. information over the reduction of E for a set of primes with density one, can we deduce global information about E?

One of the first to ask this kind of questions was Serge Lang: let E be an elliptic curve over a number field K, and let ℓ be a prime number, if E has non-trivial ℓ-torsion locally at a set of primes with density one, then does E have non-trivial ℓ-torsion over K?

Katz in 1981 studied this local-global principle, see [Kat81]. He was able to prove that if E has non-trivial ℓ-torsion locally at a set of primes with density one then there exists a K-isogenous elliptic curve which has non-trivial ℓ-torsion over K. He proved this by reducing the problem to a purely group-theoretic statement. Moreover, he was able to extend the result to 2-dimensional abelian varieties and to give a family of counterexamples in dimension 3.

Here we consider the following variation on this question: let E be an elliptic curve over a number field K, and let ℓ be a prime number, if E admits an ℓ-isogeny locally at a set of primes with density one then does E admit an ℓ-isogeny over K?

Recently, Sutherland has studied this problem, see [Sut12]. Let us recall that, except in the case when the j-invariant is 0 or 1728, whether an elliptic curve admits an ℓ-isogeny over K or not depends only on its j-invariant. As in [Sut12], we will only consider elliptic curves with j-invariant different from 0 and 1728.

Definition 1.0.1. Let K be a number field and E an elliptic curve over K. A pair $(\ell, j(E))$ is said to be *exceptional* for K if E/K admits an ℓ-isogeny locally almost everywhere, i.e. for a set of density one of primes of K, but not globally over K.

For primes of good reduction and not dividing ℓ, the definition of local isogeny is the natural one, and it is recalled in Definition 1.1.1 below.

Let us remark that if $(\ell, j(E))$ is an exceptional pair for the number field K, then any E_D, quadratic twist of E, gives rise to the same exceptional pair. Indeed, the Galois representation associated to the ℓ-torsion of E and

the one of E_D are twist of each other: $\rho_{E_D,\ell} \simeq \chi_D \otimes \rho_{E,\ell}$, where χ_D is a quadratic character. Hence their projective images are isomorphic.

A curve occurring in an exceptional pair will admit an ℓ-isogeny globally over a small extension of the base field: more precisely, we can state the following proposition, which is a sharpened version of a result of Sutherland (for a detailed discussion see Section 2.1, Proposition 2.1.4):

Proposition 1.0.2. *Let E be an elliptic curve defined over a number field K, let ℓ be a prime number and assume $\sqrt{\left(\frac{-1}{\ell}\right)\ell} \notin K$. Suppose that E/K admits an ℓ-isogeny locally at a set of primes with density one. Then E admits an ℓ-isogeny over $K(\sqrt{-\ell})$. Moreover, if $\ell = 2, 3$ or $\ell \equiv 1 \bmod 4$ then E admits a global ℓ-isogeny over K.*

There are examples, for $\ell \equiv 3 \bmod 4$ and $\ell \geq 7$, in which it is necessary to extend the base field to have a global isogeny. In particular, Sutherland proved that over $\mathbb{Q}$ the following optimal result holds:

Theorem 1.0.3 ([Sut12, Theorem 2])**.** *The pair $(7, 2268945/128)$ is the only exceptional pair for $\mathbb{Q}$.*

This theorem is proved applying [Par05, Theorem 1.1], which asserts that for all primes $\ell \equiv 3 \bmod 4$ with $\ell > 7$, the only rational non-cuspidal points on $X_{\text{split}}(\ell)(\mathbb{Q})$ correspond to elliptic curves with complex multiplication (for a definition of this modular curve see Chapter 3). Hence, over $\mathbb{Q}$ there exists only one counterexample to the local-global principle for 7-isogenies and there is none for ℓ-isogenies for $\ell > 7$.

We will prove that a similar dichotomy is true for any number field: the number of counterexamples to the local-global principle about ℓ-isogenies for $\ell > 7$ is always finite and the number of counterexamples to the local-global principle about 7-isogenies and 5-isogenies may or may not be finite, depending in one case on the rank of a given elliptic curve, in the other on a condition on the number field.

Namely, the main result of Part I of this thesis is the following:

Main Theorem. *Let K be a number field of degree d over $\mathbb{Q}$ and discriminant Δ, and let $\ell_K := \max\{\Delta, 6d{+}1\}$. The following holds:*

(1) *if $(\ell, j(E))$ is an exceptional pair for the number field K then $\ell \leq \ell_K$;*

(2) *there are only finitely many exceptional pairs for K with $7 < \ell \leq \ell_K$;*

(3) *the number of exceptional pairs for K with $\ell = 7$ is finite or infinite, according to the rank of Elkies-Sutherland's elliptic curve:*

$$y^2 = x^3 - 1715x + 33614$$

being zero or positive over K;

(4) *there exists no exceptional pair for K with $\ell = 2$ and with $\ell = 3$;*

(5) *there exist exceptional pairs for K with $\ell = 5$ if and only if $\sqrt{5}$ belongs to K. Moreover, if $\sqrt{5}$ belongs to K then there are infinitely many exceptional pairs for K with $\ell = 5$.*

Actually, we prove more precise results, that will be discussed in the following chapters. Before entering the details of the proofs, let us give a rough idea of our strategy for the point (1) above.

The pair $(\ell, j(E))$ is exceptional for a number field K if and only if the action of $G \subseteq \mathrm{GL}_2(\mathbb{F}_\ell)$, the image of the Galois representation associated to the ℓ-torsion of E, on $\mathbb{P}(E[\ell]) \simeq \mathbb{P}^1(\mathbb{F}_\ell)$ has no fixed point, whereas every $g \in G$ leaves a line stable, that is, all $g \in G$ have a reducible characteristic polynomial. Using Dickson's classification of subgroups of $\mathrm{PGL}_2(\mathbb{F}_\ell)$, one sees that, up to conjugation, G has to be either the inverse image of an exceptional group (but this case is known to happen only for small ℓ) or contained in the normalizer of a split Cartan subgroup, that is $G = \left\{ \left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & a \\ b & 0 \end{smallmatrix}\right) | a, b \in \Gamma \right\}$ for Γ a subgroup of $\mathbb{F}_\ell^*$.

In the last case, using notations as in [Par05, Section 2] or in Chapter 3 herein, exceptional pairs therefore induce points in $X_{\mathrm{split}}(\ell)(K)$ not lifting to $X_{\mathrm{sp.Car}}(\ell)(K)$ (forgetting cases corresponding to exceptional groups). The existence of such points is in general a wide open question; however, in our case, the reducibility of the characteristic polynomials implies that Γ is actually a subgroup of squares: $\Gamma \subseteq (\mathbb{F}_\ell^*)^2$. By the property of Weil pairing, one deduces that $K(\sqrt{\left(\frac{-1}{\ell}\right)\ell}) \subseteq L$, field of definition of the ℓ-isogeny. From this, in the case $\sqrt{\left(\frac{-1}{\ell}\right)\ell} \notin K$, we can conclude that the well-known shape of inertia at ℓ inside G gives a contradiction for $\ell > 6[K : \mathbb{Q}]+1$.

Part I of this thesis is organized as follows.

For the convenience of the reader, we recall in the next section the results obtained by Sutherland in [Sut12, Section 2].

In Chapter 2, we study exceptional pairs over arbitrary number fields. First we deduce the effective version of Sutherland's result, then we describe how to tackle the case not treated by Sutherland and we prove the statement (4) of the Main Theorem (see Proposition 2.1.9). Moreover, we give conditions under which an exceptional pair does not have complex multiplication. Chapter 2 closes with the proof of the bound given in (1) of the Main Theorem (Corollary 2.3.5).

In Chapter 3 we discuss finiteness results for the set of exceptional pairs and we prove statements (2) (Theorem 3.1.1), (5) (Corollary 3.2.2) and (3) (Proposition 3.3.1) of the Main Theorem.

1.1 Sutherland's results

Let us recall the definition of local ℓ-isogeny for an elliptic curve:

Definition 1.1.1. Let E be an elliptic curve over a number field K, let ℓ be a prime number. If $\mathfrak{p}$ is a prime of K where E has good reduction, $\mathfrak{p}$ not dividing ℓ, we say that E admits an ℓ-isogeny *locally* at $\mathfrak{p}$ if the reduction of E modulo $\mathfrak{p}$ admits an ℓ-isogeny defined over the residue field at $\mathfrak{p}$.

Let us remark that for a prime $\mathfrak{p}$ of K where E has good reduction, $\mathfrak{p}$ not dividing ℓ, the definition given is equivalent to say that the Néron model of E over the ring of integer of $K_{\mathfrak{p}}$ admits an ℓ-isogeny. This follows because the ℓ-isogeny in this case is étale.

Sutherland has proved, under certain conditions, that for an elliptic curve defined over a number field, the existence of local ℓ-isogenies for a set of primes with density one implies the existence of a global ℓ-isogeny:

Theorem 1.1.2 ([Sut12, Theorem 1])**.** *Let E be an elliptic curve over a number field K with $j(E) \notin \{0, 1728\}$, and let ℓ be a prime number. Assume that $\sqrt{\left(\frac{-1}{\ell}\right)\ell} \notin K$, and suppose E/K admits an ℓ-isogeny locally at a set of primes with density one. Then E admits an ℓ-isogeny over a quadratic extension of K.*

Moreover, if $\ell \equiv 1 \bmod 4$ or $\ell < 7$, then E admits an ℓ-isogeny defined over K.

Let us recall briefly how this theorem is proved. The main tool used is the theory of Galois representations attached to elliptic curves, see [Ser72], to reduce the problem to a question regarding subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$.

There is a natural action of $\mathrm{GL}_2(\mathbb{F}_\ell)$ on $\mathbb{P}^1(\mathbb{F}_\ell)$, and the induced action of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ is faithful. For an element g of $\mathrm{GL}_2(\mathbb{F}_\ell)$ or of $\mathrm{PGL}_2(\mathbb{F}_\ell)$, we will denote, respectively, by $\mathbb{P}^1(\mathbb{F}_\ell)/g$ the set of g-orbits of $\mathbb{P}^1(\mathbb{F}_\ell)$ and by $\mathbb{P}^1(\mathbb{F}_\ell)^g$ the set of elements fixed by g.

Lemma 1.1.3 ([Sut12, Lemma 1])**.** *Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ whose image H in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ is not contained in $\mathrm{SL}_2(\mathbb{F}_\ell)/\{\pm 1\}$.*

Suppose $|\mathbb{P}^1(\mathbb{F}_\ell)^g| > 0$ for all $g \in G$ but $|\mathbb{P}^1(\mathbb{F}_\ell)^G| = 0$.
Then $\ell \equiv 3 \bmod 4$ and the following holds:

(1) *H is dihedral of order $2n$, where $n > 1$ is an odd divisor of $(\ell-1)/2$;*

(2) *G is properly contained in the normalizer of a split Cartan subgroup;*

(3) *$\mathbb{P}^1(\mathbb{F}_\ell)/G$, the set of G-orbits of $\mathbb{P}^1(\mathbb{F}_\ell)$, contains an orbit of size 2.*

This result is an application of the orbit-counting lemma combined with Dickson's classification of subgroups of $\mathrm{PGL}_2(\mathbb{F}_\ell)$, see [Dic58] or [Lan76], and it is one of the key steps in the proof of Theorem 1.1.2. Let us notice that if the hypotheses of Lemma 1.1.3 are satisfied, then it follows that $\ell \neq 3$ because $n > 1$ in (1).

Remark 1.1.4. Given an elliptic curve E over a number field K, the compatibility between $\rho_{E,\ell}$, the Galois representation associated to the ℓ-torsion group $E[\ell]$, and the Weil pairing on $E[\ell]$ implies that for every $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ we have

$$\sigma(\zeta_\ell) = \zeta_\ell^{\det(\rho_{E,\ell}(\sigma))},$$

where ζ_ℓ is an ℓ-root of unity.

Hence, ζ_ℓ is in K if and only if $G = \rho_{E,\ell}(\mathrm{Gal}(\overline{\mathbb{Q}}/K))$ is contained in $\mathrm{SL}_2(\mathbb{F}_\ell)$. Moreover, using the Gauss sum: $\sum_{n=0}^{\ell-1} \zeta_\ell^{n^2} = \sqrt{\left(\frac{-1}{\ell}\right)\ell}$ and denoting by H the image of G in $\mathrm{PGL}_2(\mathbb{F}_\ell)$, it follows that H is contained in $\mathrm{SL}_2(\mathbb{F}_\ell)/\{\pm 1\}$ if and only if $\sqrt{\left(\frac{-1}{\ell}\right)\ell}$ is in K.

Sketch of the proof of Theorem 1.1.2. For every $g \in G = \rho_{E,\ell}(\mathrm{Gal}(\overline{\mathbb{Q}}/K))$, it follows from Chebotarev density theorem that there exists a prime $\mathfrak{p} \subset \mathcal{O}_K$ such that $g = \rho_{E,\ell}(\mathrm{Frob}_\mathfrak{p})$ and E admits an ℓ-isogeny locally at $\mathfrak{p}$. The Frobenius endomorphism fixes a line in $E[\ell]$, hence $|\mathbb{P}^1(\mathbb{F}_\ell)^g| > 0$ for all $g \in G$.

If $|\mathbb{P}^1(\mathbb{F}_\ell)^G| > 0$, then $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ fixes a linear subspace of $E[\ell]$ which is the kernel of an ℓ-isogeny defined over K.

Hence, let us assume $|\mathbb{P}^1(\mathbb{F}_\ell)^G| = 0$.

No subgroup of $\mathrm{GL}_2(\mathbb{F}_2)$ satisfies $|\mathbb{P}^1(\mathbb{F}_2)^G| = 0$ and $|\mathbb{P}^1(\mathbb{F}_2)^g| > 0$ for all $g \in G$, so ℓ is odd.

The hypotheses on K, combined with the Weil pairing on the ℓ-torsion, implies that some element of G has a non-square determinant, hence the image of G in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ does not lie in $\mathrm{SL}_2(\mathbb{F}_\ell)/\{\pm 1\}$. The hypotheses of Lemma 1.1.3 are satisfied, thus $\ell \equiv 3 \bmod 4$, the prime ℓ is different from 3, and $\mathbb{P}^1(\mathbb{F}_\ell)/G$ contains an orbit of size 2. Let $x \in \mathbb{P}^1(\mathbb{F}_\ell)$ be an element of this orbit, its stabilizer is a subgroup of index 2. By Galois theory, it corresponds to a quadratic extension of K over which E admits an isogeny of degree ℓ (actually, two such isogenies). □

Chapter 2

Exceptional pairs

2.1 Galois representations

The study of the local-global principle about ℓ-isogenies over an arbitrary number field K depends on $\sqrt{\left(\frac{-1}{\ell}\right)\ell}$ belonging to K or not, see Remark 1.1.4.

First, let us assume that $\sqrt{\left(\frac{-1}{\ell}\right)\ell}$ does not belong to K.

Theorem 1.1.2 implies that an exceptional pair for K, a number field not containing $\sqrt{\left(\frac{-1}{\ell}\right)\ell}$, is no longer exceptional for a quadratic extension of K: in this section we will describe this extension.

Proposition 2.1.1. *Let $(\ell, j(E))$ be an exceptional pair for the number field K with $j(E) \notin \{0, 1728\}$, and assume that $\sqrt{\left(\frac{-1}{\ell}\right)\ell} \notin K$. Let G be $\rho_{E,\ell}(\mathrm{Gal}(\overline{\mathbb{Q}}/K))$ and let H be its image in $\mathrm{PGL}_2(\mathbb{F}_\ell)$. Let $\mathscr{C} \subset G$ be the preimage of the maximal cyclic subgroup of H. Then*

$$\det(\mathscr{C}) \subseteq (\mathbb{F}_\ell^*)^2,$$

where $(\mathbb{F}_\ell^*)^2$ denotes the group of squares in $\mathbb{F}_\ell^*$.

Proof. Let $(\ell, j(E))$ be an exceptional pair for the number field K, and assume that $\sqrt{\left(\frac{-1}{\ell}\right)\ell} \notin K$. By Remark 1.1.4, this implies that H is not contained in $\mathrm{SL}_2(\mathbb{F}_\ell)/\{\pm 1\}$ hence, applying Lemma 1.1.3, we have that $\ell \equiv 3 \bmod 4$, and, up to conjugation, H is dihedral of order $2n$, where $n > 1$ is an odd divisor of $(\ell-1)/2$ and G is properly contained in the normalizer of a split Cartan subgroup.

In particular, we have that $(n, \ell+1) = 1$ and $(n, \ell) = 1$, because n is odd and it is a divisor of $\ell-1$.

Let $A \in G \subset \mathrm{GL}_2(\mathbb{F}_\ell)$ be a preimage of some generator of the maximal cyclic subgroup inside H. Let us underline that the maximal cyclic subgroup inside H is determined uniquely, up to conjugation, since Cartan subgroups are all conjugated and H has order different from 4.

Let us show that A is conjugate in $\mathrm{GL}_2(\mathbb{F}_\ell)$ to a matrix of the type $\left(\begin{smallmatrix} \alpha & 0 \\ 0 & \beta \end{smallmatrix}\right)$, with $\alpha, \beta \in \mathbb{F}_\ell^*$ and α/β of order n in $\mathbb{F}_\ell^*$.

Extending the scalars to $\mathbb{F}_{\ell^2}$ if necessary, we can put A in its Jordan normal form. Then either $A \cong \left(\begin{smallmatrix} \alpha & 0 \\ 0 & \beta \end{smallmatrix}\right)$ with $\alpha, \beta \in \mathbb{F}_{\ell^2}$, or $A \cong \left(\begin{smallmatrix} \alpha & 1 \\ 0 & \alpha \end{smallmatrix}\right)$. Since we have $A^n = \lambda \cdot \mathrm{Id}$, for $\lambda \in \mathbb{F}_\ell^*$, and $(n, \ell) = 1$ then the second case cannot occur.

We claim that $\alpha, \beta \in \mathbb{F}_\ell^*$. In fact, let us proceed by contradiction: if $\alpha, \beta \in \mathbb{F}_{\ell^2} \backslash \mathbb{F}_\ell$ then $\beta = \overline{\alpha}$, the conjugate of α over $\mathbb{F}_\ell$. This means that $\mathbb{P}^1(\mathbb{F}_\ell)^A$ is empty because A has no eigenvalues in $\mathbb{F}_\ell$ and this is not possible because E admits an ℓ-isogeny locally everywhere and by Chebotarev density theorem $A = \rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{p}})$ with $\mathfrak{p} \subset \mathcal{O}_K$ prime. Hence $\alpha, \beta \in \mathbb{F}_\ell^*$.

Let us write $\alpha = \mu^i$ and $\beta = \mu^j$ for some generator μ of $\mathbb{F}_\ell^*$, then

$$\mu^{in} = \alpha^n = \beta^n = \mu^{jn},$$

so $\mu^{n(i-j)} = 1$ and $n(j-i) \equiv 0 \bmod \ell - 1$. As n is odd, $(j-i)$ has to be even, hence also $(i+j)$ is even. Therefore $\det(A) = \alpha\beta = \mu^{i+j}$ is a square in $\mathbb{F}_\ell^*$. Moreover, since A is a preimage of some generator of the maximal cyclic subgroup inside H, then α/β must have order n. □

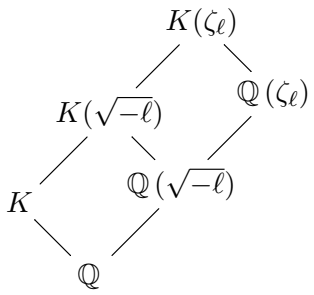
Remark 2.1.2. Let $(\ell, j(E))$ be an exceptional pair for the number field K. Let us suppose that $j(E) \notin \{0, 1728\}$ and $\sqrt{\left(\frac{-1}{\ell}\right)\ell}$ does not belong to K. Since the projective image of the Galois representation associated to E is dihedral of order $2n$, with n odd divisor of $(\ell-1)/2$, the order of G, image of the Galois representation, satisfies:

$$|G| \mid ((\ell-1) \cdot 2n) \mid \left((\ell-1) \cdot \frac{(\ell-1)}{2} \cdot 2\right) = (\ell-1)^2.$$

Proposition 2.1.3. *Let $(\ell, j(E))$ be an exceptional pair for the number field K with $j(E) \notin \{0, 1728\}$, and assume that $\sqrt{\left(\frac{-1}{\ell}\right)\ell}$ does not belong to K. Then E admits an ℓ-isogeny over $K(\sqrt{-\ell})$ (and actually, two such isogenies).*

Proof. Theorem 1.1.2 implies that $\ell \equiv 3 \bmod 4$ and $\ell \geq 7$ since $(\ell, j(E))$ is an exceptional pair. Since $\sqrt{-\ell} \notin K$, then also ζ_ℓ, the ℓ-th root of unity, is not in K by ramification theory.

Moreover, since $\ell \equiv 3 \bmod 4$, the quadratic sub field of $\mathbb{Q}(\zeta_\ell)$ is $\mathbb{Q}(\sqrt{-\ell})$. In particular: $\mathrm{Gal}(K(\zeta_\ell)/K(\sqrt{-\ell})) \subseteq (\mathbb{F}_\ell^*)^2$, the subgroup of squares inside $\mathbb{F}_\ell^*$. If ℓ does not divide the discriminant of K then the previous inclusion is an equality, since the ramifications are disjoint. Let, as before, $\rho_{E,\ell} \colon \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathrm{GL}_2(\mathbb{F}_\ell)$ be the Galois representation associated to E and let G be its image.



It follows, using notation of Proposition 2.1.1, that E admits one isogeny (actually two) on the quadratic extension L/K corresponding to the Cartan subgroup $\mathscr{C}$ which is the subgroup of diagonal matrices inside G. By Proposition 2.1.1, the elements of $\mathscr{C}$ have square determinants.

On the other hand, from the properties of the Weil pairing on the ℓ-torsion, for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ we have that $\det(\rho_{E,\ell}(\sigma)) = \chi_\ell(\sigma)$, where χ_ℓ is the mod ℓ cyclotomic character. Hence, $\mathscr{C}$ is the kernel of the character $\varphi\colon G \to \mathbb{F}_\ell^*/(\mathbb{F}_\ell^*)^2 \cong \{\pm 1\}$ which makes the following diagram commute:

$$\begin{array}{ccccc} \mathrm{Gal}(\overline{\mathbb{Q}}/K) & \xrightarrow{\rho_{E,\ell}} & G & \xrightarrow{\qquad\varphi\qquad} & \mathbb{F}_\ell^*/(\mathbb{F}_\ell^*)^2 \cong \{\pm 1\} \\ & & \downarrow{\scriptstyle \det} & \searrow^{\chi_\ell} & \uparrow \\ & & \mathrm{Gal}(K(\zeta_\ell)/K) & \hookrightarrow \mathbb{F}_\ell^* \cong \mathrm{Aut}(\mu_\ell) & \end{array}$$

The character of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ induced by φ is not trivial because there is an element in G with non square determinant since $\sqrt{-\ell}$ is not in K. By Galois theory, the kernel of φ corresponds to a quadratic extension of K, which contains $\sqrt{-\ell}$ by construction. This implies that the extension over which E admits a global ℓ-isogeny is $K(\sqrt{-\ell})$. □

Combining Proposition 2.1.3 and Theorem 1.1.2, we have proved the following result, which is Proposition 1.0.2 of the introduction:

Proposition 2.1.4. *Let E be an elliptic curve defined over a number field K with $j(E) \notin \{0, 1728\}$. Let ℓ be a prime number and let $\sqrt{\left(\frac{-1}{\ell}\right)\ell} \notin K$. Suppose that E/K admits an ℓ-isogeny locally at a set of primes with density one, then E admits an ℓ-isogeny over $K(\sqrt{-\ell})$. Moreover, if $\ell = 2, 3$ or $\ell \equiv 1 \bmod 4$ then E admits a global ℓ-isogeny over K.*

Now let us assume that $\sqrt{\left(\frac{-1}{\ell}\right)\ell}$ belongs to K.

As in the previous case, in order to analyse the local-global principle, we study subgroups of $\mathrm{SL}_2(\mathbb{F}_\ell)/\{\pm 1\}$ which do not fix any point of $\mathbb{P}^1(\mathbb{F}_\ell)$ but whose elements do fix points.

The following lemma is a variation on the result, due to Sutherland, that we already stated as Lemma 1.1.3, see [Sut12, Lemma 1 and Proposition 2]. This lemma will be the key in understanding the case in which $\sqrt{\left(\frac{-1}{\ell}\right)\ell}$ belongs to K. We will denote by $\mathfrak{S}_n$ (respectively $\mathfrak{A}_n$) the symmetric (respectively alternating) group on n-elements.

Lemma 2.1.5. *Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ whose image H in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ is contained in $\mathrm{SL}_2(\mathbb{F}_\ell)/\{\pm 1\}$. Suppose $|\mathbb{P}^1(\mathbb{F}_\ell)^g| > 0$ for all $g \in G$ but $|\mathbb{P}^1(\mathbb{F}_\ell)^G| = 0$. Then $\ell \equiv 1 \bmod 4$ and one of the followings holds:*

(1) *H is dihedral of order $2n$, where $n \in \mathbb{Z}_{>1}$ is a divisor of $\ell - 1$;*

(2) *H is isomorphic to one of the following exceptional groups: $\mathfrak{A}_4$, $\mathfrak{S}_4$ or $\mathfrak{A}_5$.*

Proof. No subgroup of $\mathrm{GL}_2(\mathbb{F}_2)$ satisfies the hypotheses of the lemma, so we assume $\ell > 2$. The orbit-counting lemma yields:

$$|\mathbb{P}^1(\mathbb{F}_\ell)/H| = \frac{1}{|H|}\sum_{h\in H}|\mathbb{P}^1(\mathbb{F}_\ell)^h| \geq \frac{1}{|H|}(\ell+|H|) > 1$$

since $|\mathbb{P}^1(\mathbb{F}_\ell)^h| > 0$ for all $h \in H$ and $|\mathbb{P}^1(\mathbb{F}_\ell)^h| = (\ell+1)$ when h is the identity.

If ℓ divides $|H|$ then H contains an element h of order ℓ and $\mathbb{P}^1(\mathbb{F}_\ell)/h$ consists of two orbits, of sizes 1 and ℓ, therefore a fortiori $(1 <)|\mathbb{P}^1(\mathbb{F}_\ell)/H| \leq 2$. But this contradicts the assumption $|\mathbb{P}^1(\mathbb{F}_\ell)^H| = 0$. Hence ℓ does not divide $|H|$.

By Dickson's classification of subgroups of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ it follows that H can be either cyclic, or dihedral or isomorphic to one the following groups: $\mathfrak{S}_4$, $\mathfrak{A}_4$, $\mathfrak{A}_5$.

We can exclude that H is cyclic. Let us indeed assume otherwise, and write $H = \langle h\rangle$. This implies that $\mathbb{P}^1(\mathbb{F}_\ell)^h = \mathbb{P}^1(\mathbb{F}_\ell)^H$ and since $|\mathbb{P}^1(\mathbb{F}_\ell)^h| > 0$ by hypothesis, we have a contradiction with $|\mathbb{P}^1(\mathbb{F}_\ell)^H| = 0$. Hence H is either dihedral, or isomorphic to $\mathfrak{S}_4$, or to $\mathfrak{A}_4$, or to $\mathfrak{A}_5$.

By [Sut12, Proposition 2], since H is contained in $\mathrm{SL}_2(\mathbb{F}_\ell)/\{\pm 1\}$, the size of the set of h-orbits of $\mathbb{P}^1(\mathbb{F}_\ell)$ is even for each $h \in H$. Moreover, as $|\mathbb{P}^1(\mathbb{F}_\ell)^h| > 1$, all h are diagonalizable on $\mathbb{F}_\ell$.

Then, applying the orbit-counting lemma, we have

$$\begin{aligned}|\mathbb{P}^1(\mathbb{F}_\ell)/h| &= \frac{1}{\mathrm{ord}(h)}\sum_{h'\in\langle h\rangle}|\mathbb{P}^1(\mathbb{F}_\ell)^{h'}| = \\ &= \frac{1}{\mathrm{ord}(h)}((\mathrm{ord}(h)-1)2+\ell+1) = 2+\frac{\ell-1}{\mathrm{ord}(h)} \qquad (*)\end{aligned}$$

where $\langle h\rangle$ denotes the cyclic subgroup of H generated by h. In particular, for elements of order 2 this implies that $\ell \equiv 1 \bmod 4$.

Let us suppose that H is a dihedral group of order $2n$. Then there exists $h \in H$ of order n, so equation $(*)$ implies that n divides $\ell-1$. □

Note that, in the course of the above proof, we have shown the following:

Corollary 2.1.6. *Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$. Assume that the image H of G in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ is contained in $\mathrm{SL}_2(\mathbb{F}_\ell)/\{\pm 1\}$. Suppose $|\mathbb{P}^1(\mathbb{F}_\ell)^g| > 0$ for all $g \in G$ but $|\mathbb{P}^1(\mathbb{F}_\ell)^G| = 0$. If H is dihedral of order $2n$, where $n \in \mathbb{Z}_{>1}$ is a divisor of $\ell-1$, then G is properly contained in the normalizer of a split Cartan subgroup and $\mathbb{P}^1(\mathbb{F}_\ell)/G$ contains an orbit of size 2.*

Let us now focus on case (2) of Lemma 2.1.5:

Corollary 2.1.7. *Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ whose projective image H is contained in $\mathrm{SL}_2(\mathbb{F}_\ell)/\{\pm 1\}$. Suppose $|\mathbb{P}^1(\mathbb{F}_\ell)^g| > 0$ for all $g \in G$ but $|\mathbb{P}^1(\mathbb{F}_\ell)^G| = 0$. Then the following holds:*
- *if H is isomorphic to $\mathfrak{A}_4$ then $\ell \equiv 1 \bmod 12$;*
- *if H is isomorphic to $\mathfrak{S}_4$ then $\ell \equiv 1 \bmod 24$;*
- *if H is isomorphic to $\mathfrak{A}_5$ then $\ell \equiv 1 \bmod 60$.*

Proof. This is an application of the orbit-counting lemma. In $\mathfrak{A}_4$ there are elements of order 2 and 3, and we have $\ell > 3$ since $\mathrm{GL}_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$. The equation $(*)$ for elements of order 3 implies that $\ell-1$ is divisible by 3, so, since $\ell \equiv 1 \bmod 4$, then $\ell \equiv 1 \bmod 12$.

Applying [Sut12, Proposition 2], we see that the parity of the values of equation $(*)$ determines the sign as permutation of any element of $\mathrm{PGL}_2(\mathbb{F}_\ell)$. Since H is contained in $\mathrm{SL}_2(\mathbb{F}_\ell)/\{\pm 1\}$, the value of equation $(*)$ has to be even for every h in H.

If H is isomorphic to $\mathfrak{S}_4$, then it contains elements of order 4 and this implies that $\ell-1$ is divisible by 8. Repeating the argument for elements of order 3 we conclude that $\ell \equiv 1 \bmod 24$.

Analogously, if H is isomorphic to $\mathfrak{A}_5$ then $\ell > 5$ since not all matrices in $\mathrm{SL}_2(\mathbb{F}_5)/\{\pm 1\} \simeq \mathfrak{A}_5$ leave a line stable. There are elements of order 3 and 5, then $\ell-1$ is divisible by 3 and 5. So, since $\ell \equiv 1 \bmod 4$, we have $\ell \equiv 1 \bmod 60$. □

Proposition 2.1.8. *Let E be an elliptic curve over a number field K of degree d over $\mathbb{Q}$ with $j(E) \notin \{0, 1728\}$, and let ℓ be a prime number. Let us suppose $\sqrt{\left(\frac{-1}{\ell}\right)\ell} \in K$ and that E/K admits an ℓ-isogeny locally at a set of primes with density one. Then:*

(1) *if $\ell \equiv 3 \bmod 4$ the elliptic curve E admits a global ℓ-isogeny over K;*
(2) *if $\ell \equiv 1 \bmod 4$ the elliptic curve E admits an ℓ-isogeny over a finite extension of K, which can ramify only at primes dividing the conductor of E and ℓ. Moreover, if $\ell \equiv -1 \bmod 3$ or if $\ell \geq 60d+1$, then E admits an ℓ-isogeny over a quadratic extension of K.*

Proof. Since $\sqrt{\left(\frac{-1}{\ell}\right)\ell}$ is contained in K, the projective image H of the Galois representation $\rho_{E,\ell}$ is contained in $\mathrm{SL}_2(\mathbb{F}_\ell)/\{\pm 1\}$, as discussed in Remark 1.1.4, so we can apply Lemma 2.1.5. This means that if the pair $(\ell, j(E))$ is an exceptional pair then $\ell \equiv 1 \bmod 4$ and H has to be either a dihedral group of order $2n$, with n dividing $\ell-1$, or an exceptional subgroup.

If the elliptic curve E admits an ℓ-isogeny over a number field L/K then there exists a one dimensional $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$-stable subspace of $E[\ell]$. This subspace

corresponds to a subgroup of the image of the Galois representation. In particular, the extension L of K over which the isogeny is defined can only ramify at primes where the representation is ramified, that is, only at primes of K dividing the conductor of E or ℓ.

If $\ell \geq 60d+1$ then H cannot be isomorphic to $\mathfrak{A}_4$, or to $\mathfrak{S}_4$ or $\mathfrak{A}_5$, for a proof of this fact see [Maz77a, p.36]. Analogously, by Corollary 2.1.7, exceptional images cannot occur if $\ell \equiv -1 \bmod 3$. Hence, by Corollary 2.1.6, in these cases the image of the Galois representation associated to E is conjugated to the normalizer of a Cartan subgroup which contains the Cartan subgroup itself with index 2. By Galois theory, then E admits a global isogeny over a quadratic extension of K. □

Let us now describe all the possibilities that can occur at 2, 3 and 5:

Proposition 2.1.9. *Let K be a number field. There exists no exceptional pair for K with $\ell = 2, 3$. If $\sqrt{5}$ belongs to K then there exist exceptional pairs $(5, j(E))$ for K and, moreover, $\mathbb{P}\rho_{E,5}(\mathrm{Gal}(\overline{\mathbb{Q}}/K))$ is a dihedral group of order dividing 8. If $\sqrt{5}$ does not belong to K then there exists no exceptional pairs for K with $\ell = 5$.*

Proof. As remarked in the proof of Theorem 1.1.2, for ℓ=2 there exists no exception to the local-global principle. Take ℓ=3. If $\sqrt{-3}$ is not in K then there exists no exceptional pair since, by Lemma 1.1.3, the projective image is a dihedral group of order $2n$ with $n \in \mathbb{Z}_{>1}$ odd (dividing $3-1$). Similarly if $\sqrt{-3}$ belongs to K there exists no exceptional pair since, by Lemma 2.1.5, $\ell \equiv 1 \bmod 4$. For ℓ=5 we have that if $\sqrt{5}$ is not in K then there exists no exceptional pair by Lemma 1.1.3. Moreover, if $\sqrt{5}$ is in K then by Lemma 2.1.5 combined with Corollary 2.1.7, the projective image can only be a dihedral group of order dividing 8. □

2.2 Complex multiplication

Sutherland in [Sut12] proved that an exceptional pair $(\ell, j(E))$ over $\mathbb{Q}$ cannot have complex multiplication: for $\ell > 7$ we refer to the proof of [Sut12, Theorem 2] and for $\ell = 7$ we refer to the direct computations in [Sut12, Section 3].

Here we study the same problem for K a number field.

Lemma 2.2.1. *Let K be a number field and E/K an elliptic curve over K with $j(E) \notin \{0, 1728\}$. Let $(\ell, j(E))$ be an exceptional pair for K. If $\ell > 2d+1$ then E cannot have complex multiplication.*

Proof. Assume that E has complex multiplication by a quadratic order $\mathcal{O}$. This means that the Galois representation $\rho_{E,\ell}$ has image included in a Borel, when ℓ ramifies in $\mathcal{O}$, or projectively dihedral (split or nonsplit, according to ℓ being split or nonsplit in $\mathcal{O}$), see [Ser66, Théorème 5].

The Borel case is clearly not possible.

By Proposition 2.1.4, there is an ℓ-isogenous elliptic curve E' that is defined over a quadratic extension L of K, but not over K, since we are in an exceptional case. Since E' is isogenous to E over L, it also must have complex multiplication by an order $\mathcal{O}'$. Since E and E' are ℓ-isogenous, by [Cox89, Theorem 7.24], the ratio between the class numbers $h(\mathcal{O}')$ and $h(\mathcal{O})$ satisfies

$$\frac{h(\mathcal{O}')}{h(\mathcal{O})} = \frac{1}{[\mathcal{O}^* : \mathcal{O}'^*]} \left(\ell - \left(\frac{\mathrm{disc}(\mathcal{O})}{\ell} \right) \right) \geq (\ell - 1)$$

since $j(E) \notin \{0, 1728\}$. In particular if $h(\mathcal{O}') = h(\mathcal{O})$ we have a contradiction. Hence assume $h(\mathcal{O}') > h(\mathcal{O})$.

Since E' is defined over L and E is defined over K then $\mathbb{Q}(j_E) \subseteq K$ and $\mathbb{Q}(j_{E'}) \subseteq L$. The ratio of the class numbers $h(\mathcal{O}')$ and $h(\mathcal{O})$ satisfies:

$$\frac{h(\mathcal{O}')}{h(\mathcal{O})} \leq [L : \mathbb{Q}] = 2d.$$

Therefore, if $\ell > 2d + 1$, we have a contradiction between the lower and the upper bound, so E cannot have complex multiplication. □

2.3 Bounds

In this section we prove statement (1) of the Main Theorem. First of all, we recall some statements concerning the image of the inertia subgroup at a prime ℓ through the Galois representation associated to ℓ-torsion of an elliptic curve E over a number field K, i.e. $\rho_{E,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathrm{GL}_2(\mathbb{F}_\ell)$.

This description leads to prove the bound which is contained in statement (1) of the Main Theorem.

Image of the inertia

Let M be a complete field with respect to a discrete valuation v, which is normalized, i.e. $v(M^*) = \mathbb{Z}$. Let $\mathcal{O}_M$ be its ring of integers, λ the maximal ideal of $\mathcal{O}_M$ and $k = \mathcal{O}_M/\lambda$ the residue field. We suppose M of characteristic 0, the residue field k finite of characteristic $\ell > 0$ and $e = v(\ell) < \infty$.

Let E be an elliptic curve having semi-stable reduction over M and let $\mathcal{E}$ be its Néron model over $\mathcal{O}_M$. Since M is of characteristic 0, we know that $E[\ell](\overline{M})$ is an $\mathbb{F}_\ell$-vector space of dimension 2.

Let $\overline{\mathcal{E}}$ be the reduction of $\mathcal{E}$ modulo λ, then $\overline{\mathcal{E}}$ is a group scheme defined over k whose ℓ-torsion is an $\mathbb{F}_\ell$-vector space with dimension strictly lower than 2. Hence, the kernel of the reduction map, can be either isomorphic to $\mathbb{F}_\ell$ (ordinary case) or to the whole $E[\ell]$ (supersingular case).

Serre, in [Ser72, Proposition 11, Proposition 12 and p.272], described all possible shapes of the image of I_ℓ, the inertia subgroup at ℓ, for the supersingular case and for the ordinary case:

Proposition 2.3.1 (Serre, supersingular case)**.** *Let E be an elliptic curve over M, complete normalized field with respect to the valuation v, and let $e = v(\ell) \geq 1$. Suppose that E has good supersingular reduction at ℓ. Then the image of I_ℓ through the Galois representation $\rho_{E,\ell} : \mathrm{Gal}(\overline{M}/M) \to \mathrm{GL}_2(\mathbb{F}_\ell)$ associated to E is cyclic of order either $(\ell^2-1)/e$ or $\ell(\ell-1)/e$.*

The two cases depend on the action of the tame inertia.

If the tame inertia acts via powers of the fundamental character of level 2, and not 1, it follows that the Newton polygon, with respect to the elliptic curve, is not broken, and that the tame inertia is given by the e-power of the fundamental character of level 2. Hence it has a cyclic image of order $(\ell^2-1)/e$.

If the elliptic curve considered is supersingular, but the tame inertia acts via powers of the fundamental character of level 1, it follows that the Newton polygon is broken, and there are points in the ℓ-torsion of the corresponding formal group which have valuation with denominator divisible by ℓ (this follows from [Ser72, p.272]). So the image of inertia has order $\ell(\ell-1)/e$.

In the ordinary case, the following proposition holds:

Proposition 2.3.2 (Serre, ordinary case)**.** *Let E be an elliptic curve over M, complete normalized field with respect to the valuation v, and let $e = v(\ell) \geq 1$. Suppose that E has semistable ordinary reduction at ℓ. Then the image of I_ℓ through the Galois representation $\rho_{E,\ell} : \mathrm{Gal}(\overline{M}/M) \to \mathrm{GL}_2(\mathbb{F}_\ell)$ associated to E is cyclic of order either $(\ell-1)/e$ or $\ell(\ell-1)/e$, and it can be represented, after the choice of an appropriate basis, respectively as*

$$\begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} * & \star \\ 0 & 1 \end{pmatrix},$$

with $* \in \mathbb{F}_\ell^*$ and $\star \in \mathbb{F}_\ell$.

Computation of the bound

Let E_λ be an elliptic curve defined over a complete field M with maximal ideal λ, residual characteristic ℓ, and let

$$d' = \begin{cases} 1 & \text{if } j(E) \not\equiv 0, 1728 \bmod \lambda, \\ 2 & \text{if } j(E) \equiv 1728 \bmod \lambda, \ell \geq 5 \\ 3 & \text{if } j(E) \equiv 0 \bmod \lambda, \ell \geq 5, \\ 6 & \text{if } j(E) \equiv 0 \bmod \lambda, \ell = 3, \\ 12 & \text{if } j(E) \equiv 0 \bmod \lambda, \ell = 2. \end{cases} \qquad (\star)$$

Then E_λ, or a quadratic twist, has semistable reduction over a finite extension of M with degree d', see for instance [BK75, pp.33-52] or [Kra90, Proposition 1 and Théorème 1].

We can now give the main result of Part I of this thesis:

Theorem 2.3.3. *Let $(\ell, j(E))$ be an exceptional pair for the number field K of degree d over $\mathbb{Q}$, such that $\sqrt{\left(\frac{-1}{\ell}\right)\ell} \notin K$ and $j(E) \notin \{0, 1728\}$. Then*

$$\ell \equiv 3 \bmod 4 \text{ and } 7 \leq \ell \leq 6d{+}1.$$

Proof. Since the pair $(\ell, j(E))$ is exceptional, E admits an ℓ-isogeny locally at a set of primes with density one, $\ell \equiv 3 \bmod 4$ and by Proposition 2.1.4 it admits an ℓ-isogeny over $L = K(\sqrt{-\ell})$.

Let K_λ be the completion of K at λ, a prime above ℓ, and let M be the smallest extension of K_λ over which $E_\lambda := E \otimes K_\lambda$ gets semi-stable reduction. After replacing E by a quadratic twist if necessary, we can assume that the extension M/K_λ has degree less or equal to 3, according to $(\star)$, since $\ell \geq 7$. Let $\overline{E}$ be the reduction of $E_{\lambda'} := E \otimes M$ modulo λ', for λ' the prime above λ.

We now look at the image of the inertia subgroup in the image of the Galois representation associated to the ℓ-torsion of E. Assume that the reduction $\overline{E}$ is supersingular. The inertia has image isomorphic to a cyclic group of order $(\ell^2{-}1)/m$ or $\ell(\ell{-}1)/m$, where m is less or equal to $3d$, according to the degree of the extension needed to have semi-stable reduction.

The Galois representation has image of order dividing $(\ell{-}1)^2$ by Remark 2.1.2.

The second case leads directly to a contradiction.

In the first case, the image of the inertia is isomorphic to a non-split torus in $\mathrm{GL}_2(\mathbb{F}_\ell)$. On the other hand, it is a subgroup of the image of the Galois representation, which is contained in the normalizer of a split Cartan, as stated in Lemma 1.1.3. Hence, this is impossible unless $(\ell^2{-}1)/m$ divides $(\ell{-}1)^2$. This means that $(\ell{+}1)/m$ divides $(\ell{-}1)$, so $(\ell{+}1)/m$ divides

2, hence, we have that $\ell \leq 2m-1$. The pair $(\ell, j(E))$ is exceptional, so $\ell \equiv 3 \bmod 4$ and $\ell \geq 7$, hence we have the following bound: $\ell \equiv 3 \bmod 4$ and $7 \leq \ell \leq 2m-1 \leq 6d-1$.

We have proved that if $\ell > 2m-1$, the reduction $\overline{E}$ is not supersingular, so it is ordinary since E_λ is semistable over M. By Proposition 2.1.3, the elliptic curve E admits two ℓ-isogenies over $L = K(\sqrt{-\ell})$, which are conjugate over L. By Lemma 1.1.3, the image G of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ acting on $E[\ell](\overline{K})$ is a subgroup of the normalizer N of a split Cartan subgroup C. From Proposition 2.1.3, we know that $N/C \simeq \mathrm{Gal}(L/K)$ is non trivial, so the image of an inertia subgroup I_λ at the place λ of K is a subgroup of G whose image in N/C is non trivial. On the other hand, Proposition 2.3.2 shows that, if $(\ell-1)/m > 2$, then I_λ contains a cyclic subgroup of order larger or equal to 3 (for another argument see [Maz77b, p.118]). It follows that I_λ contains a non-trivial Cartan subgroup (of shape $\left\{ \left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right) | a, b \in \Gamma \right\}$ for a certain non trivial subgroup Γ of $\mathbb{F}_\ell$), even after restriction of the scalars to $\mathrm{Gal}(\overline{M}/M)$. This is a contradiction with Proposition 2.3.2, as the latter says that the restriction of I_λ to $\mathrm{Gal}(\overline{M}/M)$ is a semi-Cartan subgroup (or a Borel). Hence, $(\ell-1)/m \leq 2$ so we have $\ell \equiv 3 \bmod 4$ and $7 \leq \ell \leq 2m+1 \leq 6d+1$. □

Remark 2.3.4. It is clear that Theorem 2.3.3 implies the result of Sutherland for the case $K = \mathbb{Q}$.

The previous theorem leads to prove point (1) of the Main Theorem:

Corollary 2.3.5. *Let $(\ell, j(E))$ be an exceptional pair for the number field K of degree d over $\mathbb{Q}$ and discriminant Δ, assume $j(E)$ different from $\{0, 1728\}$. Then*

$$\ell \leq \max\{\Delta, 6d+1\}.$$

Proof. If $(\ell, j(E))$ is an exceptional pair for the number field K then we distinguish two cases according to the projective image being contained or not in $\mathrm{SL}_2(\mathbb{F}_\ell)/\pm 1$. This corresponds to a condition about $\sqrt{\left(\frac{-1}{\ell}\right)\ell}$ belonging to K or not. If $\sqrt{\left(\frac{-1}{\ell}\right)\ell}$ does not belong to K we apply Theorem 2.3.3 and conclude that $7 \leq \ell \leq 6d+1$. If $\sqrt{\left(\frac{-1}{\ell}\right)\ell}$ is in K, then ℓ divides Δ. □

Chapter 3

Finiteness of exceptional pairs

Given a number field K of degree d over $\mathbb{Q}$ and discriminant Δ, the local-global principles for ℓ-isogenies holds whenever $\ell = 2, 3$ or $\ell > \max\{\Delta, 6d+1\}$ by Corollary 2.3.5 and Proposition 2.1.9. In this chapter we analyse what happens for primes smaller than the bound obtained. In particular we will prove that the local-global principle about ℓ-isogenies for elliptic curves over number fields admits only a finite number of exceptions if $\ell > 7$. We will also study the behaviour of the local-global principle at 5 and 7.

Let K be a number field and let C/K be a projective smooth curve defined over K and genus g. Our arguments will rely on the classical trichotomy between curves of genus 0, 1 and higher. When the genus is 0, the curve is isomorphic to $\mathbb{P}^1_K$ over an algebraic closure of K and therefore $C(K)$, the set of K-rational points, is either empty or infinite. If the genus of C is 1 and $C(K)$ contains at least one point over K then C/K is an elliptic curve over K and the Mordell-Weil Theorem shows that $C(K)$ is a finitely generated abelian group: $C(K) \cong T \oplus \mathbb{Z}^r$, where T is the torsion subgroup and r is a non-negative integer called the rank of the elliptic curve. If $g \geq 2$, Faltings Theorem states that the set of K-rational points is finite.

Let us recall some theory of modular curves, since it will be useful in what follows.

Let $\ell \geq 5$ be a prime number and let $\mathbb{Z}[\zeta_\ell]$ be the subring of $\mathbb{C}$ generated by a root of unity of order ℓ. The modular curve $X(\ell)$ is the compactified fine moduli space which classify pairs (E, α), where E is a generalized elliptic curve over a scheme S over $\mathrm{Spec}(\mathbb{Z}[1/\ell, \zeta_\ell])$ and $\alpha : (\mathbb{Z}/\ell\mathbb{Z})^2_S \xrightarrow{\sim} E[\ell]$ is an isomorphism of group schemes over S which is a full level ℓ-structure, up to isomorphism of pairs i.e. isomorphisms of elliptic curves which preserve the level structure. A full level ℓ-structure on a generalized elliptic curve E over S is a pair of points (P_1, P_2), satisfying $P_1, P_2 \in E[\ell]$ and $e_\ell(P_1, P_2) = \zeta_\ell$ where e_ℓ is the Weil pairing on $E[\ell]$. Let us recall that a full level ℓ-structure corresponds to give a symplectic pairing on $(\mathbb{Z}/\ell\mathbb{Z})^2$ via $\langle (1,0), (0,1) \rangle = \zeta_\ell$. For more details, see [KM85] or [Gro90].

Let G be a subgroup of $GL_2(\mathbb{Z}/\ell\mathbb{Z})$. We will denote as $X_G(\ell) := G\backslash X(\ell)$ the quotient of the modular curve $X(\ell)$ by the action of G on the full level ℓ-structure. The modular curve $X_G(\ell)$ has a geometrically irreducible model over $\mathbb{Q}(\zeta_\ell)^{\det(G)}$, see [Maz77b, pp.115 – 116] or [DR73, IV, 3.20.4].

In particular, if G is the Borel subgroup then $X_G(\ell)$ is the modular curve $X_0(\ell)$ over $\mathbb{Q}$. This modular curve parametrizes elliptic curves with a cyclic ℓ-isogeny, that is, pairs (E, C), where E is a generalized elliptic curve and C is the kernel of a cyclic ℓ-isogeny, up to isomorphism.

If G is a split Cartan subgroup (respectively, the normalizer of a split Cartan subgroup) we will denote the modular curve $X_G(\ell) := X_{\text{sp.Car}}(\ell)$ (respectively, $X_{\text{split}}(\ell)$). The curve $X_{\text{sp.Car}}(\ell)$ (respectively, $X_{\text{split}}(\ell)$) parametrizes elliptic curves endowed with an ordered (respectively, unordered) pair of independent cyclic ℓ-isogenies.

Following Mazur [Maz77b], we will denote as $X_{\mathfrak{A}_4}(\ell)$ (respectively $X_{\mathfrak{S}_4}(\ell)$ and $X_{\mathfrak{A}_5}(\ell)$) the modular curves obtained taking as $G \subset GL_2(\mathbb{Z}/\ell\mathbb{Z})$ the inverse image of $\mathfrak{A}_4 \subset \mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$ (respectively $\mathfrak{S}_4$ and $\mathfrak{A}_5 \subset \mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$). Let us remark that exceptional projective images $\mathfrak{A}_4, \mathfrak{S}_4$ and $\mathfrak{A}_5$ can occur only for particular values of ℓ, see [Ser72, Sections 2.5 and 2.6]. The modular curves $X_{\mathfrak{A}_4}(\ell)$ and $X_{\mathfrak{A}_5}(\ell)$ have geometrically irreducible models over the quadratic subfield of $\mathbb{Q}(\zeta_\ell)$. The same holds for $X_{\mathfrak{S}_4}(\ell)$ if $\ell \not\equiv \pm 3 \bmod 8$, otherwise the model is over $\mathbb{Q}$.

Remark 3.0.6. Let E/K be an elliptic curve which is occurring in an exceptional pair $(\ell, j(E))$ for the number field K. Let us suppose that the projective image of $\rho_{E,\ell}$ is dihedral. Hence, $(E, \rho_{E,\ell})$ corresponds to a K-rational point in $X_{\text{split}}(\ell)$ by Lemma 1.1.3 and Corollary 2.1.6. Moreover, $E[\ell](\overline{K})$ contains two conjugate lines L_1 and L_2 over L/K, where L/K is quadratic (Propositions 2.1.4 and 2.1.8). These lines correspond to the isogenies $\alpha : E \to E/L_1$ and $\beta : E \to E/L_2$ defined over L. Hence, they give a pair of L-rational points (taking respectively $\alpha\beta^\vee$ and $\beta\alpha^\vee$ as isogeny structure) on $X_0(\ell^2)$ which are conjugate by the Fricke involution w_{ℓ^2}, for a definition see [Par05, Section 2]. Let us recall that there exists a isomorphism defined over $\mathbb{Q}$ between $X_0(\ell^2)$ and $X_{\text{sp.Car}}(\ell)$.

Remark 3.0.7. If $(\ell, j(E))$ is an exceptional pair for the number field K and $\sqrt{\left(\frac{-1}{\ell}\right)\ell} \notin K$ then the prime ℓ is congruent to 3 mod 4 and hence to 7 or 11 mod 12, while if $\sqrt{\left(\frac{-1}{\ell}\right)\ell} \in K$ then the prime ℓ is congruent to 1 mod 4 and hence to 1 or 5 mod 12.

3.1 The case $11 \leq \ell \leq \ell_K$

Theorem 3.1.1. *If $\ell > 7$, then the number of exceptional pairs $(\ell, j(E))$, for a given number field K, is finite.*

Proof. Given an exceptional pair $(\ell, j(E))$ for the number field K it corresponds to a K-rational point on one of the following modular curves:

$X_{\mathrm{split}}(\ell)$, $X_{\mathfrak{A}_4}(\ell)$, $X_{\mathfrak{S}_4}(\ell)$ or $X_{\mathfrak{A}_5}(\ell)$, by Lemma 1.1.3 and Lemma 2.1.5. Let us analyse each possible case.

Let us recall that the genus of $X_{\mathrm{split}}(\ell)$ is given by the following formula, for a reference [Maz77b, p.117]:

$$g(X_{\mathrm{split}}(\ell)) = \frac{1}{24}\left(\ell^2 - 8\ell + 11 - 4\left(\frac{-3}{\ell}\right)\right).$$

Hence, if $\ell \equiv 1$ or $7 \bmod 12$, then $g(X_{\mathrm{split}}(\ell)) = \frac{1}{24}(\ell^2 - 8\ell + 7)$. Otherwise, if $\ell \equiv 5$ or $11 \bmod 12$, then $g(X_{\mathrm{split}}(\ell)) = \frac{1}{24}(\ell^2 - 8\ell + 15)$. Therefore, the modular curve $X_{\mathrm{split}}(\ell)$ has genus larger than 2 for $\ell \geq 11$, and it has only finitely many K-rational points by Faltings Theorem.

Let us now study the modular curves $X_{\mathfrak{A}_4}(\ell)$, $X_{\mathfrak{S}_4}(\ell)$ and $X_{\mathfrak{A}_5}(\ell)$. The genus of these modular curves is given by the following formulae, see [CH05, Section 2]:

$$\begin{aligned}
g(X_{\mathfrak{A}_4}(\ell)) &= \frac{1}{288}(\ell^3 - 6\ell^2 - 51\ell + 294 + 18\epsilon_2 + 32\epsilon_3) \\
g(X_{\mathfrak{S}_4}(\ell)) &= \frac{1}{576}(\ell^3 - 6\ell^2 - 87\ell + 582 + 54\epsilon_2 + 32\epsilon_3) \\
g(X_{\mathfrak{A}_5}(\ell)) &= \frac{1}{1440}(\ell^3 - 6\ell^2 - 171\ell + 1446 + 90\epsilon_2 + 80\epsilon_3)
\end{aligned}$$

where ϵ_2 is equal to 1 if $\ell \equiv 1 \bmod 4$ and to -1 if $\ell \equiv 3 \bmod 4$, and ϵ_3 is equal to 1 if $\ell \equiv 1 \bmod 3$ and to -1 if $\ell \equiv -1 \bmod 3$. We stress again that these exceptional cases occur only for certain values of ℓ, see [Ser72, Sections 2.5 and 2.6], and the formulae given will not be integral for general values of ℓ, as already noticed in [CH05, p.3072]. By Corollary 2.1.7 if an exceptional pair has projective image isomorphic to $\mathfrak{A}_4$ then $\ell \equiv 1 \bmod 12$ and we have that the genus of $X_{\mathfrak{A}_4}(\ell)$ is greater than 2 for all $\ell \geq 13$. Similarly for projective image isomorphic to $\mathfrak{S}_4$ or to $\mathfrak{A}_5$ the genus of the respective modular curves is greater than 2 for primes satisfying the appropriate congruence. □

3.2 The case $\ell = 5$

Now we study the local-global principle for 5-isogenies. In order to do so, we recall the structure of $X(5)$ at the cusps. The modular interpretation of $X(5)(\overline{\mathbb{Q}})$ associates with each cusp a Néron polygon $\mathcal{P}$ with 5 sides. The Néron polygon is endowed with the structure of generalized elliptic curve and enhanced with a basis of $\mathcal{P}[5] \cong \mu_5 \times \mathbb{Z}/5\mathbb{Z}$, where μ_5 is the set of 5-th root of unity, up to automorphisms of $\mathcal{P}$:

$$\begin{array}{rcl}
(\{\pm 1\} \times \mu_5) \times \mathcal{P}[5] & \to & \mathcal{P}[5] \\
\left(\begin{pmatrix} \epsilon & \alpha \\ 0 & \epsilon \end{pmatrix}, \begin{pmatrix} w \\ j \end{pmatrix}\right) & \mapsto & \begin{pmatrix} w^\epsilon \alpha^j \\ \epsilon j \end{pmatrix}
\end{array}$$

where $\epsilon \in \{\pm 1\}$ and $\alpha, w \in \mu_n$. The set of cusps of $X(5)(\overline{\mathbb{Q}})$ is a Galois set with an action of $GL_2(\mathbb{Z}/5\mathbb{Z})$. The modular interpretation of $X_G(5)$ associates to each cusp an orbit of the enhanced Néron polygon under the action of the group G.

The local-global principle for 5-isogenies is related with V_4, the Klein 4-group. Let us recall that there is a unique non-trivial 2-dimensional irreducible projective representation τ of V_4 in $\mathrm{PGL}_2(\mathbb{F}_5)$ and, up to conjugation, this representation is given by:

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

For a prime $\ell \geq 5$, we will denote as $X_{V_4}(\ell)$ the modular curves $X_G(\ell)$ obtained taking as $G \subset GL_2(\mathbb{Z}/\ell\mathbb{Z})$ the inverse image of $V_4 \subset \mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

Proposition 3.2.1. *Over* $\mathrm{Spec}(\mathbb{Q}(\sqrt{5}))$*, the modular curve* $X_{V_4}(5)$ *is isomorphic to* $\mathbb{P}^1$*.*

Proof. The genus of $X(5)$ over $\mathbb{Q}(\zeta_5)$ is 0. The field of constants of $X_{V_4}(5)$ is $\mathbb{Q}(\zeta_5)^{\det(G)}$ where G is the inverse image of V_4 in $\mathrm{GL}_2(\mathbb{F}_5)$.

Since $V_4 \subset \mathrm{SL}_2(\mathbb{F}_5)/\{\pm 1\}$ and $\mathbb{F}_5^* \subset G$, then $\det(G) = (\mathbb{F}_5^*)^2$. This means that $X_{V_4}(5)$ is geometrically irreducible over $Q(\sqrt{5})$ and its genus is 0.

The set of cusps of $X(5)(\overline{\mathbb{Q}})$ is in $1-1$ correspondence with the quotient of the group of isomorphisms as $\mathbb{F}_5$-vector spaces between $\mathbb{F}_5^2$ and $\mu_5 \times \mathbb{F}_5$ by the action of $\{\pm 1\} \times \mu_5$.

To show that over $\mathrm{Spec}(\mathbb{Q}(\sqrt{5}))$ the modular curve $X_{V_4}(5)$ is isomorphic to $\mathbb{P}^1$ it is enough to show that the set of $\mathbb{Q}(\sqrt{5})$-rational points of $X_{V_4}(5)$ is not empty.

Let $\phi_{\zeta_5} : \mathbb{F}_5^2 \xrightarrow{\sim} \mu_5 \times \mathbb{F}_5$ be the isomorphism given by $\phi_{\zeta_5}((1,0)) = (\zeta_5, 0)$, $\phi_{\zeta_5}((0,1)) = (1,1)$. The orbit of the cusp corresponding to ϕ_{ζ_5} under the action of $\{\pm 1\} \times \mu_5$ is the following set:

$$\begin{aligned}&\{((\zeta_5,0),(1,1)),((\zeta_5^{-1},0),(1,-1)),((\zeta_5,0),(\zeta_5,1)),((\zeta_5^{-1},0),(\zeta_5^{-1},-1)),\\ &((\zeta_5,0),(\zeta_5^{2},1)),((\zeta_5^{-1},0),(\zeta_5^{-2},-1)),((\zeta_5,0),(\zeta_5^{-2},1)),\\ &((\zeta_5^{-1},0),(\zeta_5^{2},-1)),((\zeta_5,0),(\zeta_5^{-1},1)),((\zeta_5^{-1},0),(\zeta_5,-1))\}.\end{aligned}$$

On the set of cusps we have a Galois action by $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$. In particular, acting with $-1 \in \mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ on the cusp $((\zeta_5,0),(1,1))$ we obtain the cusp $((\zeta_5^{-1},0),(1,1))$ which does not define the same cusps on $X(5)(\overline{\mathbb{Q}})$. However, the action of -1 on the class of the cusp $((\zeta_5,0),(1,1))$ preserve

the orbit of the cusp under G: in fact G, inverse image of V_4 in $\mathrm{GL}_2(\mathbb{F}_5)$, is the group given by

$$\left\{ \begin{pmatrix} x & 0 \\ 0 & \pm x \end{pmatrix}, \begin{pmatrix} 0 & \pm x \\ x & 0 \end{pmatrix} \middle| x \in \mathbb{F}_5^* \right\},$$

and under the action of $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \in G$ we have that the cusp $((\zeta_5^{-1}, 0), (1, 1))$ of $X(5)(\overline{\mathbb{Q}})$ is mapped to $((\zeta_5, 0), (1, 1))$.

It follows that the cusp $((\zeta_5, 0), (1, 1))$ in $X_{V_4}(5)(\overline{\mathbb{Q}})$ is stable under the action of $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}(\sqrt{5}))$. This implies that $X_{V_4}(5)(\mathbb{Q}(\sqrt{5}))$ is non-empty. □

Corollary 3.2.2. *There exist infinitely many exceptional pairs $(5, j(E))$ for the number field K if and only if $\sqrt{5}$ belongs to K.*

Proof. By Proposition 2.1.9, there is an exceptional pair $(5, j(E))$ for the number field K only if $\sqrt{5}$ belongs to K.

If $(5, j(E))$ is an exceptional pair for the number field K then the projective image of the Galois representation associated to the elliptic curve E over K is a dihedral group of order dividing 8 (Lemma 2.1.5 combined with Corollary 2.1.7). In particular, the image projective image of the Galois representation can be the Klein 4-group V_4. By Proposition 3.2.1, over $\mathrm{Spec}(\mathbb{Q}(\sqrt{5}))$ the modular curve $X_{V_4}(5)$ is isomorphic to $\mathbb{P}^1$, then $X_{V_4}(5)(K)$ is non-empty if and only if $\sqrt{5}$ belongs to K. In particular, if $\sqrt{5}$ belongs to K then there exist infinitely many exceptional pairs $(5, j(E))$ since $X_{V_4}(5)$ is isomorphic to $\mathbb{P}^1$ over $\mathrm{Spec}(K)$. □

3.3 The case $\ell = 7$

The local-global principle for 7-isogenies leads us to a dichotomy between a finite and an infinite number of counterexamples according to the rank of a specific elliptic curve that we call the Elkies-Sutherland curve:

Proposition 3.3.1. *If $\ell = 7$ then the number of exceptional pairs $(7, j(E))$ for a number field K, is finite or infinite, depending on the rank of the elliptic curve*

$$E' : y^2 = x^3 - 1715x + 33614$$

being 0 or positive respectively.

Proof. If $\sqrt{-7} \in K$ then by Lemma 2.1.5 there is no exceptional pair. Let us suppose that $\sqrt{-7}$ is not in K. As shown by Sutherland in [Sut12, Section 3] and explained in Remark 3.0.6, the modular curve to deal with is the twist of $X_0(49)$ by $\mathrm{Gal}(K(\sqrt{-7})/K)$ with respect to w_{49}, the Fricke involution on $X_0(49)$.

Using the computations done by Elkies, as stated in [Sut12, Section 3], we have that each $K(\sqrt{-7})$-rational point of E' corresponds to a class of isomorphism of elliptic curves over K, such that every elliptic curve in the class gives an exceptional pair at 7. Explicitly, if the $K(\sqrt{-7})$-rational point of E' has coordinates (u, v), let $t = (3u - v + 42)/(u + 2v)$, then the j-invariant of the isomorphism class of elliptic curves which are exceptional for the local-global principle for 7-isogenies is equal to

$$\frac{-(t-3)^3(t-2)(t^2+t-5)^3(t^2+t+2)^3(t^4-3t^3+2t^2+3t+1)^3}{(t^3-2t^2-t+1)^7}.$$

Hence, if the rank of E' over K is positive there are infinitely many counterexamples to the local-global principle about 7-isogenies, while if the rank is 0 there are only finitely many. □

Remark 3.3.2. As shown by Sutherland in [Sut12, Section 3], over $\mathbb{Q}(i)$ the curve E has positive rank, so there are infinitely many counterexamples on this field to the local-global principle about 7-isogenies.

The proof of our Main Theorem is now complete.

Examples for the case $\ell = 7$

Let E be an elliptic curve defined over a number field K. The global L-series $L_E(s, K)$ of E, see [Sil09, p.449], is formally defined by the Euler product:

$$L_E(s,K) = \prod_{\substack{v \\ \text{good reduction}}} (1 - a_v q_v^{-s} + q_v^{1-2s})^{-1} \cdot \prod_{\substack{v \\ \text{bad reduction}}} (1 - a_v q_v^{-s})^{-1}$$

where q_v is the cardinality of the residue field k_v of K at v and if E has bad reduction at v then $a_v = 0, 1$ or -1 according to the reduction type, while if E has good reduction at v then a_v satisfies $|\overline{E}(k_v)| = q_v + 1 - a_v$.

The following conjectures are related to the L-function attached to an elliptic curve over a number field:

Conjectures. *Let E/K be an elliptic curve over a number field K.*

- **Hasse-Weil Conjecture.** *The L-function $L_E(s, K)$ has an analytic continuation to $\mathbb{C}$ and satisfies a functional equation*

$$L_E^*(s,K) = w(E/K)L_E^*(2-s,K),$$

  where $w(E/K)$ is called root number and determines the sign of the functional equation.
- **Birch-Swinnerton-Dyer Conjecture.** *The L-function $L_E(s, K)$ satisfies:* $\operatorname{ord}_{s=1} L_E(s,K) = r$, *where r is the rank of $E(K)$.*
- **Parity Conjecture**:$(-1)^r = w(E/K)$.

3.3 The case $\ell = 7$

Let E be the elliptic curve $y^2 = x^3 - 1715x + 33614$ over a number field K, not containing $\sqrt{-7}$. If we assume that the parity conjecture holds true, then if the rank of the L-function $L_E(s, K)$ is odd, there are infinitely many counterexamples to the local-global principle about 7-isogenies.

For $\mathbb{Q}(\sqrt{-23})$, by an easy computation in SAGE, it is possible to show that $L_E(s, \mathbb{Q}(\sqrt{-23}))$ has odd analytic rank, hence the curve E has positive rank, so there are infinitely many counterexamples on this field to the local-global principle about 7-isogenies. Note that, since this is a degree 2 extension of $\mathbb{Q}$, according to Theorem 2.3.3, the only primes for which the local-global principle could fail are 7, 11 and 23. For 11 and 23 there are only finitely many counterexamples by our Main Theorem.

On the other hand, using SAGE, we have been able to show that the rank of the elliptic curve $y^2 = x^3 - 1715x + 33614$ is zero on the number fields $\mathbb{Q}(\sqrt{-D})$ for D in the following table:

$\mathbb{Q}(\sqrt{-14})$	$\mathbb{Q}(\sqrt{-119})$	$\mathbb{Q}(\sqrt{-210})$
$\mathbb{Q}(\sqrt{-21})$	$\mathbb{Q}(\sqrt{-133})$	$\mathbb{Q}(\sqrt{-217})$
$\mathbb{Q}(\sqrt{-35})$	$\mathbb{Q}(\sqrt{-154})$	$\mathbb{Q}(\sqrt{-231})$
$\mathbb{Q}(\sqrt{-42})$	$\mathbb{Q}(\sqrt{-161})$	$\mathbb{Q}(\sqrt{-238})$
$\mathbb{Q}(\sqrt{-91})$	$\mathbb{Q}(\sqrt{-182})$	$\mathbb{Q}(\sqrt{-259})$
$\mathbb{Q}(\sqrt{-105})$	$\mathbb{Q}(\sqrt{-203})$	$\mathbb{Q}(\sqrt{-287})$

Table 3.1: Number fields over which $y^2 = x^3 - 1715x + 33614$ has rank 0.

We have obtained this list using the fact that the L-function of E over a quadratic extension of the rational by $\sqrt{d}$, for an integer d, is equal to the product of the L-function of E over $\mathbb{Q}$ times the L-function of the d-quadratic twist of E over $\mathbb{Q}$.

Remark 3.3.3. The list given in Table 3.1 can be explained using half integer weight modular forms and Waldspurger's formula, see [Wal81]. We will not treat this topic in this dissertation, since it is far beyond our purposes. Let us just underline that Waldspurger's formula leads to link coefficients of half integer weight modular forms to values at 1 of the global L-function of elliptic curves. The table [PT07, Table 6.3] is particularly relevant for the Elkies-Sutherland elliptic curve.

Part II

Images of residual modular Galois representations

Chapter 4

Introduction and Preliminaries

For any pair of positive integers n and k, called respectively level and weight, we define the following objects: $M(n,k)_{\mathbb{C}}$, the complex vector space of modular forms of weight k on $\Gamma_1(n)$ and $S(n,k)_{\mathbb{C}}$, the subspace of cusp forms. Let $\mathbb{T}$ be the associated Hecke algebra, i.e. the $\mathbb{Z}$-subalgebra of $\mathrm{End}_{\mathbb{C}}(S(n,k)_{\mathbb{C}})$ generated by the Hecke operators T_p for every prime p and the diamond operators $\langle d\rangle$ for every $d \in (\mathbb{Z}/n\mathbb{Z})^*$. The Hecke algebra $\mathbb{T}$ is finitely generated as a $\mathbb{Z}$-module, for further details see [EC11, Theorem 2.5.11] or [DS05, p.234]. Whenever needed, we will stress the weight and the level for the Hecke algebra changing the notation to $\mathbb{T}(n,k)$. We will also write $S(\Gamma_1(n),k)_{\mathbb{C}}$ if we want to stress the level structure, otherwise we will use the notation $S(n,k)_{\mathbb{C}}$. Let us fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$, we will denote as $G_{\mathbb{Q}}$ the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. We have the following result, see [DS74, Théorème 6.7] or [EC11, Theorem 2.5.2], due to Shimura and Deligne:

Theorem 4.0.4. *Let n and k be positive integers. Let $\mathbb{F}$ be a finite field, ℓ its characteristic, and $f : \mathbb{T} \to \mathbb{F}$ a morphism of rings. Then there is a continuous semi-simple representation $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F})$ that is unramified outside $n\ell$ such that for all primes p not dividing $n\ell$ we have:*

$$\mathrm{Trace}(\rho_f(\mathrm{Frob}_p)) = f(T_p) \text{ and } \det(\rho_f(\mathrm{Frob}_p)) = f(\langle p\rangle)p^{k-1} \text{ in } \mathbb{F}.$$

Such a ρ_f is unique up to isomorphism.

A ring morphism as in Theorem 4.0.4 corresponds to an eigenform with coefficients in $\mathbb{F}$, for more details see [EC11, p.58].

The space $S(n,k)_{\mathbb{C}}$ is decomposed by characters:

$$S(n,k)_{\mathbb{C}} := \bigoplus_{\epsilon:(\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*} S(n,k,\epsilon)_{\mathbb{C}}$$

where $S(n,k,\epsilon)_{\mathbb{C}} := \{f \in S(n,k)_{\mathbb{C}} | \forall d \in (\mathbb{Z}/n\mathbb{Z})^*, \langle d\rangle f = \epsilon(d)f\}$.

We associate a Hecke algebra to each $S(n,k,\epsilon)_{\mathbb{C}}$, as before. This Hecke algebra, that we will denote as $\mathbb{T}_\epsilon$, is the $\mathcal{O}_\epsilon$-subalgebra in the complex endomorphism ring of $S(n,k,\epsilon)_{\mathbb{C}}$ generated by the Hecke operators T_n for $n \geq 1$, where $\mathcal{O}_\epsilon$ is the sub-ring of $\mathbb{C}$ generated by the image of the character

ϵ. Note that the algebra $\mathbb{T}_\epsilon$ is free of finite rank as a $\mathbb{Z}$-module. The Hecke algebra $\mathbb{T}_\epsilon$ is a quotient of the Hecke algebra $\mathbb{T}$:

$$\mathrm{I} \hookrightarrow \mathbb{T} \twoheadrightarrow \mathbb{T}_\epsilon$$

where the ideal I is given by $\mathrm{I} := (\langle d \rangle - \epsilon(d) | d \in (\mathbb{Z}/n\mathbb{Z})^*)$, and the quotient map is defined by restriction of Hecke operators, and the obvious identification for diamond operators, for an idea of the proof see [Wie05, Proposition 3.3.5]. Then we deduce the following corollary from Theorem 4.0.4:

Corollary 4.0.5. *Let n and k be positive integers, let $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character and let $f : \mathbb{T}_\epsilon \to \overline{\mathbb{F}}_\ell$ be a morphism of rings. Then there is a continuous semi-simple representation $\rho_f : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ that is unramified outside $n\ell$, such that for all primes p not dividing $n\ell$ we have:*

$$\mathrm{Trace}(\rho_f(\mathrm{Frob}_p)) = f(T_p) \text{ and } \det(\rho_f(\mathrm{Frob}_p)) = f(\langle p \rangle) p^{k-1} \text{ in } \overline{\mathbb{F}}_\ell.$$

Such a ρ_f is unique up to isomorphism.

A ring morphism of this type corresponds to a mod ℓ eigenform with character $\overline{\epsilon} : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell$ given by $a \mapsto \overline{\epsilon}(a) := f(\langle a \rangle)$ for $a \in (\mathbb{Z}/n\mathbb{Z})^*$.

Let us recall that the Hecke algebra $\mathbb{T}$ and the Hecke algebra $\mathbb{T}_\epsilon$ for level n and weight $k \geq 2$ and character $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathcal{O}_\epsilon$ can be computed in polynomial time in n and k, using deterministic algorithms based on modular symbols; for an explicit computation of Hecke operators see [Ste07, Chapter 8] and for the computation of $\mathbb{T}$ and $\mathbb{T}_\epsilon$ see [Ste07, Chapter 9, Theorem 9.23 and Theorem 9.22].

Our goal is to outline of an algorithm, which receives as input: n and k positive integers, a prime ℓ not dividing n and such that $2 \leq k \leq \ell + 1$, a character $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ and a morphism of rings $f : \mathbb{T}_\epsilon(n, k) \to \overline{\mathbb{F}}_\ell$, and which gives as output the image of the Galois representation ρ_f, given by Corollary 4.0.5, up to conjugation, as a subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$, in a reasonable time.

Moreover, we want to have an "efficient" algorithm, i.e. an algorithm which gives the aforementioned output computing the lowest possible number of Hecke operators and their image through the ring morphism f. In Chapter 6, we will explain more about this efficiency problem and describe the strategy we followed.

Remark 4.0.6. The algorithm outlined in the second part of thesis takes as input: a pair of positive integers n and k, a prime ℓ not dividing n and such that $2 \leq k \leq \ell + 1$, a character $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ and a morphism of ring $f : \mathbb{T}_\epsilon(n, k) \to \overline{\mathbb{F}}_\ell$. It gives as output the image of the associated Galois representation ρ_f up to conjugation. Is this enough to obtain all possible

images of residual modular Galois representations i.e. of all continuous odd representations $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$?

If n and ℓ are not coprime, say $n = \ell^a m$ with $a \geq 0$ and m not divisible by ℓ, then the representation attached to an eigenform for $\Gamma_1(n)$ over a finite field of characteristic ℓ also arises from an eigenform for $\Gamma_1(m)$ of possibly different weight than k: see [Ser87, p.195 Remarque]. In fact, thanks to Ribet level lowering, see [Rib94] for $\ell \geq 3$ and [Buz00] for $\ell = 2$, there exists a morphism of ring $f' : \mathbb{T}_\epsilon(m, k') \to \overline{\mathbb{F}}_\ell$, for $k' \geq k$, such that $\rho_{f'} \cong \rho_f$. If the weight k is not between 2 and $\ell + 1$, then there exists an eigenform g in the same level but of weight $2 \leq k' \leq \ell + 1$ such that ρ_g is isomorphic to $\rho_f \otimes \chi_\ell^a$, that is the twist of the representation ρ_f by a powers of the modℓ cyclotomic character χ_ℓ^a, for $a \in \mathbb{Z}/(\ell - 1)\mathbb{Z}$, see [Edi92, Theorem 3.4]. In Chapter 8 we will study the problem of twisting.

Therefore, the restrictions upon the choice of n, ℓ and k do not give any loss of generality.

In Part II of this thesis we outline an algorithm for computing the image of a residual modular 2-dimensional semi-simple Galois representation. This means that the algorithm will determine the image as a finite subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$, up to conjugation, as well as certain local properties of the representation and tabulate the result in a database.

Two different mod ℓ modular forms can give rise to the same Galois representation: the coefficients indexed by the primes dividing the level and the characteristic may differ. Hence, either we solve this problem mapping the form to a higher level, or we study how to describe the coefficients at primes dividing the level and the characteristic, so that we can list all possibilities. In order to describe these coefficients, it is needed to know local properties of the Galois representation, i.e. the restriction of the representation to the decomposition group at the corresponding primes.

Associated to the algorithm there is a database which stores all the data obtained. The algorithm is cumulative and built with a bottom-up approach: for any new level n, we will store in the database the system of eigenvalues at levels dividing n and weights smaller than the weight considered, so that there will be no need to re-do the computations if the representation arises from lower level or weight.

Similarly, if a Galois representation arises as a twist of a representation of lower conductor, the algorithm will detect such data and it will not re-do any computation to determine the projective image of the representation: it is already stored in the database. On the other hand, once the data at a certain level is computed, the database will fill in all the contribution at higher level coming from degeneracy morphism and twisting, so that the computation at a certain level will be performed only when we are dealing with a new object.

Let us introduce shortly the design of the algorithm, this is done in details in Chapter 11.

The algorithm follows results of Dickson, Khare-Wintenberger and Faber on the classification, up to conjugation, of the finite subgroups of $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$.

For every data not coming from lower level or weight, we determine if the associate representation is reducible or not. If the representation is irreducible, then we compute the field of definition of the representation, see Proposition 9.1.1.

In order to determine the image up to conjugation, as shown in Chapter 5, it is enough to know the projective image of the representation, up to conjugation, and the set of determinants. Hence, we compute the field of definition of the projective representation, see Proposition 9.2.1, Proposition 9.2.2 and Algorithm 9.2.3.

To decide about the projective image of the representation we perform a list of checks according to Dickson's classification, unless the representation arises from twisting of a representation of lower conductor, in which case the projective image is already stored in the database. In Chapter 10 we show how to verify that a representation has projective image of dihedral type or isomorphic to either $\mathfrak{A}_4$, or $\mathfrak{S}_4$ or $\mathfrak{A}_5$. In the latter case, we relate such projectively exceptional image to data coming from characteristic 2, 3 and 5, for more details see Proposition 10.2.1 and the related section in Chapter 10. Once we have excluded all exceptional cases i.e. all cases in which the image is exceptional, see Definition 5.1.3, the image is "big", meaning that it contains the special linear group of degree 2 of the extension of $\mathbb{F}_\ell$ corresponding to the field of definition of the projective image.

The representation ρ_f can be computed, as explained in [EC11], in time polynomial in n, k and the cardinality of $\mathbb{F}$, where $\mathbb{F}$ is a finite field of characteristic ℓ where the representation is defined, ℓ not dividing n.The computation of the image of a residual 2-dimensional odd semi-simple Galois representation is a totally different matter than the computation of the representation itself: in particular, there is no need to know explicitly the representation in order to compute its image.

Part II of this thesis is organized as follows.

In the next sections of this chapter, we introduce the necessary preliminaries on Katz modular forms and Serre's conjecture, which nowadays is Khare--Wintenberger Theorem. The set-up of these sections is towards a quick introduction of the material and notation we need. The reader is therefore encouraged to consult the references given in each section, in which this material, and much more, is explained.

In Chapter 5 we explain how the image will be described and we prove that any finite subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ occurring as image of an irreducible odd

representation is determined, up to conjugation in $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$, by its projective image and its set of determinants. This is done through a case-by-case analysis using Dickson's classification.

In Chapter 6 we prove that working with coefficients up to the Sturm bound is enough to check isomorphism between residual modular semi-simple 2-dimensional Galois representations coming from forms of the same level and weight. In particular, see Theorem 6.3.5 and Theorem 6.3.6 in which we deal with the coefficients indexed by the primes dividing the level and the characteristic.

In Chapter 7 we deal with reducible representations. The main idea of this chapter is to check equalities between mod ℓ modular forms and the reduction modulo ℓ of certain Eisenstein series, see Theorem 7.2.3.

Twisting a representation by a character is a basic operation in representation theory. In order to describe the projective image of the representation we are studying, we investigate the conductor of the twist and the local description of the representation at primes dividing the conductor. The problem of twisting a representation by a character is studied in Chapter 8, where several useful results are collected about the conductor of the twist, see Proposition 8.2.1, Proposition 8.2.4 and Proposition 8.2.6. Moreover, we outline an algorithm which returns the local description of the representation at the primes dividing the level and the characteristic, see Algorithm 8.2.9.

In Chapter 9, results about the field of definition of the representation and of the projective representation are presented, see Proposition 9.1.1, Proposition 9.2.1 and Proposition 9.2.2. In particular, we prove that, if the representation is irreducible and does not arise from lower level or weight, then the coefficients up to the Sturm bound are enough to determine the field of definition of the linear representation. In the case of the field of definition of the projective representation, we give a characterization and an algorithm to compute it, see Algorithm 9.2.3.

In Chapter 10 we deal with irreducible representations with projective image of dihedral type or projectively exceptional type, i.e. projectively isomorphic to the symmetric group on 4 elements or the alternating group on 4 or 5 elements. In the projective dihedral case we show the existence of a twist for the representation and we describe the character for which such a twist occurs, see Proposition 10.1.1 and Corollary 10.1.2. When the image is projectively exceptional, we give a new approach and a construction for these kinds of representations, using representation theory and the Khare-Wintenberger Theorem.

The outlined algorithm is summarized in Chapter 11, where also an explanation of the associate database is given.

In the appendix, we analyse degeneracy maps between modular curves and

we deduce results about residual modular Galois representations and their level of realization, see Theorem A.3.1. These results are not used in the algorithm.

4.1 Katz modular forms

For n and k positive integers, a prime ℓ not dividing n, an algebraic closure $\overline{\mathbb{F}}_\ell$ of $\mathbb{F}_\ell$, let $M(\Gamma_1(n),k)_{\overline{\mathbb{F}}_\ell}$ be the space of Katz modular forms of weight k for $\Gamma_1(n)$ on $\overline{\mathbb{F}}_\ell$, see [Kat73], [Kat77] and [Edi92]. Let $S(\Gamma_1(n),k)_{\overline{\mathbb{F}}_\ell}$ be the subspace of $M(\Gamma_1(n),k)_{\overline{\mathbb{F}}_\ell}$ whose elements have q-expansions that are power series with constant term zero at all cusps. We will write $S(\Gamma_1(n),k)_{\overline{\mathbb{F}}_\ell}$ (respectively $M(\Gamma_1(n),k)_{\overline{\mathbb{F}}_\ell}$) if we want to stress the level structure, otherwise we will use the notation $S(n,k)_{\overline{\mathbb{F}}_\ell}$ (respectively $M(n,k)_{\overline{\mathbb{F}}_\ell}$). It is possible to define Hecke operators and diamond operators on the space of Katz modular forms of weight k for $\Gamma_1(n)$ on $\overline{\mathbb{F}}_\ell$, hence a Hecke algebra, see [Gro90, Section 3] or [Kat73, 1.11].

Let us recall that, in weight at least 2 and characteristic larger than 3, every Katz cusp form on $\Gamma_1(n)$ is classical, see [Ser87], i.e. reduction of a characteristic zero form of the same level and weight, see [Kat73, Theorem 1.8.1 and Theorem 1.8.2] and [DI95, Theorem 12.3.2]. The reduction map is the map from $S(\Gamma_1(n),k)_{\overline{\mathbb{Z}}_\ell}$ to $S(\Gamma_1(n),k)_{\overline{\mathbb{F}}_\ell}$, where $\overline{\mathbb{Z}}_\ell$ is the integral closure of $\mathbb{Z}_\ell$ in $\overline{\mathbb{Q}}_\ell$ and the space $S(\Gamma_1(n),k)_{\overline{\mathbb{Z}}_\ell}$ is the module of ℓ-adic cusp forms in the sense of Katz, see [Kat73, Section 2.2.0]. In particular, the following lemma holds:

Lemma 4.1.1 ([Edi97, Lemma 1.9, 1]). *Let ℓ be a prime, $n \geq 1$ an integer not divisible by ℓ and $k \geq 2$ an integer. If $n \neq 1$ or if $\ell > 3$ then the map $S(\Gamma_1(n),k)_{\overline{\mathbb{Z}}_\ell} \to S(\Gamma_1(n),k)_{\overline{\mathbb{F}}_\ell}$ is surjective.*

For any character $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$, let $M(\Gamma_1(n),k,\epsilon)_{\overline{\mathbb{F}}_\ell}$ denote the $\overline{\mathbb{F}}_\ell$-submodule of $M(\Gamma_1(n),k)_{\overline{\mathbb{F}}_\ell}$ of elements f such that for all $d \in (\mathbb{Z}/n\mathbb{Z})^*$, $\langle d\rangle f = \epsilon(d)f$. If f is a non-zero element of $M(\Gamma_1(n),k)_{\overline{\mathbb{F}}_\ell}$ which is an eigenform, then there is a unique character $\overline{\epsilon} : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ such that $f \in M(\Gamma_1(n),k,\overline{\epsilon})_{\overline{\mathbb{F}}_\ell}$. For any character $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$, let

$$S(\Gamma_1(n),k,\epsilon)_{\overline{\mathbb{F}}_\ell} := \{f \in S(\Gamma_1(n),k)_{\overline{\mathbb{F}}_\ell} | \forall d \in (\mathbb{Z}/n\mathbb{Z})^*, \langle d\rangle f = \epsilon(d)f\}$$

be the space of Katz cusp forms of weight k for $\Gamma_1(n)$ and character ϵ. To shorten the notation, when there is no need to stress the level structure, we will use $S(n,k,\epsilon)_{\overline{\mathbb{F}}_\ell}$ instead of $S(\Gamma_1(n),k,\epsilon)_{\overline{\mathbb{F}}_\ell}$ (similarly for $M(\Gamma_1(n),k,\epsilon)_{\overline{\mathbb{F}}_\ell}$).

Let us remark that, also in this case, not all Katz modular forms are reduction of forms in characteristic zero. Indeed, the following map is not always

surjective:

$$S(n,k,\tilde{\epsilon})_{\mathcal{O}_{\tilde{\epsilon}}} \to S(n,k,\overline{\epsilon})_{\mathbb{F}},$$

where $\mathcal{O}_{\tilde{\epsilon}}$ is the ring of integers of the number field where the lift $\tilde{\epsilon}$ of ϵ is defined, $\mathbb{F}$ is the residue field of $\mathcal{O}_{\tilde{\epsilon}}$ at a prime above ℓ, and $S(n,k,\tilde{\epsilon})_{\mathcal{O}_{\tilde{\epsilon}}}$ is the subspace of $S(n,k,\tilde{\epsilon})_{\mathbb{C}}$ which contains cusp forms whose q-expansion has coefficients in $\mathcal{O}_{\epsilon}$. In fact, the following lemma, which is analogous to Lemma 4.1.1, holds:

Carayol's Lemma. *Let $n,\ k \geq 2$ be positive integers and ℓ be a prime not dividing n. Let $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{Z}}_\ell^*$ be a character with $\epsilon(-1) = (-1)^k$, and let $\overline{\epsilon} : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ be its reduction.*

1. *If $\ell \geq 5$ then the map $M(n,k,\epsilon)_{\overline{\mathbb{Z}}_\ell} \to M(n,k,\overline{\epsilon})_{\overline{\mathbb{F}}_\ell}$ is surjective.*
2. *If $f \in M(n,k,\overline{\epsilon})_{\overline{\mathbb{F}}_2}$ is an eigenform with ρ_f irreducible and f is not the reduction of a form in characteristic zero, then ρ_f is induced from $\mathbb{Q}(\sqrt{-1})$.*
3. *If $f \in M(n,k,\overline{\epsilon})_{\overline{\mathbb{F}}_3}$ is an eigenform with ρ_f irreducible and f is not reduction of a form in characteristic zero, then ρ_f is induced from $\mathbb{Q}(\sqrt{-3})$.*

For a proof of this statement see [Car89] and [Edi97].

Let us also recall that if $n > 4$ is an integer and ℓ is a prime not dividing n, then the space of mod ℓ cusp forms $S(\Gamma_1(n),k)_{\overline{\mathbb{F}}_\ell}$ is isomorphic to the space of global sections of the line bundle $\omega^{\otimes k}(-\text{Cusps})$ on the modular curve $X_1(n)_{\overline{\mathbb{F}}_\ell}$. Analogously, $M(\Gamma_1(n),k)_{\overline{\mathbb{F}}_\ell}$ is isomorphic to $\mathrm{H}^0(X_1(n)_{\overline{\mathbb{F}}_\ell}, \omega^{\otimes k})$, see [Gro90, Proposition 2.2] and for details on modular curves see [KM85] and [Gro90].

The Hasse invariant and the derivation θ_ℓ

There exists a unique modular form $A_\ell \in M(\Gamma_1(1), \ell-1)_{\overline{\mathbb{F}}_\ell}$, the Hasse invariant in characteristic ℓ, that has q-expansion 1 at all cusps; see [KM85, 12.4]. Let ℓ be a prime not dividing n, if f is a Katz modular form on $\overline{\mathbb{F}}_\ell$ of weight $k \geq 2$, for $\Gamma_1(n)$, which is an eigenform, then the product $A_\ell f$ is an eigenform of weight $k+\ell-1$ for $\Gamma_1(n)$. Using this property, we can find examples of non-liftable mod ℓ modular forms, for instance: $A_2\Delta$, which is a cusp form of level 1 and weight 13 over $\mathbb{F}_2$, and $A_3\Delta$, which is a cusp form of level 1 and weight 14 over $\mathbb{F}_3$.

Let ℓ be a prime, n and k be positive integers such that $(\ell, n) = 1$ and $2 \leq k \leq \ell+1$. Let $f \in S(\Gamma_1(n),k)_{\overline{\mathbb{F}}_\ell}$ be an eigenform, then the systems of eigenvalues attached to f and to $A_\ell f$ are the same. This follows from [Gor02, Theorem 5.4 and Section 5.3].

Let θ_ℓ be the derivation on modular forms over $\overline{\mathbb{F}}_\ell$ defined by Katz in [Kat77]. It increases weights by $\ell+1$ and acts on q-expansions at all cusps as $q\,d/dq$. In particular, if f is a Katz modular form on $\overline{\mathbb{F}}_\ell$ which is an eigenform and whose q-expansion at some cusp is non-constant, then $\theta_\ell(f)$ is an eigenform with $T_\ell\theta_\ell(f) = 0$. Moreover, the Galois representations of f and $\theta_\ell(f)$ are twists of each other by the mod ℓ cyclotomic character: $\rho_{\theta_\ell(f)} \cong \chi_\ell \otimes \rho_f$, see [Edi92, Section 3.1].

Let f be a Katz modular form on $\overline{\mathbb{F}}_\ell$ whose q-expansion at some cusp is constant, then the weight of f is a multiple of $\ell-1$; see [Kat77, Section 1]. This implies that f is a scalar multiple of a power of A_ℓ, so the q-expansion of f at every cusp is constant. Furthermore, each Hecke operator T_p with p a prime number not dividing $n\ell$ acts on f as multiplication by $(p+1)/p$. So, it follows that f is an eigenform for those Hecke operators. Moreover, this implies that the Galois representation ρ_f is isomorphic to $1 \oplus \chi_\ell^{-1}$.

Proposition 4.1.2 ([Kat77, Corollary (5) and (6)])**.** *Let ℓ be a prime, n and k be positive integers such that $(\ell, n) = 1$ and $2 \le k \le \ell+1$. If $f \in M(\Gamma_1(n), k)_{\overline{\mathbb{F}}_\ell}$ is such that $\theta_\ell(f) = 0$, then f has a unique expression of the form*

$$f = A_\ell^r g^\ell,$$

where the integer r satisfies $0 \le r \le \ell-1$ and $r+k \equiv 0 \bmod \ell$, and the form g belongs to $M(\Gamma_1(n), j)_{\overline{\mathbb{F}}_\ell}$ where j satisfies $\ell j + r(\ell-1) = k$.

Corollary 4.1.3. *Let $\ell \ge 5$ be a prime and n a positive integer not divisible by ℓ. If $f \in M(\Gamma_1(n), \ell+1)_{\overline{\mathbb{F}}_\ell}$ is such that $\theta_\ell(f) = 0$, then $f = 0$.*

Proof. If $\theta_\ell(f) = 0$ then by Proposition 4.1.2 we have that there exist an integer r and a constant c such that $f = c \cdot A_\ell^r$. This implies that $\ell - 1$ divides $\ell + 1$ and this can occur if and only if $\ell = 2, 3$. □

4.2 Khare-Wintenberger Theorem

A crucial ingredient that we use to compare Katz eigenforms is modularity i.e. Serre's conjecture. This conjecture in its strong form has been proved by Khare and Wintenberger, in [KW09a] and [KW09b], using results of Kisin.

Let ℓ be a prime, a continuous Galois representation

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}\,/\mathbb{Q}\,) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$$

has a conductor, $\mathrm{cond}(\rho)$, and a weight, $k(\rho)$, for the definitions of these integers and a more complete explanation we refer to [Ser87, Section 1.2 and Section 2] and to [Edi92, Section 4]: $k(\rho)$ for us is the minimal weight in the sense of [Edi92].

Let us briefly recall the definition of the conductor. The representation ρ is continuous, therefore its image is a finite group and it is isomorphic to the Galois group of a number field K. Hence, ρ is unramified at all but finitely many primes. The number $\mathrm{N}(\rho)$ is the Artin conductor of ρ away from ℓ. Let p be a prime number different from ℓ. Let I_p denote the inertia subgroup at p of G corresponding to a place of K above p, and let $I_p = G_{0,p} \supset G_{1,p} \supset \cdots$ be the higher ramification subgroups: $G_{i,p}$ is the subgroup of the decomposition group, that we will denote as G_p, at the chosen place whose elements act trivially on the ring of integers modulo the $(i+1)$th power of the maximal ideal. The valuation of $\mathrm{N}(\rho)$ at p, that we will denote as $\mathrm{N}_p(\rho)$ is given by the formula, see [Ser78, pp.171-174]:

$$\mathrm{N}_p(\rho) = \sum_{i \geq 0} \frac{1}{[G_{0,p} : G_{i,p}]} \dim(V/V^{G_{i,p}}), \qquad (*)$$

where V is the two-dimensional $\overline{\mathbb{F}}_\ell$-vector space underlying the representation and $V^{G_{i,p}}$ is its subspace of invariants under $G_{i,p}$. As observed in [Edi97, p.213], replacing $V/V^{G_{i,p}}$ by the kernel of the map to the co-invariants $V \to V_{G_{i,p}}$, where

$$V_{G_{i,p}} := V/\left\langle \{v - hv \,|\, \forall v \in V,\, h \in G_{i,p}\} \right\rangle,$$

gives the same result.

Let us underline that the conductor $\mathrm{N}(\rho)$ reflects the ramification away from ℓ. On the other hand, the weight $k(\rho)$ is defined in terms of the ramification at ℓ.

Let ψ, ψ' denote the fundamental characters of level 2, i.e. the characters of the tame inertia with values in $\overline{\mathbb{F}}_\ell^*$ induced by the embeddings of fields $\mathbb{F}_{\ell^2} \hookrightarrow \overline{\mathbb{F}}_\ell$, see [Ser87, Section 2 and Proposition 1]. The weight $k(\rho)$ of a continuous 2-dimensional Galois representation ρ is defined according to the following definition:

Definition 4.2.1 ([Edi92, Definition 4.3])**.** Let ρ be a continuous 2-dimensional Galois representation and let ρ_ℓ be its restriction to the decomposition group at ℓ. We associate an integer $k(\rho)$ to ρ as follows:

1. suppose that ϕ, ϕ' are characters of G_ℓ of level 2 and we have

$$\rho_\ell \cong \begin{pmatrix} \phi & 0 \\ 0 & \phi' \end{pmatrix}.$$

   After interchanging ϕ and ϕ' if necessary, we have $\phi = \psi^a \psi'^b$ and $\phi' = \psi'^a \psi^b$ with $0 \leq a < b \leq \ell - 1$. Then, we set $k(\rho) = 1 + \ell a + b$.

2. Suppose that ϕ, ϕ' are characters of G_ℓ of level 1.

(a) If $\rho_\ell|_{I_{\ell,w}}$ is trivial, where $I_{\ell,w}$ is the wild inertia subgroup, then we have

$$\rho_\ell \cong \begin{pmatrix} \chi_\ell^a & 0 \\ 0 & \chi_\ell^a \end{pmatrix},$$

with $0 \leq a \leq b \leq \ell - 2$. Then, we set $k(\rho) = 1 + \ell a + b$.

(b) If $\rho_\ell|_{I_{\ell,w}}$ is not trivial, we have

$$\rho_\ell \cong \begin{pmatrix} \chi_\ell^\beta & * \\ 0 & \chi_\ell^\alpha \end{pmatrix},$$

for unique α, β such that $0 \leq \alpha \leq \ell - 2$ and $1 \leq \beta \leq \ell - 1$. Then, we set $a = \min\{\alpha, \beta\}$ and $b = \max\{\alpha, \beta\}$. If $\chi_\ell^{\beta-\alpha} = \chi_\ell$ and $\rho_\ell \otimes \chi_\ell^{-\alpha}$ is not finite at ℓ then we set $k(\rho) = 1 + \ell a + b + \ell - 1$; otherwise $k(\rho) = 1 + \ell a + b$.

Serre conjectured, [Ser87, Conjecture 3.2.4?] and [Edi97, Conjecture 1.8], that if ρ is irreducible and odd, then it is modular i.e. there exists a modular form f of level $\mathrm{N}(\rho)$ and weight $k(\rho)$ such that the associated representation, as in Theorem 4.0.4, is isomorphic to ρ. Let us remark that for ρ being odd means that characteristic polynomial of a complex conjugation in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is equal to $t^2 - 1 \in \overline{\mathbb{F}}_\ell[t]$. Serre's conjecture has been proved by Khare-Wintenberger in [KW09a] and [KW09b]:

Khare-Wintenberger Theorem ([KW09a, Theorem 1.2]). *Let ℓ be a prime number and let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be an absolutely irreducible, continuous, odd representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then there exists a modular form f of level $\mathrm{N}(\rho)$ and weight $k(\rho)$ which is a normalized eigenform and such that ρ and ρ_f, are isomorphic.*

For an odd prime ℓ, an odd residual Galois representation in characteristic ℓ is irreducible if and only of it is absolutely irreducible: this follows because the image of a complex conjugation has distinct eigenvalues.

Let us now state, and recall the proof, of a result essentially due to Livné:

Lemma 4.2.2 ([Wie04, Lemma 11]). *Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be an odd, continuous representation of conductor $\mathrm{N}(\rho)$, and let k be a positive integer. If $f \in S(\Gamma_1(m), k)_{\overline{\mathbb{F}}_\ell}$ is an eigenform such that $\rho_f \cong \rho$, then $\mathrm{N}(\rho)$ divides m.*

Proof. By multiplying with the Hasse invariant, if necessary, we can assume that the weight k is at least 2. Hence, the form f can be lifted to characteristic zero in the same level, see [DI95, Theorem 12.3.2]. Let g be the newform that corresponds to a lift $\tilde{f}$ of f of level m, with $\tilde{f}$ and eigenform. Let N be the level of g. By construction, the Galois representation ρ_g reduces to ρ. By [Liv89, Proposition 0.1] we have that $\mathrm{N}(\rho)$ divides N. As N divides m, the lemma follows. □

Remark 4.2.3. The previous lemma states that, given a modular, odd, continuous 2-dimensional Galois representation ρ of conductor $N(\rho)$, there are infinitely many mod ℓ modular forms of level multiple of the conductor such that the associated 2-dimensional Galois representation are equivalent to ρ.

If the representation ρ is irreducible, then, by Khare-Wintenberger Theorem there exists a modular form of level $N(\rho)$ and weight $k(\rho)$ such that the associated representation is equivalent to ρ.

If we restrict ourself to work only with mod ℓ modular forms with weight between 2 and $\ell+1$ then, given a modular, odd, continuous 2-dimensional Galois representation ρ, there exist at most two mod ℓ modular forms of level $N(\rho)$ and weight between 2 and $\ell+1$ with associated 2-dimensional Galois representation, as in Corollary 4.0.5, which are equivalent to ρ. This follows from the theory of θ_ℓ-cycles, see [Edi92, Section 3.2].

Moreover, if we require the weight to be minimal, it follows that if the weight is different from ℓ then there exists one mod ℓ modular forms of level $N(\rho)$ and weight between 2 and $\ell+1$ with associated 2-dimensional Galois representation equivalent to ρ. In weight ℓ there exist at most two such forms. In this case, indeed, it can happen that the weight $k(\rho)$ is 1 and so the two forms in weight ℓ are images of a mod ℓ modular forms of weight 1 through the embeddings given respectively by the Frobenius and the multiplication by the Hasse invariant, see [Edi06, Section 4.1] and [Wie05, Section 4.5].

Chapter 5

Image

Let n and k be positive integers, let ϵ be a character of $(\mathbb{Z}/n\mathbb{Z})^*$ with values in $\mathbb{C}^*$ and let $f : \mathbb{T}_\epsilon(n,k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings, where ℓ is a prime not dividing n and $2 \leq k \leq \ell + 1$. The aim of this part of the thesis is to give an algorithm which determines the image of the associated Galois representation ρ_f, as in Corollary 4.0.5, up to conjugacy as subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$.

In this chapter we prove that the image of the representation in $\mathrm{GL}_2(\mathbb{F})$, where $\mathbb{F}$ is the field of definition of the representation, is determined, up to conjugation in $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$, once we have computed the set of determinants of the representation and the projective image $\mathbb{P}\rho_f(G_\mathbb{Q}) \subset \mathrm{PGL}_2(\mathbb{F}')$ of the representation, where $\mathbb{F}'$ is the field of definition of the projective representation. In Chapter 9 we will show that it is possible to compute such fields.

In the first section of this chapter we recall the classification of the subgroups of $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$ given in Dickson's Theorem, this is a key element for the algorithm we want to outline. In the second section, we describe the output of the algorithm. We explain how to express the image of the Galois representation ρ_f, up to conjugacy as subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$, using the projective image and the set of determinants, under the hypothesis of having already determined the definition field for the representation and the projective representation.

5.1 Projective image

Let n and k be positive integers, let $\epsilon\colon (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character and let $f\colon \mathbb{T}_\epsilon(n,k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings from the Hecke algebra of level n, weight k and character $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ to an algebraic closure of $\mathbb{F}_\ell$, where ℓ is a prime not dividing n. Let ρ_f be the Galois representation associated to f in Corollary 4.0.5, and let $\mathbb{F}$ be the field of definition for the representation.

The image of the representation ρ_f is a conjugate of a subgroup of $\mathrm{GL}_2(\mathbb{F})$.

In the following Theorem, due to Dickson, see [Dic58] and [Lan76], are listed all finite subgroups of $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$, for $\ell \geq 3$, up to conjugation:

Dickson's Theorem. *Let $\ell \geq 3$ be a prime and H a finite subgroup of $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$. Then a conjugate of H is one of the following groups:*

– *a finite subgroup of the upper triangular matrices;*
– $\mathrm{SL}_2(\mathbb{F}_{\ell^r})/\{\pm 1\}$ *or* $\mathrm{PGL}_2(\mathbb{F}_{\ell^r})$ *for* $r \in \mathbb{Z}_{>0}$*;*
– *a dihedral group* D_{2n} *with* $n \in \mathbb{Z}_{>1}$ *and* $(\ell, n) = 1$*;*
– *a subgroup isomorphic to either* $\mathfrak{A}_4$*, or* $\mathfrak{S}_4$ *or* $\mathfrak{A}_5$*.*

In the last case, i.e. when H is conjugate to a subgroup of $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$ isomorphic to either $\mathfrak{A}_4$, or $\mathfrak{S}_4$ or $\mathfrak{A}_5$, we give the following definition:

Definition 5.1.1. Let $\ell \geq 3$ be a prime and let G be a subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$. If the projective image of G is conjugate to a subgroup of $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$ isomorphic to either $\mathfrak{A}_4$, or $\mathfrak{S}_4$ or $\mathfrak{A}_5$, we call G *projectively exceptional.*

In characteristic 2, there is a similar classification to the one presented in Dickson's Theorem:

Theorem 5.1.2 ([KW09a, Lemma 6.1])**.** *Let H be a finite subgroup of* $\mathrm{PGL}_2(\overline{\mathbb{F}}_2)$*. Then a conjugate of H is one of the following groups:*
– *a finite subgroup of the upper triangular matrices;*
– $\mathrm{SL}_2(\mathbb{F}_{2^r})/\{\pm 1\}$ *or* $\mathrm{PGL}_2(\mathbb{F}_{2^r})$ *for* $r \in \mathbb{Z}_{>0}$*;*
– *a dihedral group* D_{2n} *with* $n \in \mathbb{Z}_{>1}$ *and* $(n, 2) = 1$*.*

In particular, if $\ell > 5$ and the order of G is divisible by ℓ, then either G is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F})$, where $\mathbb{F}$ is the field of definition of the representation, or G contains $\mathrm{SL}_2(\mathbb{F}')$, where $\mathbb{F}'$ is the field of definition of the projective representation. If the order of G is prime to the characteristic of the field, then its projective image is:
– either cyclic and G is contained in a Cartan subgroup;
– or dihedral, and G is contained in the normalizer of a Cartan subgroup but not in the Cartan subgroup itself;
– or conjugate to a subgroup isomorphic to one of the following groups: $\mathfrak{A}_4$, $\mathfrak{S}_4$, or $\mathfrak{A}_5$.

Let us recall that a Cartan subgroup C is a semi-simple maximal abelian subgroup of $\mathrm{GL}_2(\mathbb{F})$ and a Borel subgroup is a maximal closed connected solvable subgroup of $\mathrm{GL}_2(\mathbb{F})$. Hence, the subgroup of upper-triangular matrices is a Borel subgroup in $\mathrm{GL}_2(\mathbb{F})$. Since the representation ρ_f is semi-simple, if the projective image is cyclic and the order of G is prime to the characteristic, then the representation ρ_f is reducible: its image is an abelian group, while in the other cases it is irreducible.

What we have just discussed motivates the following definition:

Definition 5.1.3. Let n and k be two positive integers, let ℓ be a prime such that $(n, \ell) = 1$ and $2 \leq k \leq \ell + 1$, and let $\epsilon\colon (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character. Let $f\colon \mathbb{T}_\epsilon(n, k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings and let $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the representation attached to f in Corollary 4.0.5. If $G := \rho_f(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ has order prime to ℓ we call the image *exceptional.* Moreover, we refer to the

field of definition of the projective representation $\mathbb{P}\rho$ as the *Dickson's field* for the representation.

We will discuss about reducible representations in Chapter 7 and we will study irreducible representation with exceptional images in Chapter 10. In order to determine the projective image we need to determine the Dickson field of the representation, which is the field of definition of the projective representation and this is done in Chapter 9.

Remark 5.1.4. In characteristic 2, 3 and 5 we give a more explicit statement of Dickson's Theorem, since it will be useful in the following discussion.

For $\ell = 2$, let us underline that in Theorem 5.1.2 groups with projective image isomorphic to $\mathfrak{A}_4$, $\mathfrak{S}_4$ and $\mathfrak{A}_5$ are not explicitly listed, this follows because:
- $\mathfrak{S}_4$ cannot occur as irreducible representation: any element in $\mathrm{GL}_2(\overline{\mathbb{F}}_2)$ of order a power of 2 is forced to be of order 1 or 2.
- $\mathfrak{A}_4$ has a normal subgroup of order 4, hence, any group with projective image $\mathfrak{A}_4$ is conjugate to a subgroup of the upper triangular matrices of $\mathrm{GL}_2(\overline{\mathbb{F}}_2)$: for any finite extension $\mathbb{F}$ of $\mathbb{F}_2$, a Sylow 2-subgroup of $\mathrm{GL}_2(\mathbb{F})$ is given by the unipotent matrices. For more details and a proof see [Fab11, Proposition 4.13].
- $\mathfrak{A}_5$ is isomorphic to $\mathrm{SL}_2(\mathbb{F}_4)$. Since all icosahedral groups are conjugated, see [Fab11, Proposition 4.23], the Dickson's field of the representation is $\mathbb{F}_4$.

For $\ell = 3$, Dickson's Theorem can be stated in the following way: let H a finite subgroup of $\mathrm{PGL}_2(\overline{\mathbb{F}}_3)$, then a conjugate of H is one of the following groups:
- a finite subgroup of the upper triangular matrices;
- $\mathrm{SL}_2(\mathbb{F}_{3^r})/\{\pm 1\}$ or $\mathrm{PGL}_2(\mathbb{F}_{3^r})$ for $r \in \mathbb{Z}_{>0}$;
- a dihedral group D_{2n} with $n \in \mathbb{Z}_{>1}$ and $(n, 3) = 1$;
- a subgroup isomorphic to $\mathfrak{A}_5$.

In any odd characteristic all octahedral (respectively tetrahedral) groups, i.e. groups isomorphic to $\mathfrak{A}_4$ (respectively $\mathfrak{S}_4$), are conjugate, see [Fab11]. In particular, we have that $\mathfrak{S}_4$ is isomorphic to $\mathrm{PGL}_2(\mathbb{F}_3)$ and applying [Fab11, Proposition 4.17] we have that the Dickson's field of the representation is $\mathbb{F}_3$. Similarly, $\mathfrak{A}_4$ is isomorphic to $\mathrm{SL}_2(\mathbb{F}_3)/\{\pm 1\}$ and by [Fab11, Proposition 4.14] the Dickson's field of the representation is $\mathbb{F}_3$.

Let us remark that icosahedral groups, i.e. groups isomorphic to $\mathfrak{A}_5$, are all conjugate in characteristic different from 5 and that they can occur in characteristic 3 only over extensions of $\mathbb{F}_9$ by [Fab11, Theorem A (4)]. Hence, in this last case $\mathbb{F}_9$ is a subfield of the field of definition of the projective representation since it is the Dickson's field of the representation.

For $\ell = 5$, we have that $\mathfrak{A}_5$ is isomorphic to $\mathrm{SL}_2(\mathbb{F}_5)/\{\pm 1\}$ and that all icosahedral groups are conjugate to $\mathrm{SL}_2(\mathbb{F}_5)/\{\pm 1\}$ by [Fab11, Proposition 4.23].

Applying [Fab11, Proposition 4.13] and [Fab11, Proposition 4.17], we conclude that the Dickson's field for projectively exceptional groups is $\mathbb{F}_5$.

In the following remark we give a criterion to decide if the image of a modular semi-simple 2-dimensional irreducible Galois representation is exceptional.

Remark 5.1.5. For any field k, let $\varphi : \mathrm{PGL}_2(k) \to k$ be the function defined by $\varphi(\gamma) = \mathrm{Trace}(\gamma)^2/\det(\gamma)$ with $\gamma \in \mathrm{PGL}_2(k)$. The following statement holds:

Proposition 5.1.6 ([Bos11, Proposition 1]). *Let $q \geq 4$ be a prime power and let $\varphi : \mathrm{PGL}_2(\mathbb{F}_q) \to \mathbb{F}_q$. Let G be a subgroup of $\mathrm{SL}_2(\mathbb{F}_q)/\{\pm 1\}$. Then we have $G = \mathrm{SL}_2(\mathbb{F}_q)/\{\pm 1\}$ if and only if $\varphi(G) = \mathbb{F}_q$.*

This gives a test to control beforehand if the representation is not exceptional, and we will see that this will be relevant for projectively exceptional images.

5.2 Image

Let n and k be positive integers, let $\epsilon\colon (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character and let $f\colon \mathbb{T}_\epsilon(n,k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings, where ℓ is a prime not dividing n. Let ρ_f be the associated semi-simple Galois representation, as in Corollary 4.0.5. In this section we will use the following notation: $G = \rho_f(G_{\mathbb{Q}}) \subset \mathrm{GL}_2(\mathbb{F})$ is the image of the representation, where $\mathbb{F}$ is the field of definition of ρ_f; the image of the projective representation is denoted by $H = \pi(G)$, where $\mathrm{GL}_2(\mathbb{F}) \xrightarrow{\pi} \mathrm{PGL}_2(\mathbb{F})$ is the quotient map, and $D := \{\det(g) \in \mathbb{F}^*, \forall g \in G\} \subseteq \mathbb{F}^*$ is the set of determinants, i.e. the image of the map $\det : G \to \mathbb{F}^*$.

The representation is semi-simple, therefore if it is reducible, then it is decomposable. Hence, if we determine the characters in which it splits, then we have a complete description of the image. This problem is addressed in Chapter 7

If the representation is irreducible and projectively dihedral, i.e. H is a dihedral subgroup of $\mathrm{PGL}_2(\mathbb{F})$, then there exist a character, corresponding to a quadratic extension of $\mathbb{Q}$, such that the representation ρ_f is the induced representation of $G_{\mathbb{Q}}$ by this character, in Chapter 10 we will prove this statement. We will also show that there exists a quadratic character such that the representation and its twist by this character are equivalent. By Dickson's Theorem, in this case the projective image contains a maximal cyclic subgroups of order d not divisible by ℓ. Therefore, the projective image is isomorphic, up to conjugation, to $\mu_d(\overline{\mathbb{F}}_\ell) \rtimes \mathbb{Z}/2\mathbb{Z}$, with the action given by $z \mapsto z^{-1}$. Conjugation corresponds to the choice of an embedding

for $\mu_d(\overline{\mathbb{F}}_\ell)$. As stated in [Ser72, Section 2.6, ii)] and [Ser72, Proposition 17], the image G is then contained in the normalizer of a Cartan subgroup. Let $\mathbb{F}'$ be the field of definition of the projective representation, the following two cases can occur:

1. d divides the cardinality of $\mathbb{F}'^*$. In this case there exists an embedding $\zeta_d \mapsto \left(\begin{smallmatrix} \overline{\zeta}_d & 0 \\ 0 & 1 \end{smallmatrix}\right)$ where $\overline{\zeta}_d$ is an element of order d. Since all normalizers of split Cartan subgroups are Galois conjugated, see [Lan76, Chapter XI], we have that the image is given by
$$G \cong \left\{ A \begin{pmatrix} \overline{\zeta}_d^i & 0 \\ 0 & 1 \end{pmatrix}, A \begin{pmatrix} 0 & \overline{\zeta}_d^j \\ 1 & 0 \end{pmatrix} \text{ for } i,j \in \mathbb{Z}/d\mathbb{Z} \text{ and } A \in D \right\}$$
2. d does not divide the cardinality of $\mathbb{F}'^*$, but d divides the cardinality of $\mathbb{F}'(\sqrt{\delta})^*$, where $\delta \in \mathbb{F}'^*$ is not a square. In this case there is an embedding $\zeta_d \mapsto \left(\begin{smallmatrix} \alpha & 0 \\ 0 & \overline{\alpha} \end{smallmatrix}\right)$ where $\alpha \in \mathbb{F}'(\sqrt{\delta})$ is an element of order d. Hence, G is a Normalizer of a non-split Cartan, see [Ser72, Section 2.1, b)].

In the remaining cases, i.e. when the representation is not reducible and the projective image is not dihedral, we derive the description of the image from Goursat's Lemma, see [Rib76a, Section V]:

Goursat's lemma. *Let A, A' be groups, and let B be a subgroup of $A \times A'$ such that the two projections $p_1 : B \to A$ and $p_2 : B \to A'$ are surjective. Let N be the kernel of p_2 and N' the kernel of p_1. Then the image of B in $A/N \times A'/N'$ is the graph of an isomorphism $A/N \approx A'/N'$.*

If the field of definition of the projective image is $\mathbb{F}_2$, then the representation is reducible or dihedral by Theorem 5.1.2: let us recall that

$$\mathrm{PGL}_2(\mathbb{F}_2) \cong \mathrm{GL}_2(\mathbb{F}_2) \cong D_6 \cong \mathfrak{S}_3,$$

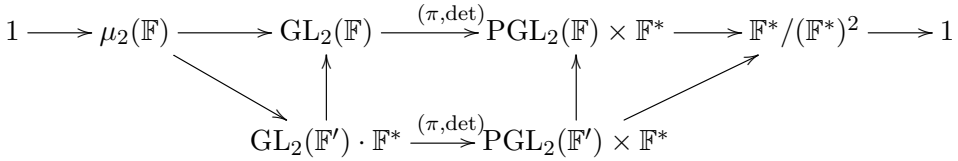
and in both cases we are not interested in using this approach.

Let $\mathbb{F}$ be a finite field, such that $\mathbb{F}_2 \not\subset \mathbb{F}$, then the following sequence is exact:

$$1 \to \mu_2(\mathbb{F}) \to \mathrm{GL}_2(\mathbb{F}) \overset{(\pi,\det)}{\longrightarrow} \mathrm{PGL}_2(\mathbb{F}) \times \mathbb{F}^* \to \mathbb{F}^*/(\mathbb{F}^*)^2 \to 1 \qquad (\dagger)$$

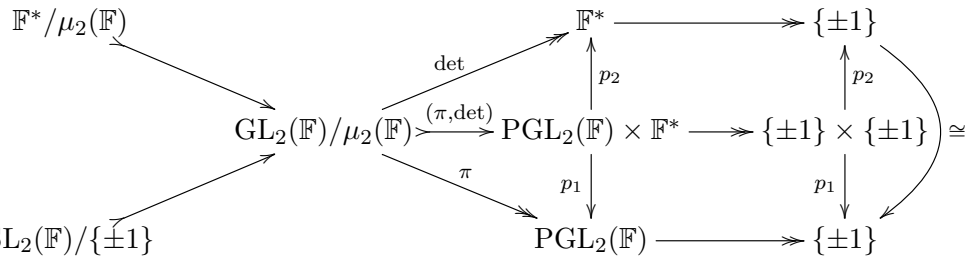
where $\mu_2(\mathbb{F})$ and $\mathbb{F}^*/(\mathbb{F}^*)^2$ are respectively the kernel and the co-kernel of the map $(\pi, \det)$. For $\mathbb{F}_2$ we have that $\mathrm{PGL}_2(\mathbb{F}_2) \cong \mathrm{GL}_2(\mathbb{F}_2)$.

Let $\mathbb{F}'$ be a subfield of $\mathbb{F}$, let us recall that if $\mathbb{F} \neq \mathbb{F}_2$, then we have the following sequence:



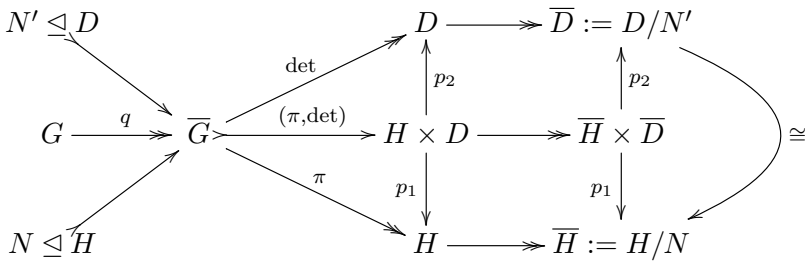
where the group $\mathrm{GL}_2(\mathbb{F}') \cdot \mathbb{F}^*$ is the subgroup of $\mathrm{GL}_2(\mathbb{F})$ given by matrices of $\mathrm{GL}_2(\mathbb{F}')$ multiplied by scalar matrices in $\mathbb{F}^*$. We will call such a group a *scalar extension* of $\mathrm{GL}_2(\mathbb{F}')$ by $\mathbb{F}$.

Let us denote by q the quotient map $\mathrm{GL}_2(\mathbb{F}) \to \mathrm{GL}_2(\mathbb{F})/\mu_2(\mathbb{F})$. The map $(\pi, \det)$ in sequence (†) is injective on $\mathrm{GL}_2(\mathbb{F})/\mu_2(\mathbb{F})$. Hence, we have the following diagram:



and by Goursat's Lemma, we conclude that the image of $\mathrm{GL}_2(\mathbb{F})/\mu_2(\mathbb{F})$ in the quotient is uniquely determined since the isomorphism is unique.

Let $\mathbb{F}$ and $\mathbb{F}'$ be respectively the field of definition of the representation and of the projective representation and let $\overline{G} := q(G)$. Let us assume that the representation is irreducible and not dihedral, since these cases are treated in a different way. We have the following diagram:



where: $\overline{G} \subseteq \mathrm{GL}_2(\mathbb{F})/\mu_2(\mathbb{F})$, by definition of the map q; the group $H \times D$ is a subgroup of $\mathrm{PGL}_2(\mathbb{F}') \times \mathbb{F}^*$ since $\mathbb{F}$ and $\mathbb{F}'$ are the fields of definitions of the image and the projective image respectively; and N, N' are respectively normal subgroups in H and D. Let us remark that N contains all matrices with determinant one of $\overline{G}$, since it is the intersection of $\overline{G}$ with $\mathrm{SL}_2(\mathbb{F})/\{\pm 1\}$, and, similarly, N' contains the scalar matrices of $\overline{G}$: it is the centre of $\overline{G}$. Since $D \subseteq \mathbb{F}^*$, then $\overline{D}$ is a cyclic subgroup. Applying Goursat's lemma it follows that $\overline{H}$ is a cyclic group too since the image of $\overline{G}$ in $\overline{H} \times \overline{D}$ is the graph of an isomorphism between $\overline{H}$ and $\overline{D}$. Then $N \trianglelefteq H$ is a normal subgroups with cyclic quotient.

The representation is irreducible and its projective image is not dihedral, therefore we have the following list of possible projective images H by Dickson's Theorem:

- $H \supseteq \mathrm{SL}_2(\mathbb{F}')/\{\pm 1\}$. If $\mathbb{F}'$ is neither $\mathbb{F}_2$ nor $\mathbb{F}_3$, then $N = \mathrm{SL}_2(\mathbb{F}')/\{\pm 1\}$ or $N = H$, hence, $\overline{H} \subseteq \{\pm 1\}$. This follows because $\mathrm{SL}_2(\mathbb{F}')/\{\pm 1\}$ is a simple group under these hypotheses. The case $\mathbb{F}' = \mathbb{F}_2$ is excluded by our assumptions, and the possibility $\mathbb{F}' = \mathbb{F}_3$ is treated in the cases of octahedral and tetrahedral projective image since we have respectively $\mathrm{SL}_2(\mathbb{F}_3)/\{\pm 1\} \cong \mathfrak{A}_4$ and $\mathrm{PGL}_2(\mathbb{F}_3) \cong \mathfrak{S}_4$.
- $H \cong \mathfrak{S}_4$, then either $N = \mathfrak{A}_4$ and so $\overline{H} = \{\pm 1\}$, or $N = H$, therefore $\overline{H} = \{1\}$.
- $H \cong \mathfrak{A}_4$, then either $N \cong V_4$ is the subgroup given by double transpositions, then $\overline{H} \cong C_3$ the cyclic group of 3 elements, or $N = H$, then $\overline{H} = \{1\}$.
- $H \cong \mathfrak{A}_5$, then $N = \mathfrak{A}_5$ so $\overline{H} = \{1\}$, since $\mathfrak{A}_5$ is simple.

From this list we deduce that if H is not isomorphic to $\mathfrak{A}_4$, Goursat's lemma implies that the group $\overline{G}$ is uniquely determined. In the remaining case, if $\overline{H} \cong C_3$ there are be two possible isomorphism which are twist of each other. We will see that they correspond to the choice of a character of C_3 and, in particular, we will show that also in this case we can determine $\overline{G}$ uniquely. Moreover, if -1 belongs to G then $G = q^{-1}(\overline{G})$, hence it is possible determine G, the image of the representation, up to conjugacy as subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$.

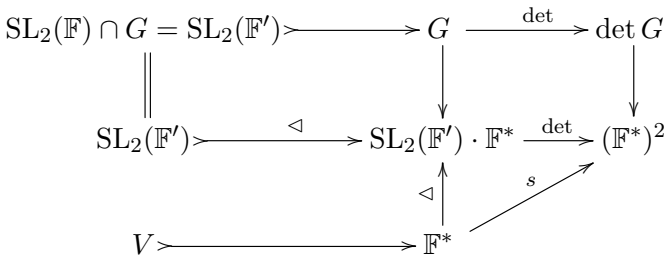
Now we will proceed to describe G, up to conjugacy as subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$, for all possible H, listed according to Dickson Theorem. We will not consider the reducible and the dihedral case. We will also show, case by case, that -1 belongs to G.

– $H \supseteq \mathrm{SL}_2(\mathbb{F}')/\{\pm 1\}$ where $\mathbb{F}'$ is the field of definition of the projective representation.

Proposition 5.2.1. *Let ℓ be a prime and let $\mathbb{F}$ be a finite extension of $\mathbb{F}_\ell$. Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F})$ with projective image $H = \mathrm{SL}_2(\mathbb{F}')/\{\pm 1\}$ where $\mathbb{F}' \subseteq \mathbb{F}$. Then, up to conjugation as subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$,*

$$G = (\mathrm{SL}_2(\mathbb{F}') \cdot \mathbb{F}^* \xrightarrow{\det} (\mathbb{F}^*)^2)^{-1}(\det G).$$

Proof. Since $H = \mathrm{SL}_2(\mathbb{F}')/\{\pm 1\}$, then by [EC11, Lemma 2.5.1] we have that G contains $\mathrm{SL}_2(\mathbb{F}')$. Moreover, since $G \subseteq \mathrm{GL}_2(\mathbb{F})$ we have also that $G \subset \mathrm{SL}_2(\mathbb{F}') \cdot \mathbb{F}^*$ because H is $\mathrm{SL}_2(\mathbb{F}')/\{\pm 1\}$. In this case -1 belongs to the image G since it belongs to $\mathrm{SL}_2(\mathbb{F}')$. The following diagram resume the hypotheses:



where $V = (\mathbb{F}^* \xrightarrow{s} (\mathbb{F}^*)^2)^{-1}(\det G)$ and s is the map sending x to x^2. Since $\mathrm{SL}_2(\mathbb{F}') \subseteq G \subseteq \mathrm{SL}_2(\mathbb{F}') \cdot \mathbb{F}^*$ and $G = V \cdot \mathrm{SL}_2(\mathbb{F}')$ then the statement follows. □

Proposition 5.2.2. *Let ℓ be a prime and let $\mathbb{F}$ be a finite extension of $\mathbb{F}_\ell$. Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F})$ with projective image $H = \mathrm{PGL}_2(\mathbb{F}')$ where $\mathbb{F}' \subseteq \mathbb{F}$. Then, up to conjugation as subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$,*

$$G = (\mathrm{GL}_2(\mathbb{F}') \cdot \mathbb{F}^* \xrightarrow{\det} \mathbb{F}^*)^{-1}(\det G).$$

Proof. The proof is analogous to the proof of Proposition 5.2.1, but in this case we have the following inclusions $\mathrm{SL}_2(\mathbb{F}') \subseteq G \subseteq \mathrm{GL}_2(\mathbb{F}') \cdot \mathbb{F}^*$. □

Remark 5.2.3. If the projective image is isomorphic to $\mathrm{SL}_2(\mathbb{F}')/\{\pm 1\}$, then the determinants of the matrices in G belong to the set of squares $(\mathbb{F}^*)^2$, while if the projective image is isomorphic to $\mathrm{PGL}_2(\mathbb{F}')$, then they belong to $\mathbb{F}^*$.

– $H \cong \mathfrak{A}_4$

Let us recall that the group $\mathfrak{A}_4$ has no non-trivial 2-dimensional irreducible linear representation. Moreover, let r be a positive integer, the second cohomology group $\mathrm{H}^2(\mathfrak{A}_4, \mathbb{Z}/2^r\mathbb{Z})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ by [Que95, Proposition 2.1 (i)]. Therefore, since this group classifies the central extensions of $\mathfrak{A}_4$

with kernel $\mathbb{Z}/2^r\mathbb{Z}$, we have that there exists only one non-trivial extension up to isomorphism. For $r = 1$, this extension is isomorphic to the group $\mathrm{SL}_2(\mathbb{F}_3)$ since $\mathrm{SL}_2(\mathbb{F}_3)/\{\pm 1\} \cong \mathfrak{A}_4$, and this group does admit 2-dimensional irreducible representations.

The complex linear 2-dimensional irreducible representations of $\mathrm{SL}_2(\mathbb{F}_3)$ are listed in Table 5.1 below.

$\mathrm{SL}_2(\mathbb{F}_3)$	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}-1&0\\0&-1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&-1\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}-1&1\\0&-1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}-1&-1\\0&-1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)$
$\mathrm{Trace}(\tau_1)$	2	-2	-1	-1	1	1	0
$\mathrm{Trace}(\tau_2)$	2	-2	$1+\zeta$	$-\zeta$	ζ	$-1-\zeta$	0
$\mathrm{Trace}(\tau_3)$	2	-2	$-\zeta$	$1+\zeta$	$-1-\zeta$	ζ	0

Table 5.1: List of the traces of 2-dimensional irreducible representations of $\mathrm{SL}_2(\mathbb{F}_3)$ in characteristic zero, computed in PARI/GP. In the first row are listed representatives for the conjugacy classes. In the table ζ denotes a fixed 3-rd root of unity.

The representations τ_1, τ_2 and τ_3 are three 2-dimensional faithful irreducible representations of $\mathrm{SL}_2(\mathbb{F}_3)$ in characteristic zero and they are twist of each other by a character acting on C_3, the maximal cyclic group inside $\mathfrak{A}_4$. Hence, we have that $\tau_2(\mathrm{SL}_2(\mathbb{F}_3))$ and $\tau_3(\mathrm{SL}_2(\mathbb{F}_3))$ are contained in the scalar extension of $\tau_1(\mathrm{SL}_2(\mathbb{F}_3))$ by $\mathbb{Z}[\zeta]^*$.

Let us remark that the representations of $\mathrm{SL}_2(\mathbb{F}_3)$ in characteristic ℓ are reduction modulo ℓ of the representations in characteristic zero. The representation τ_1 is realized over $\mathbb{Z}$, while the representations τ_2 and τ_3 are realized over $\mathbb{Z}[\zeta]$.

Let λ be a maximal ideal over ℓ in the field of definition of the representation, composing with the projection to the quotient we have a representation in characteristic ℓ. Let us still denote by τ_1, τ_2 and τ_3 the three representation obtained fixing a maximal ideal over ℓ and reducing the characteristic zero representation modulo that ideal. We have that $\tau_2(\mathrm{SL}_2(\mathbb{F}_3))$ and $\tau_3(\mathrm{SL}_2(\mathbb{F}_3))$ are contained in the scalar extension of $\tau_1(\mathrm{SL}_2(\mathbb{F}_3))$ by $\mathbb{F}_{\ell^2}^*$. Moreover, let us remark that for an odd prime ℓ, the representations τ_1, τ_2 and τ_3 are three 2-dimensional faithful irreducible representations of $\mathrm{SL}_2(\mathbb{F}_3)$ in characteristic ℓ. Meanwhile, for $\ell = 2$ they are 2-dimensional representation of C_3, hence they are reducible.

The images of the projective representations given composing τ_1, τ_2 and τ_3 with the natural quotient map are isomorphic to $\mathfrak{A}_4$ in any characteristic different from 2. In characteristic 2 they are isomorphic to C_3 and their kernel is V_4, the Klein four group, given by double transpositions in $\mathfrak{A}_4$.

Proposition 5.2.4. *Let $\ell > 3$ be a prime and let $\mathbb{F}$ be a finite extension of $\mathbb{F}_\ell$. Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F})$ with projective image $H \subset \mathrm{PGL}_2(\mathbb{F})$, and such that G acts irreducibly on $\mathbb{P}^1(\mathbb{F})$. Let us assume that H is isomorphic to $\mathfrak{A}_4$. Then -1 belongs to G and the group G, up to conjugation as subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$, is given by*

$$G = (\tau_1(\mathrm{SL}_2(\mathbb{F}_3)) \cdot \mathbb{F}^* \xrightarrow{\det} (\mathbb{F}^*)^2)^{-1}(\det G),$$

where τ_1 is the reduction modulo ℓ of the representation in Table 5.1.

Proof. Under the hypotheses of the proposition we have the following diagram:

$$\begin{array}{ccccc} \overline{\mathbb{F}}_\ell^* & \rightarrowtail & \mathrm{GL}_2(\overline{\mathbb{F}}_\ell) & \xrightarrow{\pi} & \mathrm{PGL}_2(\overline{\mathbb{F}}_\ell) \\ \uparrow & & \uparrow & & \uparrow \\ G \cap \overline{\mathbb{F}}_\ell^* & \rightarrowtail & G & \xrightarrow{\pi} & H \cong \mathfrak{A}_4. \end{array}$$

Let us recall that there is only a subgroup, up to conjugation, isomorphic to $\mathfrak{A}_4$ in $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$ by [Bea10, Proposition 4.1] or [Fab11, Proposition 4.14]. Since $\mathfrak{A}_4$ has no normal subgroup of order 2 then H is contained in $\mathrm{SL}_2(\overline{\mathbb{F}}_\ell)/\{\pm 1\}$. Therefore, for $\ell > 3$ the following diagram is exact:

$$\begin{array}{ccccc} \{\pm 1\} & \rightarrowtail & \mathrm{SL}_2(\overline{\mathbb{F}}_\ell) & \xrightarrow{\pi} & \mathrm{SL}_2(\overline{\mathbb{F}}_\ell)/\{\pm 1\} \\ & & \uparrow{\scriptstyle \tau_1} & & \uparrow \\ \{\pm 1\} & \rightarrowtail & \mathrm{SL}_2(\mathbb{F}_3) & \twoheadrightarrow & \mathfrak{A}_4 \cong \mathrm{SL}_2(\overline{\mathbb{F}}_3)/\{\pm 1\} \cong H \cong \pi(\tau_1(\mathrm{SL}_2(\mathbb{F}_3))) \end{array}$$

where the map τ_1 is a 2-dimensional representation of $\mathrm{SL}_2(\mathbb{F}_3)$, given reducing the representation in Table 5.1 modulo ℓ. Let us remark that the field of definition of the representation τ_1 is $\mathbb{F}_\ell$.

Let us show that -1 belongs to G. Proceeding by contradiction, let us assume -1 is not in G. This means that $G \cap \overline{\mathbb{F}}_\ell^*$ is cyclic of odd order, by simple computation. Therefore, the determinant is a character of odd order once restricted to $G \cap \overline{\mathbb{F}}_\ell^*$. So, extending G by scalars, the intersection $G \cap \overline{\mathbb{F}}_\ell^*$ is trivial: this corresponds to twist the action of G on $\mathbb{P}^1(\mathbb{F})$ with a power of the determinant. Hence, there exists a non-trivial scalar extension of G which is isomorphic to $\mathfrak{A}_4$ and is a subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$. Since $\mathfrak{A}_4$ does not admit 2-dimensional non-trivial irreducible representations, we get a contradiction.

Since -1 belongs to G we have that the image of the determinant has 2-power order and also $G \cap \overline{\mathbb{F}}_\ell^*$ has 2-power order.

Let $\sigma \in \mathfrak{A}_4$ be an element of order 3, and let $\tilde{\sigma}$ be a preimage of σ. Then $\pi(\tilde{\sigma}^3) = 1$ so $\tilde{\sigma}^3 \in G \cap \overline{\mathbb{F}}_\ell^*$. This group is a cyclic group of 2-power order,

hence, the order of $\tilde{\sigma}$ is $3 \cdot 2^t$ for $t \in \mathbb{Z}_{>0}$. Let $\tilde{\sigma}' = \tilde{\sigma}^{2^t}$, hence $\tilde{\sigma}'$ has order 3 and $\pi(\tilde{\sigma}') = \sigma^{\pm 1}$ has order 3.

Let G_3 be the subgroup of G generated by elements of order 3. The subgroup G_3 maps surjectively to $\mathfrak{A}_4$ via π, since $\mathfrak{A}_4$ is generated by 3-cycles. Moreover, G_3 is contained in $\mathrm{SL}_2(\mathbb{F})$ and its intersection with the scalar matrices in given by $\{\pm 1\}$, otherwise $\mathfrak{A}_4$ would have a 2-dimensional representation. This means that G_3 is a subgroup of $\mathrm{SL}_2(\mathbb{F})$ and by construction it is a central extension of $\mathfrak{A}_4$ by $\{\pm 1\}$:

$$\begin{array}{ccccc} G \cap \overline{\mathbb{F}}_\ell^* & \hookrightarrow & G & \xrightarrow{\pi} & H \cong \mathfrak{A}_4 \\ \uparrow & & \uparrow & \nearrow & \\ \{\pm 1\} & \hookrightarrow & G_3 & \longrightarrow & \mathrm{SL}_2(\mathbb{F}). \end{array}$$

Therefore, G_3 is isomorphic to $\mathrm{SL}_2(\mathbb{F}_3)$ because $\mathrm{H}^2(\mathfrak{A}_4, \mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$ and the trivial extension has no 2-dimensional irreducible representations. So G_3 is the image of a 2-dimensional irreducible representations of $\mathrm{SL}_2(\mathbb{F}_3)$ in $\mathrm{SL}_2(\mathbb{F})$. From Table 5.1, it follows that $G_3 = \tau_1(\mathrm{SL}_2(\mathbb{F}_3))$ since the other representations are twist of τ_1 by a non-trivial character, hence are not defined over $\mathbb{F}_3$. The group G and the subgroup G_3 both surject to a group isomorphic to $\mathfrak{A}_4$. This implies that for all $g \in G$ there exists $g' \in G_3$ and $\lambda \in \det(G)$ such that $g = g'\lambda$, uniquely up to sign, by construction of G_3. Hence, we have that

$$G_3 \cong \tau_1(\mathrm{SL}_2(\mathbb{F}_3)) \subseteq G \subseteq \tau_1(\mathrm{SL}_2(\mathbb{F}_3)) \cdot \mathbb{F}^*.$$

Therefore, we have:

$$\begin{array}{ccc} G & \xrightarrow{\det} & \det G \\ \downarrow & & \downarrow \\ \tau_1(\mathrm{SL}_2(\mathbb{F}_3)) \cdot \mathbb{F}^* & \xrightarrow{\det} & (\mathbb{F}^*)^2, \end{array}$$

so the statement holds. □

Remark 5.2.5. If the projective image is isomorphic to $\mathfrak{A}_4$, then it is contained in $\mathrm{SL}_2(\mathbb{F}')/\{\pm 1\}$, where $\mathbb{F}'$ is the field of definition of the projective representation. So, the set of determinant of the representation is a subset of the set of squares of $\mathbb{F}$, field of definition of the representation.

– $H \cong \mathfrak{S}_4$

The group $\mathfrak{S}_4$ has no non-trivial 2-dimensional irreducible linear representations.

Let r be a positive integer, the second cohomology group $\mathrm{H}^2(\mathfrak{S}_4, \mathbb{Z}/2^r\mathbb{Z})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ by [Que95, Proposition 2.4 (i)]. Therefore, since this group classifies the central extensions of $\mathfrak{S}_4$ with kernel $\mathbb{Z}/2^r\mathbb{Z}$, we have that there exist three non-trivial extension by $\mathbb{Z}/2^r\mathbb{Z}$ up to isomorphism. Among them only one is odd: this follows from [Que95, Lemma 3.2]. For $r = 1$, this extension is isomorphic to the group $\mathrm{GL}_2(\mathbb{F}_3)$ since $\mathrm{PGL}_2(\mathbb{F}_3) \cong \mathfrak{S}_4$.

The complex linear 2-dimensional irreducible representations of $\mathrm{GL}_2(\mathbb{F}_3)$ are listed in the following table:

$\mathrm{GL}_2(\mathbb{F}_3)$	$\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}-1 & 0\\ 0 & -1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}0 & 1\\ -1 & 0\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}0 & 1\\ 1 & -1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}0 & 1\\ 1 & 1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}-1 & 1\\ 0 & -1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$
$\mathrm{Trace}(\rho_1)$	2	2	2	0	0	-1	-1	0
$\mathrm{Trace}(\rho_2)$	2	-2	0	α	$-\alpha$	-1	1	0
$\mathrm{Trace}(\rho_3)$	2	-2	0	$-\alpha$	α	-1	1	0

Table 5.2: List of the traces of 2-dimensional irreducible representations of $\mathrm{GL}_2(\mathbb{F}_3)$ in characteristic zero, computed in PARI/GP. In the first row are listed representatives for the conjugacy classes. In the table α denotes $\sqrt{-2}$.

The representations ρ_1 is not faithful and it corresponds to a representation of $\mathfrak{S}_3$. The representations ρ_2 and ρ_3 are 2-dimensional faithful irreducible representations. They are twists of each other and they are defined over $\mathbb{Z}[\alpha]$. In particular, $\rho_3 \cong \rho_2 \otimes \det \rho_2$.

Proposition 5.2.6. *Let $\ell > 3$ be a prime and let $\mathbb{F}$ be a finite extension of $\mathbb{F}_\ell$. Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F})$ with projective image $H \subset \mathrm{PGL}_2(\mathbb{F})$, and such that G acts irreducibly on $\mathbb{P}^1(\mathbb{F})$. Let us assume that H is isomorphic to $\mathfrak{S}_4$. Then -1 belongs to G and the group G, up to conjugation as subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$, is given by*

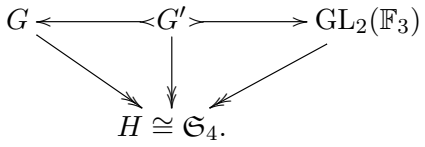
$$G = (\rho_2(\mathrm{GL}_2(\mathbb{F}_3)) \cdot \mathbb{F}^* \xrightarrow{\det} \mathbb{F}^*)^{-1}(\det G),$$

where ρ_2 is the reduction modulo ℓ of the representation in Table 5.2.

Proof. We will use the same notation of the proof of Proposition 5.2.4. Since $\mathfrak{A}_4 \subset \mathfrak{S}_4$ we have that -1 belongs to G. Moreover, we have that:

$$\begin{array}{ccccc} G & \hookleftarrow & G_3 \cong \mathrm{SL}_2(\mathbb{F}_3) & \hookrightarrow & \mathrm{GL}_2(\mathbb{F}_3) \cong \mathrm{SL}_2(\mathbb{F}_3) \rtimes \mathbb{F}_3^* \\ \downarrow & & \downarrow & & \downarrow \\ \mathfrak{S}_4 & \hookleftarrow & \mathfrak{A}_4 & \hookrightarrow & \mathfrak{S}_4. \end{array}$$

Let G' be the subgroup of G given by $G' := G_3 \rtimes \mathbb{F}_3^* \cong G_3 \rtimes \{\pm 1\}$. Then G' is isomorphic to $\mathrm{GL}_2(\mathbb{F}_3)$ and it surjects to H:



This implies that for all $g \in G$ there exists $g' \in G'$ and $\lambda \in \det G$ such that $g = g'\lambda$ uniquely up to sign. Hence, we have that

$$G' \cong \rho_2(\mathrm{GL}_2(\mathbb{F}_3)) \subseteq G \subseteq \rho_2(\mathrm{GL}_2(\mathbb{F}_3)) \cdot \mathbb{F}^*,$$

and so the statement holds. □

Remark 5.2.7. Let us remark that, since $\rho_3 = \rho_2 \otimes \det(\rho_2)$ and $\det(\rho_2)$ belongs to $\{\pm 1\}$, the choice of ρ_2 instead of ρ_3 does not change the image of the representation up to conjugation.

– $H \cong \mathfrak{A}_5$

The group $\mathfrak{A}_5$ has no non-trivial 2-dimensional irreducible linear representations.

Let r be a positive integer, the second cohomology group $\mathrm{H}^2(\mathfrak{A}_5, \mathbb{Z}/2^r\mathbb{Z})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ by [Que95, Proposition 2.1 (i)]. Therefore, there exists only one non-trivial extension up to isomorphism. For $r = 1$, this extension is isomorphic to the group $\mathrm{SL}_2(\mathbb{F}_5)$ since $\mathrm{PGL}_2(\mathbb{F}_5) \cong \mathfrak{S}_4$, and this group does admit 2-dimensional irreducible representations.

The complex linear 2-dimensional irreducible representations of $\mathrm{SL}_2(\mathbb{F}_5)$ are listed in the following table:

$\mathrm{SL}_2(\mathbb{F}_5)$	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}-1&0\\0&-1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}0&-1\\1&-1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}2&0\\0&3\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&2\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}0&-1\\1&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}-1&1\\0&-1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}-1&2\\0&-1\end{smallmatrix}\right)$
$\mathrm{Trace}(\iota_1)$	2	-2	-1	0	η	η^2	1	$-\eta$	$-\eta^2$
$\mathrm{Trace}(\iota_2)$	2	-2	-1	0	η^2	η	1	$-\eta^2$	$-\eta$

Table 5.3: List of the traces of 2-dimensional irreducible representations of $\mathrm{SL}_2(\mathbb{F}_5)$ in characteristic zero, computed in PARI/GP. In the first row are listed representatives for the conjugacy classes. In the table η denotes a fixed 5-th root of unity.

The representations ι_1 and ι_2 are 2-dimensional faithful irreducible representations and they are twist of each other. Moreover, there is an outer automorphism for which this two representations are conjugate (for example conjugation by $\left(\begin{smallmatrix}2&0\\0&1\end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_5)$), hence up to conjugation in $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$, these representation have the same image.

Proposition 5.2.8. *Let ℓ be an odd prime different from 5 and let $\mathbb{F}$ be a finite extension of $\mathbb{F}_\ell$. Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F})$ with projective image $H \subset \mathrm{PGL}_2(\mathbb{F})$, and such that G acts irreducibly on $\mathbb{P}^1(\mathbb{F})$. Let us assume that H is isomorphic to $\mathfrak{A}_5$. Then -1 belongs to G and G, up to conjugation as subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$, is given by*

$$G = (\iota_1(\mathrm{SL}_2(\mathbb{F}_5)) \cdot \mathbb{F}^* \xrightarrow{\det} (\mathbb{F}^*)^2)^{-1}(\det G),$$

where ι_1 is the reduction modulo ℓ of the representation in Table 5.3.

Proof. There is only a subgroup, up to conjugation, isomorphic to $\mathfrak{A}_5$ in $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$ by [Bea10, Proposition 4.1] or [Fab11, Proposition 4.22]. Since $\mathfrak{A}_5$ has no normal subgroup of order 2 then H is contained in $\mathrm{SL}_2(\overline{\mathbb{F}}_\ell)/\{\pm 1\}$. Since $\mathfrak{A}_4 \subseteq \mathfrak{A}_5$, we can proceed as in Proposition 5.2.4 and conclude that -1 belongs to G.

Let $[G, G]$ be the commutator of G, let us recall that $\mathfrak{A}_5$ is a perfect group i.e. $\mathfrak{A}_5 = [\mathfrak{A}_5, \mathfrak{A}_5]$. By hypotheses G surjects to $\mathfrak{A}_5$ so also $[G, G]$ surject to $[\mathfrak{A}_5, \mathfrak{A}_5] = \mathfrak{A}_5$. Moreover, $[G, G] \in \mathrm{SL}_2(\overline{\mathbb{F}}_\ell)$ since elements of the form $ghg^{-1}h^{-1}$ have determinant 1. Hence, we have the following diagram:

$$\begin{array}{ccccc} G & \twoheadleftarrow & [G,G] & \hookrightarrow & \mathrm{SL}_2(\overline{\mathbb{F}}_\ell) \\ & \searrow & \downarrow & & \uparrow \\ & & \mathfrak{A}_5 & \twoheadleftarrow & \mathrm{SL}_2(\mathbb{F}_5) \end{array}$$

which implies that $\forall g \in G$ there exist $g' \in [G, G]$ and $\lambda \in (\det G)$ such that $g = g'\lambda$ uniquely up to sign. Since $[G, G] \in \mathrm{SL}_2(\overline{\mathbb{F}}_\ell)$ and $\mathrm{H}^2(\mathfrak{A}_5, \mathbb{Z}/2\mathbb{Z})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, then $[G, G] \cong \mathrm{SL}_2(\mathbb{F}_5)$. Hence, we conclude that

$$[G, G] \cong \iota_1(\mathrm{SL}_2(\mathbb{F}_5)) \subseteq G \subseteq \iota_1(\mathrm{SL}_2(\mathbb{F}_5)) \cdot \mathbb{F}^*.$$

And, since up to conjugation in $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ the representations ι_1 and ι_2 are equivalent, the statement follows. □

Remark 5.2.9. In Proposition 5.2.4 and 5.2.6 we assume the characteristic different from 2 and 3. Indeed, in the first case the representation is reducible by Theorem 5.1.2. In characteristic 3, projective image isomorphic to $\mathfrak{A}_4$ or to $\mathfrak{S}_4$ corresponds to have big image. In this last case we apply Proposition 5.2.1 and Proposition 5.2.2 to determine the image of the linear 2-dimensional representation: the set of determinant is known, hence we distinguish the two cases. Analogously, in Proposition 5.2.8 we assume the characteristic different from 2 and 5. Indeed, in both cases, projective image isomorphic to $\mathfrak{A}_5$ corresponds to have big image, therefore we apply Proposition 5.2.1 to determine the image of the linear 2-dimensional representation.

Chapter 6

Comparing eigenforms

In this chapter we address the problem of comparing eigenforms. Let f and g be two mod ℓ eigenforms of the same level and weight. If the prime indexed coefficients of the q-expansion of f and g are equal up to a constant, depending on the level and the weight, the Sturm bound, then the two eigenforms are equal. Hence, the associated Galois representations are isomorphic.

It can happen that two different modular forms at the same level and weight give rise to isomorphic Galois representations. These forms, seen as old-forms at some higher level, are equal up to the Sturm bound at that level, which is greater than the one at the starting level. This follows because the prime indexed coefficients of the q-expansion at which such forms differ are made into zeros, see Section 6.2.

If a representation comes from a form of level n, we do not want make computation at level higher then n. Moreover, if a representation already appears at lower level, then we do not want re-do the computations. Therefore, in this chapter we study how to compare two eigenforms at a given level, studying the local description of the representation at primes dividing the conductor and the characteristic. In particular, we give a complete description of the eigenforms in the old-space.

In the first section of this chapter, we describe the known bounds for comparing eigenforms at a given level. In the second section, we explain how to compare eigenforms in different levels using degeneracy maps, we show that this approach implies the computation of an high number of Hecke operators. In the third section, we solve this problem using the local description for the representation and in the last section we give a first introduction to the algorithm and its preliminary steps.

6.1 Bounds

Let n and k be positive integers, let ℓ be prime not dividing n and such that $2 \leq k \leq \ell+1$. Let $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ be a character and let $f : \mathbb{T}_\epsilon(n,k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings. Let $f_{n,k}$ be the system of eigenvalues associated to the morphism f:

$$\begin{aligned} f_{n,k}\colon \mathcal{P} &\to \overline{\mathbb{F}}_\ell \times \overline{\mathbb{F}}_\ell \\ p &\mapsto (f(T_p), f(\langle p \rangle)) \end{aligned}$$

where $\mathcal{P}$ is the set of primes and $\langle p \rangle$ is zero if p divides n.

A system of eigenvalues at level n is uniquely determined once it is known for a finite set of primes by Sturm Theorem. This result is a very useful computational criterion in determining when two modular forms are congruent, for a reference see [Stu87, Theorem 1] and [Ste07, Section 9.4]. Let us recall that for a congruence subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$, the width of the cusp ∞ for Γ is the positive integer h defined by $\Gamma \cap \left(\begin{smallmatrix} 1 & \mathbb{Z} \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & h\mathbb{Z} \\ 0 & 1 \end{smallmatrix}\right)$.

Sturm Theorem ([Stu87, Theorem 1]). *Let $n \geq 1$ be an integer and let Γ be a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ containing $\Gamma(n)$. Let h be the width of the cusp ∞ for Γ. Let f be a modular form on Γ of weight k, with coefficients in a discrete valuation ring R contained in $\mathbb{C}$. Let $\mathbb{F}$ be the residue field of R. Suppose that the image $\sum a_m q^{m/h}$ in $\mathbb{F}[[q^{1/h}]]$ of the q-expansion of f has $a_m = 0$ for all $m \leq k[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]/12$. Then $a_m = 0$ for all m, i.e. f is congruent to 0 modulo the maximal ideal of R.*

Suppose $n \geq 5$. Sturm Theorem then follows from the fact that the line bundle of modular forms of weight k on $X(n)_{\mathbb{C}}$ has degree:

$$\deg(\omega^{\otimes k}) = \frac{k}{24} \cdot [\mathrm{SL}_2(\mathbb{Z}) : \Gamma(n)],$$

see [KM85, Corollary 10.13.12]. Indeed, since we are working on a stack, we have to divide the order of a zero at a point x by the order of $\mathrm{Aut}(x)$, so the result follows using as x the cusp at ∞ for Γ, see [Edi06, Proposition 4.2 and Remark 4.3].

Moreover, we can state the following Corollary, derived from an observation at the end of [Stu87, Theorem 1] and stated in this form in [Ras09, Theorem 2.1]:

Corollary 6.1.1. *Let Γ be a subgroup of $\mathrm{SL}_2(\mathbb{Z})$. Let h be the width of the cusp ∞ for Γ. Let f be a cusp form on Γ of weight k, with coefficients in a discrete valuation ring R contained in $\mathbb{C}$. Let $\mathbb{F}$ be the residue field of R, and suppose that the image $\sum a_m q^{m/h}$ in $\mathbb{F}[[q^{1/h}]]$ of the q-expansion of f has $a_m = 0$ for all $m \leq k[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]/12 - \#(\mathrm{Cusps})$. Then $a_m = 0$ for all m, i.e. f is congruent to 0 modulo the maximal ideal of R.*

The integer $k[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]/12$ is known as the Sturm bound for $M(\Gamma, k)_{\mathbb{C}}$, and we will refer to $n \leq k[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]/12 - \#(\mathrm{Cusps})$ as the Sturm bound for $S(\Gamma, k)_{\mathbb{C}}$. We will use the notation $B(n, k)$ to refer to such bounds.

There is a similar result about congruences between eigenforms with character, in which the study of diamond operators and Atkin-Lehner operators allows to lower the bound:

Corollary 6.1.2 ([BS02, Corollary 1.7]). *Let n and k be positive integers, let $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ a character and let f_1 and f_2 be eigenforms in $S(n,k,\epsilon)_{\mathbb{C}}$ with coefficients in the ring of integers of a number field, and let $\mathfrak{p}$ be a maximal ideal herein. Assume that $n \geq 5$, let $B(n,k)$ be the Sturm bound for cusp forms for $\Gamma_0(n)$ and weight k, and let S be the set of prime divisors of n not dividing $n/\operatorname{cond}(\epsilon)$. If $a_q(f_1) \equiv a_q(f_2) \bmod \mathfrak{p}$ for all primes $q \in S$ and all primes $q \leq B(n,k)/2^{|S|}$, then $f_1 \equiv f_2 \bmod \mathfrak{p}$.*

The set S in the previous corollary can be taken larger, we refer to [BS02] for more details and to [Edi06, Remark 4.3].

It is an immediate consequence of the previous statements that if we determine the system of eigenvalues up to $B(n,k)$ then the system of eigenvalues is uniquely associated (up to isomorphism) to a morphism of rings $f\colon \mathbb{T}_\epsilon(n,k) \to \overline{\mathbb{F}}_\ell$. Any mod ℓ modular form which has the same system of eigenvalues of the one associated to f up to the Sturm bound is equal to f (from here on we will not make any distinction between f seen as ring homomorphism from the Hecke algebra to a finite field and f seen as the associated mod ℓ eigenform).

Let us recall a result of Buzzard which states that the Sturm bound for modular forms of level n with character is the same as the one for $\Gamma_0(n)$.

Corollary 6.1.3 ([Ste07, Corollary 9.20]). *Let $\mathfrak{m}$ be a prime ideal in the ring of integers $\mathcal{O}$ of a number field. Suppose $f, g \in M(n,k,\epsilon)_{\mathcal{O}}$ are modular forms with Dirichlet character $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ and assume that $a_q(f) \equiv a_q(g)$ mod $\mathfrak{m}$ for all $q \leq k\tau/12$, where*

$$\tau = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(n)] = \#\mathbb{P}^1(\mathbb{Z}/n\mathbb{Z}) = n \cdot \prod_{p|n \text{ prime}} \left(1 + \frac{1}{p}\right).$$

Then $f \equiv g$ mod $\mathfrak{m}$.

Let us conclude this section with the following result which gives bounds to compare forms in different weights:

Kohnen Theorem ([Koh04, Theorem 1]). *Let k_1, k_2 and n be positive integers, $k_1, k_2 \geq 2$, and let χ be a mod n Dirichlet character.*

Let $f_1 \in M(\Gamma_1(n), k_1, \chi)_{\mathbb{C}}$ and $f_2 \in M(\Gamma_1(n), k_2, \chi)_{\mathbb{C}}$, and let ℓ be a prime number. Assume that the q-expansions of f_1 and f_2 have coefficients in the ring of integers of a number field, and let λ be a maximal ideal herein such that $(\ell) \subset \lambda$. If $a_m(f_1) = a_m(f_2) \bmod \lambda$ for every m such that

$$m \leq \frac{\max\{k_1, k_2\}}{12} \cdot \begin{cases} [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(n) \cap \Gamma_1(\ell)] & \text{if } \ell > 2, \\ [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(n) \cap \Gamma_1(4)] & \text{if } \ell = 2 \end{cases}$$

then $a_m(f_1) = a_m(f_2) \bmod \lambda$ for every m.

In [Koh04], this result is stated under the assumption $k_1 \neq k_2$, but, as remarked in [Tak11, Section 2.1.2], the result is still true for $k_1 = k_2$. Indeed, for $\ell > 2$ we have that $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(n)] \leq [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(n) \cap \Gamma_1(\ell)]$, so the result holds by Sturm's Theorem. In the case $\ell = 2$ we have the analogous conclusion.

6.2 Using degeneracy maps

In this section we give a criterion to decide if two eigenforms for $\Gamma_1(n)$ over $\overline{\mathbb{F}}_\ell$ give rise to isomorphic Galois representations. We will use some theory on modular curves, see [KM85] and [Gro90] for a complete explanation. Analogous statements can be found in [CKR10].

Let n and k be positive integers, let ℓ be a prime not dividing n and let us fix $\overline{\mathbb{F}}_\ell$, an algebraic closure of $\mathbb{F}_\ell$. Suppose $n = mp^r$ with $r \geq 1$ and where p is a prime not dividing m. We have two degeneracy maps B_p and α on the modular curve $X_1(n)_{\overline{\mathbb{F}}_\ell}$:

$$\begin{array}{ccc} & X_1(m,p^r)_{\overline{\mathbb{F}}_\ell} & \\ {\scriptstyle B_p}\swarrow & & \searrow{\scriptstyle \alpha} \\ X_1(m,p^{r-1})_{\overline{\mathbb{F}}_\ell} & & X_1(m,p^{r-1})_{\overline{\mathbb{F}}_\ell} \end{array}$$

Using the moduli interpretation for $X_1(n)_{\overline{\mathbb{F}}_\ell}$, i.e. considering E/S, an elliptic curve over an $\overline{\mathbb{F}}_\ell$-scheme S, with P and Q respectively points of order m and p^r, we have the following description of the degeneracy maps: α is the forgetful map $\alpha\colon (E,P,Q) \longmapsto (E,P,pQ)$ and B_p is the p-th degeneracy map defined by $B_p\colon (E,P,Q) \mapsto (E/\langle p^{r-1}Q\rangle, \beta(P), \beta(Q))$, where β is an isogeny such that

$$\langle p^{r-1}Q\rangle \rightarrowtail E \xrightarrow{\beta} E/\langle p^{r-1}Q\rangle.$$

For any positive integers m dividing n and d dividing n/m, we define a degeneracy map $B_d^*\colon M(\Gamma_1(m),k)_{\overline{\mathbb{F}}_\ell} \to M(\Gamma_1(n),k)_{\overline{\mathbb{F}}_\ell}$, which maps a Katz modular form at level m to one of level n, as the map induced in cohomology by the map B_d. In terms of the q-expansion at the cusp ∞, this map is the substitution $q \mapsto q^d$:

$$f = \sum_{n\geq 0} a_n(f)q^n \longmapsto B_d^*(f) = \sum_{n\geq 0} a_n(f)q^{dn}$$

for further details see [EC11, p.40]. If needed, we will also stress the levels of the spaces of modular forms in the notation of the degeneracy map: we will write $B^*_{d,n,m}$ to denote the map B_d^* that we have just defined.

For every prime number p, using the degeneracy maps, we define the following morphism :

$$\eta_p \colon M(\Gamma_1(n),k)_{\overline{\mathbb{F}}_\ell} \to \begin{cases} M(\Gamma_1(np),k)_{\overline{\mathbb{F}}_\ell} & \text{if } p \mid n \\ M(\Gamma_1(np^2),k)_{\overline{\mathbb{F}}_\ell} & \text{if } p \nmid n \end{cases}$$

by

$$\eta_p = \begin{cases} B^*_{1,n,np} - B^*_{p,n,np} T_p & \text{if } p \mid n; \\ B^*_{1,n,np^2} - B^*_{p,n,np^2} T_p + p^{k-1} B^*_{p^2,n,np^2} \langle p \rangle & \text{if } p \nmid n. \end{cases}$$

From the compatibility relation between Hecke operators and degeneracy maps, it follows that for a given prime p we have $T_p \eta_p = 0$.

Let n_1, n_2, k be positive integers and let ℓ be a prime number $\ell \nmid n_1 n_2$, we will use the following notation:

$$\begin{aligned} N(n_1,n_2) &:= \operatorname{lcm}(n_1,n_2) \prod_{p \mid n_1 n_2 \text{ prime}} p, \\ d_k(n_1,n_2,\ell) &:= \frac{k+\ell+1}{12} [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N(n_1,n_2))]. \end{aligned}$$

Lemma 6.2.1. *Let n_1 and n_2 be integers, and let ℓ be a prime not dividing $n_1 n_2$. Let $f_1 \in S(\Gamma_1(n_1),k)_{\overline{\mathbb{F}}_\ell}$ and $f_2 \in S(\Gamma_1(n_2),k)_{\overline{\mathbb{F}}_\ell}$ be eigenforms. If $\epsilon_{f_1} = \epsilon_{f_2}$ and the coefficients of the the q-expansions at the cusp ∞ of f_1 and f_2 satisfy $a_p(f_1) = a_p(f_2)$ for all primes p not dividing $N(n_1,n_2)$ and $p \leq d_k(n_1,n_2,\ell)$, then ρ_{f_1} and ρ_{f_2} are isomorphic.*

Proof. For all primes p dividing $n_1 n_2$ we apply the operators η_p to f_1 and to f_2. In this way, we have two forms $f_1', f_2' \in S(\Gamma_1(n_1,n_2),k)_{\overline{\mathbb{F}}_\ell}$ with $a_p(f_1') = a_p(f_2') = 0$ for all primes p dividing $n_1 n_2$ and with the same character by hypothesis.

Together with our assumptions, this gives $a_p(\theta_\ell(f_1')) = a_p(\theta_\ell(f_2'))$ for all primes $p \leq d_k(n_1,n_2,\ell)$. This implies that for some $\lambda \in \overline{\mathbb{F}}_\ell^*$, the q-expansions of $\theta_\ell(f_1')$ and $\lambda\theta_\ell(f_2')$ agree up to order $d_k(n_1,n_2,\ell)$. Hence, by Sturm Theorem, or more precisely by Corollary 6.1.3, yields $\theta_\ell(f_1') = \lambda\theta_\ell(f_2')$. In particular, this implies that ρ_{f_1} and ρ_{f_2} are isomorphic. □

Combining Kohnen's result with Lemma 6.2.1 we have the following corollary:

Corollary 6.2.2. *Let n_1 and n_2 be integers, and let ℓ be a prime not dividing $n_1 n_2$. Let $f_1 \in S(\Gamma_1(n_1),k_1)_{\overline{\mathbb{F}}_\ell}$ and $f_2 \in S(\Gamma_1(n_2),k_2)_{\overline{\mathbb{F}}_\ell}$ be eigenforms and assume $k_1, k_2 \geq 2$. If $\epsilon_{f_1} = \epsilon_{f_2}$ and the coefficients of the the q-expansions*

at the cusp ∞ *of* f_1 *and* f_2 *satisfy* $a_p(f_1) = a_p(f_2)$ *for all primes* p *with* $p \nmid n_1 n_2 \ell$ *and*

$$p \leq \frac{\max\{k_1, k_2\}}{12} \cdot \begin{cases} [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N(n_1, n_2)) \cap \Gamma_1(\ell)] & \text{if } \ell > 2, \\ [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N(n_1, n_2)) \cap \Gamma_1(4)] & \text{if } \ell = 2 \end{cases},$$

then ρ_{f_1} *and* ρ_{f_2} *are isomorphic.*

Let us remark that if the weights k_1 and k_2 are not both greater than 2 then multiplying by the Hasse invariant we are in the hypotheses of Corollary 6.2.2. In Lemma 6.2.1 and Corollary 6.2.2 we are dealing with mod ℓ cusp forms. The general case can be deduced from the following theorem, in which is given a bound to compare two semi-simple 2-dimensional continuous odd Galois representations:

Theorem 6.2.3 ([Tak11, Theorem 1])**.** *Let* ℓ *be a prime number and let* n *be an integer not divisible by* ℓ*. Let* ρ, ρ' *be two semi-simple, 2-dimensional, continuous, Galois representations with Artin conductor dividing* n*. Assume* ρ *is odd.*

Let

$$n' = \prod_{\substack{p \mid n \\ p^2 \nmid n}} p,$$

$$\kappa(n, \ell) = \begin{cases} \ell/12 \cdot (\ell^2 - 1)^2 n n' \prod_{p \mid n} (1 + 1/p) & \text{if } \ell > 2, \\ 4 n n' \prod_{p \mid n} (1 + 1/p) & \text{if } \ell = 2 \end{cases}.$$

If $\det(1 - \rho(\mathrm{Frob}_p)T) = \det(1 - \rho'(\mathrm{Frob}_p)T)$ *in* $\overline{\mathbb{F}}_\ell[T]$ *for every prime* $p \leq \kappa(n, \ell)$ *and not dividing* ℓn*, then* ρ *is isomorphic to* ρ'*.*

The bound $\kappa(n, \ell)$, given in the previous Theorem, is obtained combining the Sturm Theorem and the result by Kohnen, presented at the beginning of this chapter. In particular it uses Khare-Wintenberger Theorem, in the case of irreducible representation, and the observation that the weight is bounded by $\ell^2 - 1$ for reducible representations.

Remark 6.2.4. The method described in this section is not efficient. In fact, using degeneracy maps, we move the problem of comparing forms of different level and weight to the problem of comparing forms of the same level. In order to do so, we map the forms into the space of modular forms with greater level and weight and then do the comparison. This procedure avoids the study of the primes dividing the level, that are the primes where the associated representation can ramify.

In terms of the Sturm bound and, hence, of the number of Hecke operators needed, following this approach we have to compute many more operators

than the ones up to the Sturm bound at the given level. A rough comparison tell us that for mod ℓ modular forms at level n, with n not divisible by ℓ, we have to compute operators up to approximatively $\ell^2 kn^2/12$ instead of approximatively $kn/12$. In particular, the number of the operators required to perform an equality check depends on the characteristic ℓ, and, for computational purposes, this is extremely relevant.

In order to avoid the level raising, we need to study what happens at the primes dividing the level.

For all primes p dividing the level n, what is the relation between $f(T_p)$ and ρ_f? What values can $f(T_p)$ assume for all primes p dividing the level n in terms of ρ_f? What values can $f(T_\ell)$ assume? Answering these questions is the first step in order to compare eigenforms at level n using the Sturm bound at level n.

6.3 Using modularity and local description

Let n and k be positive integers, let ℓ be a prime number not dividing n, such that $2 \leq k \leq \ell + 1$. Let $f : \mathbb{T}(n,k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings and let $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the unique, up to isomorphism, continuous semi-simple representation attached to it, as stated in Theorem 4.0.4. In this section we recall statements about the local representation at ℓ and at primes dividing the level n.

Local representation at ℓ

Let $G_\ell = \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell) \subset G_{\mathbb{Q}}$ be the decomposition subgroup at ℓ. Let I_ℓ be the inertia subgroup, $I_{\ell,w}$ the wild inertia subgroup at ℓ and $I_t = I_\ell/I_{\ell,w}$ the tame inertia subgroup.

Theorem 6.3.1 (Deligne)**.** *Let n be a positive integer, let ℓ be a prime not dividing n, let $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character and let k be a positive integer $2 \leq k \leq \ell + 1$. Let $f : \mathbb{T}_\epsilon(n,k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings such that $f(T_\ell) \neq 0$. Then $\rho_f|_{G_\ell}$ is reducible, and up to conjugation in $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$, we have*

$$\rho_f|_{G_\ell} \cong \begin{pmatrix} \chi_\ell^{k-1}\lambda(\overline{\epsilon}(\ell)/f(T_\ell)) & * \\ 0 & \lambda(f(T_\ell)) \end{pmatrix}$$

where $\lambda(a)$ is the unramified character of G_ℓ taking $\mathrm{Frob}_\ell \in G_\ell/I_\ell$ to a, for any $a \in \overline{\mathbb{F}}_\ell^*$ and $\overline{\epsilon} : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ is the character defined by $\overline{\epsilon}(b) = f(\langle b \rangle)$ for all $b \in (\mathbb{Z}/n\mathbb{Z})^*$.

Proof. See [Gro90, Section 12 and Proposition 12.1]. □

In [Gro90, Proposition 12.1] Gross proved that, denoted by V the 2-dimensional $\overline{\mathbb{F}}_\ell$-vector space underlying the representation ρ_f of $G_\mathbb{Q}$, there is an exact sequence of G_ℓ-modules: $0 \to D \to V \to D' \to 0$, with D and D' of dimension 1, such that G_ℓ acts on D by $\chi_\ell^{k-1}\lambda(\epsilon(\ell)/f(T_\ell))$ and on D' by the unramified character $\lambda(f(T_\ell)$. Moreover, this sequence of G_ℓ-modules is always non-split if the form f has filtration $k+1$, in the sense of [Gro90, p.459]. As remarked in [Gro90, p.488], in this case the representation ρ_f is "très ramifiée" at ℓ, in the sense of [Ser87, p.186]. If the weight of f is between 2 and ℓ, the splitting of the sequence is connected to the existence of companion forms: see [Gro90, Theorem 13.10]. Moreover, if k is not ℓ the existence of a companion form means that the representation ρ_f is tamely ramified at ℓ, in the sense of [Ser87, p.186]. For weight ℓ, the existence of a companion form means that the representation ρ_f is unramified at ℓ, see [Gro90, Corollary 13.11].

Theorem 6.3.2 (Fontaine)**.** *Let n be a positive integer, let ℓ be a prime not dividing n, let $\epsilon\colon (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character and let k be a positive integer $2 \leq k \leq \ell+1$. Let $f\colon \mathbb{T}_\epsilon(n,k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings such that $f(T_\ell) = 0$. Then $\rho_f|_{G_\ell}$ is irreducible, and up to conjugation in $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$, we have*

$$\rho_f|_{I_\ell} \cong \begin{pmatrix} \varphi'^{k-1} & 0 \\ 0 & \varphi^{k-1} \end{pmatrix}$$

where $\varphi', \varphi\colon I_t \to \overline{\mathbb{F}}_\ell^*$ are the two fundamental characters of level 2 (viewed as characters of I_ℓ via the natural surjection $I_\ell \to I_\ell/I_{\ell,w} = I_t$).

Proof. See [Edi92, Section 6]. □

Local representation at primes dividing the level

Let p be a prime dividing n. Let $G_p = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \subset G_\mathbb{Q}$ be the decomposition subgroup at p. Let I_p be the inertia subgroup, $I_{p,w}$ the wild inertia subgroup and I_t the tame inertia subgroup.

Serre in [Ser87, Conjecture 3.2.6$_?$] states a Conjecture about the local structure of a continuous irreducible 2-dimensional odd Galois representation at primes dividing the conductor and the characteristic. This conjecture has been proved by Vignéras in [Vig89], for primes dividing the conductor but not the characteristic, and by Gross in [Gro90] in the remaining case.

Theorem 6.3.3 (Gross-Vignéras)**.** *Let $\rho : G_\mathbb{Q} \to \mathrm{GL}(V)$ be a continuous, odd, irreducible representation of the absolute Galois group over $\mathbb{Q}$ to a 2-dimensional $\overline{\mathbb{F}}_\ell$-vector space V. Let $n = \mathrm{N}(\rho)$ and $k = k(\rho)$, let $f \in S(n,k)_{\overline{\mathbb{F}}_\ell}$ be an eigenform such that $\rho_f \cong \rho$. Let p be a prime divisor of ℓn.*

(1) *If $f(T_p) \neq 0$, then there exists a stable line $D \subset V$ for the action of G_p, the decomposition subgroup at p, such that the inertia group at p acts trivially on V/D. Moreover, $f(T_p)$ is equal to the eigenvalue of* Frob_p *which acts on V/D.*

(2) *If $f(T_p) = 0$, then there exists no stable line $D \subset V$ as in* (1).

Let us make some remarks and observations. If p divides n, then there exists at most one line $D \subset V$ with the properties stated in (1): otherwise there would be a contradiction with the representation being ramified at p. Moreover, such a line exists if and only if $v_p(n) = 1$ or $v_p(n) = v_p(\mathrm{cond}(\epsilon)) \geq 2$ since if $v_p(n) \geq 2$ and $v_p(\mathrm{cond}(\epsilon)) = 0$ then $f(T_p) = 0$ by [DS74, 1.8]. If $v_p(n) = 1$ and $v_p(\mathrm{cond}(\epsilon)) = 0$ then the eigenvalue of Frob_p acting on V/D satisfies $f(T_p)^2 = \tilde{\epsilon}(p)p^{k-2}$, where $\tilde{\epsilon}$ is the character satisfying:

$$\begin{array}{ccc} (\mathbb{Z}/n\mathbb{Z})^* & \xrightarrow{\quad\epsilon\quad} & \overline{\mathbb{F}}_\ell^* \\ & \searrow \quad \nearrow_{\tilde{\epsilon}} & \\ & (\mathbb{Z}/(n/p)\mathbb{Z})^* & \end{array}$$

We have already described the local representation at ℓ, let us remark that if the representation is ramified at ℓ then the line D as in (1) exists unique, while if the representation is not ramified at ℓ (hence, its weight is ℓ), then there are two possible eigenvalues of Frob_ℓ.

Before giving the statement of the main results of this section, let us recall the Deligne-Serre lifting lemma, since it will be a crucial element in the proof.

Deligne-Serre lifting lemma

Deligne-Serre lifting lemma ([DS74, Lemma 6.11])**.** *Let M be a finitely generated free module on a discrete valuation ring $\mathcal{O}$, with maximal ideal $\mathfrak{m}$, residue field k, and field of fractions K. Let T be a commuting family of endomorphisms of M. Let $f \in M \otimes k$ be a nonzero common eigenvector of $t \in T$ and let $a_t \in k$ be the corresponding eigenvalue. Then there exists a discrete valuation ring $\mathcal{O}'$ containing $\mathcal{O}$, with maximal ideal $\mathfrak{m}'$ such that $\mathcal{O} \cap \mathfrak{m}' = \mathfrak{m}$, with field of fractions K' a finite extension of K, and a nonzero element $\tilde{f}$ of $M' = \mathcal{O}' \otimes_{\mathcal{O}} M$ which is an eigenvector of all $t \in T$ of eigenvalue $\tilde{a}_t$, such that $\tilde{a}_t \equiv a_t$ modulo $\mathfrak{m}'$.*

Proof. In [DS74] are given two different proofs of this statement. The key point is that, denoted by H be the subalgebra of $\mathrm{End}(M)$ generated by T, one may suppose that $K \otimes H$ is a product of artinian rings, after making a finite extension of scalars if needed. □

Corollary 6.3.4. *Let n be a positive integer, let ℓ be a prime number not dividing n, and let k be a positive integer $2 \leq k \leq \ell+1$. Let $f \in S(\Gamma_1(n), k)_{\overline{\mathbb{F}}_\ell}$ be an eigenform for all Hecke operators. Then there exists a discrete valuation ring $\mathcal{O}_{K_\lambda}$ that contains $\mathbb{Z}_\ell$ and has maximal ideal λ satisfying $\mathbb{Z}_\ell \cap \lambda = (\ell)$ so that there exists a nonzero $\tilde{f} \in S(\Gamma_1(n), k)_{\mathcal{O}_{K_\lambda}}$ which is a simultaneous eigenform for all Hecke operators, with eigenvalues equal to the eigenvalues of f once reduced modulo λ.*

Proof. This statement follows from the Deligne-Serre lifting lemma, observing that $\mathbb{T}(n,k)$ is free of finite rank as $\mathbb{Z}$-module. □

The "old-space"

Let n and k be positive integers, let ℓ be a prime number not dividing n, such that $2 \leq k \leq \ell + 1$. Let $f : \mathbb{T}(n,k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings and let $\rho_f : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the unique, up to isomorphism, continuous semi-simple representation attached to it, as stated in Theorem 4.0.4.

The Hecke algebra $\mathbb{T}(n,k)$ is free of finite rank as $\mathbb{Z}$-module, then, by the Deligne-Serre lifting lemma and Corollary 6.3.4, we can choose a lift $\tilde{f}$ of f of level n:

$$\begin{array}{ccc} \mathbb{T}(n,k) & \xrightarrow{\tilde{f}} & \mathcal{O}_{K_\lambda} \\ & \searrow^{f} & \downarrow \\ & & \overline{\mathbb{F}}_\ell \end{array}$$

where $\mathcal{O}_{K,\lambda}$ is the completion of $\mathcal{O}_K$, the ring of integer of the number field K, given in Corollary 6.3.4, at a chosen prime λ containing ℓ. For each choice of λ in K such that $(\ell) \subset \lambda$, we have an ℓ-adic Galois representation $\rho_{\tilde{f}} : G_\mathbb{Q} \to \mathrm{GL}_2(K_\lambda)$ associated to $\tilde{f}$, hence we have a compatible system of Galois representations. Let us denote by V_λ the vector space over K_λ underlying the representation, then

$$\rho_{\tilde{f}} \colon G_\mathbb{Q} \to \mathrm{GL}(V_\lambda).$$

Let $\tilde{f}_{\mathrm{new}}$ be the newform giving rise to $\tilde{f}$, i.e. $\tilde{f}_{\mathrm{new}}$ is a modular form new of weight k and level $\mathrm{cond}(\rho_{\tilde{f}_{\mathrm{new}}})$, which is a divisor of n, as already recalled in Lemma 4.2.2. Moreover, $\rho_{\tilde{f}_{\mathrm{new}}}$ is isomorphic to $\rho_{\tilde{f}}$ by definition, and the semi-simplification of its reduction modulo ℓ is equivalent to ρ_f by construction.

By the Deligne-Serre lifting lemma and Corollary 6.3.4 the form $\tilde{f}$ is an eigenform for all Hecke operators at level n. The newform $\tilde{f}_{\mathrm{new}}$ is an eigenform for all Hecke operators at level $\mathrm{cond}(\rho_{\tilde{f}_{\mathrm{new}}})$. Let us recall that there is a Dirichlet series associated to $\tilde{f}_{\mathrm{new}}$, its L-function, see for example [DS05, Section 5.9], which has an Euler product expansion by [DS05, Theorem 5.9.2].

The L-function associated to $\tilde{f}_{\text{new}}$ is the L-function of the compatible system of $\rho_{\tilde{f}}$. This is due to the work of Shimura, Langlands, Deligne [Del73, Section 9], Carayol [Car86], and it has the following consequence, stated in [DI95, Theorem 12.5.14], the Euler factor of the L-function of (the compatible system of) $\rho_{\tilde{f}}$ at p, prime dividing $\text{cond}(\rho_{\tilde{f}_{\text{new}}})$, has degree at most 1 and it is given by:

$$\det(1 - p^{-s}\,\text{Frob}_p, (V_\lambda)_{I_p})^{-1} = (1 - \tilde{f}_{\text{new}}(T_p)p^{-s})^{-1},$$

where I_p is the inertia group at p, and $(V_\lambda)_{I_p}$ is the space of inertia coinvariants:

$$(V_\lambda)_{I_p} \colon = V/\left\langle \{v - hv \,|\, \forall v \in V_\lambda, h \in I_p\} \right\rangle.$$

For any prime q not dividing $\text{cond}(\rho_{\tilde{f}_{\text{new}}})$, the Euler factor of the L-function of $\tilde{f}_{\text{new}}$ has degree at most 2 and it is equal to:

$$\det(1 - q^{-s}\,\text{Frob}_q, (V_\lambda)_{I_q})^{-1} = (1 - \tilde{f}_{\text{new}}(T_q)q^{-s} + \tilde{f}_{\text{new}}(\langle q \rangle)q^{k-1-2s})^{-1}.$$

The following theorem hold:

Theorem 6.3.5. *Let n and k be positive integers, let ℓ be a prime not dividing n, and such that $2 \leq k \leq \ell + 1$. Let $f : \mathbb{T}(n,k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings and let $\rho_f : G_{\mathbb{Q}} \to \text{GL}_2(\overline{\mathbb{F}}_\ell)$ be the unique, up to isomorphism, continuous semi-simple representation corresponding to it, as in Corollary* 4.0.5. *Let p be a prime dividing n and let $\text{N}_p(n)$ denote the valuation at p of n. The following holds:*

(a) if $\text{N}_p(\rho_f) = 0$, let $\overline{\alpha}$ and $\overline{\beta}$ be the eigenvalues of $\rho_f(\text{Frob}_p)$, then
- *if $\text{N}_p(n) = 1$ then $f(T_p) \in \{\overline{\alpha}, \overline{\beta}\}$;*
- *if $\text{N}_p(n) > 1$ then $f(T_p) \in \{0, \overline{\alpha}, \overline{\beta}\}$.*

(b) if $\text{N}_p(\rho_f) > 0$ and $f(T_p) \neq 0$, then there exists a unique unramified quotient line for the representation and $f(T_p)$ is the eigenvalue of Frob_p on it.

Moreover, if $f(T_\ell) \neq 0$ then then $f(T_\ell) = \mu$, where μ is the scalar representing the action of Frob_ℓ on an unramified quotient line for the representation, meanwhile if $f(T_\ell) = 0$ there exist no such line.

Proof. As the Hecke algebra $\mathbb{T}(n,k)$ is free of finite rank as $\mathbb{Z}$-module, we apply the Deligne-Serre lifting lemma so we choose a lift $\tilde{f}$ of f with the same level of f: $\tilde{f} \colon \mathbb{T}(n,k) \to \mathcal{O}_{K_\lambda}$, where $\mathcal{O}_{K,\lambda}$ is the completion of $\mathcal{O}_K$, the ring of integer of the number field K, at a chosen prime λ containing ℓ. For each choice of λ in K, $(\ell) \subset \lambda$, we have an ℓ-adic Galois representation associated to $\tilde{f}$ that we denote as $\rho_{\tilde{f}} \colon G_{\mathbb{Q}} \to \text{GL}_2(K_\lambda)$. Let us denote by V_λ the vector space over K_λ where the representation $\rho_{\tilde{f}}$ is realized.

Let $\tilde{f}_{\text{new}}$ be the newform giving rise to $\tilde{f}$. Hence, $\text{cond}(\rho_{\tilde{f}_{\text{new}}})$ divides n.

Let us prove statement (a).

Let p be a prime dividing n but not $\mathrm{cond}(\rho_{\tilde{f}_{\mathrm{new}}})$. Then the representation $\rho_{\tilde{f}_{\mathrm{new}}}$ is unramified at p, so $\tilde{f}_{\mathrm{new}}(T_p) = \mathrm{Trace}(\rho_{\tilde{f}_{\mathrm{new}}}(\mathrm{Frob}_p))$. Let α, β be the eigenvalues of $\rho_{\tilde{f}_{\mathrm{new}}}(\mathrm{Frob}_p)$. Let $r = \mathrm{N}_p(n)$. Following [Par99, Sections 3.3 and 3.4], if $r = 1$ then $\tilde{f}(T_p) \in \{\alpha, \beta\}$ hence, reducing modulo λ, we have that $f(T_p) \in \{\overline{\alpha}, \overline{\beta}\}$ where $\overline{\alpha}$ is the image of α through the reduction map (similarly $\overline{\beta}$). On the other hand, if $r \geq 2$ then $\tilde{f}(T_p) \in \{0, \alpha, \beta\}$ hence reducing modulo λ we have that $f(T_p) \in \{0, \overline{\alpha}, \overline{\beta}\}$. In both cases ρ_f is unramified at p and we have

$$x^2 - \tilde{f}_{\mathrm{new}}(T_p)x + \tilde{f}_{\mathrm{new}}(\langle p \rangle)p^{k-1} = (x - \alpha)(x - \beta).$$

Let us now prove statement (b).

Let p be a prime dividing $\mathrm{cond}(\rho_{\tilde{f}_{\mathrm{new}}})$. Then $\rho_{\tilde{f}}$ is ramified at p. This implies that $\dim_{K_\lambda}((V_\lambda)_{I_p})$ is 0 or 1. In the first case we have that $\tilde{f}(T_p) = 0$ by [Par99], hence, reducing modulo λ we have that $f(T_p) = 0$. In the second case, $(V_\lambda)_{I_p}$ is 1 dimensional, hence Frob_p acts as a scalar on it.

To study the local behaviour at ℓ, we will use Theorems 6.3.1 and 6.3.2. If $f(T_\ell) = 0$ then the representation restricted to the decomposition group at ℓ is irreducible, hence, $\dim_{K_\lambda}((V_\lambda)_{I_\ell})$ is 0. Therefore, $\tilde{f}(T_\ell) = 0$ by [Par99] and so $f(T_\ell) = 0$. On the other hand, if $f(T_\ell) \neq 0$ then the representation restricted to the decomposition group at ℓ can be either tamely ramified, or wildly ramified since the weight is larger than 2. In both cases, by Theorem 6.3.2 we have that $\dim_{K_\lambda}((V_\lambda)_{I_\ell})$ is 1. Hence Frob_ℓ acts as a scalar on it. □

What we have just discussed is essential for the comparison of two Katz modular forms in particular in order to determine the contribution at higher level coming from forms of lower level.

Let $f : \mathbb{T}(n, k) \to \overline{\mathbb{F}}_\ell$ and $g : \mathbb{T}(m, k) \to \overline{\mathbb{F}}_\ell$ be two Katz modular forms such that $m = \mathrm{cond}(\rho_g)$, the integer n is a multiple of m not divisible by ℓ and $2 \leq k \leq \ell + 1$. We want to decide if $\rho_f \cong \rho_g$ only using the Sturm Bound $B(n, k)$, i.e. the Sturm bound for modular forms of $\Gamma_0(n)$ and weight k. For the level part, this is equivalent to say that we want to know if "f is in the subspace of the old-space given by g at level n" i.e. f is in the subspace of $M(\Gamma_1(n), k)_{\overline{\mathbb{F}}_\ell}$ given by g through the degeneracy maps from level m to level n.

Theorem 6.3.6. *Let n, m and k be positive integers with n a multiple of m. Let ℓ be a prime not dividing n, and such that $2 \leq k \leq \ell + 1$. Let $f : \mathbb{T}(n, k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings and let $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the unique, up to isomorphism, continuous semi-simple representation*

corresponding to it. Let $g : \mathbb{T}(m,k) \to \overline{\mathbb{F}}_\ell$ *be a morphism of rings and let* $\rho_g : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ *be the corresponding Galois representation. Let us assume that* $\mathrm{N}(\rho_g) = m$ *and that the weight of* ρ_g *is minimal. The following holds:*

- *if* ρ_f *is ramified at* ℓ *then* ρ_f *is isomorphic to* ρ_g *if and only if* f *is in the subspace of the old-space given by* g *at level* n.
- *if* ρ_f *is unramified at* ℓ *then* ρ_f *is isomorphic to* ρ_g *if and only if* f *is either in the subspace of the old-space given by* g *at level* n *or in the subspace of the old-space given by* g' *at level* n*, where* g' *is the form such that* $g'(T_p) = g(T_p)$ *for all primes* p *different from* ℓ *and* $g'(T_\ell)$ *satisfies:*

$$x^2 - \mathrm{Trace}(\rho_f(\mathrm{Frob}_\ell))x + \det(\rho_f(\mathrm{Frob}_\ell)) = (x - g(T_\ell))(x - g'(T_\ell)).$$

Proof. Let us assume that ρ_f is ramified at ℓ.

If f is in the subspace of the old-space given by g at level n then by the description of the old-space, i.e. Theorem 6.3.5, we have that ρ_f is isomorphic to ρ_g.

Let us show that if ρ_f is isomorphic to ρ_g then f is in the subspace of the old-space given by g at level n. By hypotheses the conductor of ρ_g is m, hence the conductor of ρ_f is m since the two representations are isomorphic. For all unramified primes the characteristic polynomials of the two representations are the same, hence $\mathrm{Trace}(\rho_f(\mathrm{Frob}_p)) = \mathrm{Trace}(\rho_g(\mathrm{Frob}_p))$ so $f(T_p) = g(T_p)$ for all primes p not dividing $n\ell$.

All the possible values of $f(T_p)$ for p prime dividing $n\ell$ are listed in Theorem 6.3.5, hence, from the isomorphism of the representations, it follows that f is in the subspace of the old-space given by g at level n.

Let us assume that ρ_f is unramified at ℓ.

This implies that the weight is ℓ and the representation arises from a form in weight one, which gives rise to two different forms in weight ℓ, as images of the Frobenius or through multiplication by the Hasse invariant, as already underlined in Remark 4.2.3. Let g' be the form such that $g'(T_p) = g(T_p)$ for all primes p different from ℓ and $g'(T_\ell)$ is equal to the other eigenvalue of the Hecke operator T_ℓ i.e. $g'(T_\ell)$ satisfies:

$$x^2 - \mathrm{Trace}(\rho_f(\mathrm{Frob}_\ell))x + \det(\rho_f(\mathrm{Frob}_\ell)) = (x - g(T_\ell))(x - g'(T_\ell)).$$

If f is either in the subspace of the old-space given by g at level n or in the subspace of the old-space given by g' then the representations ρ_f and ρ_g are isomorphic. Vice-versa, if the representations are isomorphic then the conductor of ρ_f is m and in Theorem 6.3.5 all the possible values of $f(T_p)$ for p prime dividing $n\ell$ are listed, hence since the isomorphism of the representations holds then f is in the subspace of the old-space given by g at level n or in the subspace of the old-space given by g' at level n. □

Algorithm 6.3.7 (Check if two mod ℓ forms give rise to the same 2-dimensional residual Galois representation)**.** Let n, m, k be positive integers with n a multiple of m. Let ℓ be a prime not dividing n such that $2 \leq k \leq \ell + 1$.

Let $\psi : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$ be a character. Let $g : \mathbb{T}_\psi(m,k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings and let $\rho_g : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the representation attached to g in Corollary 4.0.5. Assume that the representation ρ_g does not arise from lower level i.e. there exists no form of lower level with equivalent Galois representation.

Let $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character. Let $f : \mathbb{T}_\epsilon(n,k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings and let $\rho_f : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the representation attached to f in Corollary 4.0.5. Let $\overline{\epsilon} : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ be the character defined by $\overline{\epsilon}(a) = f(\langle a \rangle))$ for all $a \in (\mathbb{Z}/n\mathbb{Z})^*$. Analogously, let $\overline{\psi} : (\mathbb{Z}/m\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ be the character defined by $\overline{\psi}(b) = g(\langle b \rangle)$ for all $b \in (\mathbb{Z}/m\mathbb{Z})^*$.

Input: n, m, k, ℓ, $\overline{\epsilon}$, $\overline{\psi}$, $f(T_p)$ and $g(T_p)$ for p prime $p \leq B(n,k)$ where $B(n,k)$ is the Sturm bound for modular forms for $\Gamma_0(n)$ and weight k;
Output: if $\rho_g \cong \rho_f$ return 1; otherwise return 0.

---

if $\overline{\epsilon}(b) \neq \overline{\psi}(b)$ for $b \in (\mathbb{Z}/m\mathbb{Z})^*$ **then**
  return 0 and **stop**
else
  if $g(T_\ell) = 0$ and $f(T_\ell) \neq 0$ **then**
    return 0 and **stop**
  else if $g(T_\ell) \neq 0$ **then**
    if $k \neq \ell$ **then**
      if $f(T_\ell) \neq g(T_\ell)$ **then**
        return 0 and **stop**
    else
      if $f(T_\ell) \neq g(T_\ell)$ and g comes from weight 1 **then**
        Compute g' as in Theorem 6.3.6
        if $f(T_\ell) \neq g'(T_\ell)$ **then**
          return 0 and **stop**
      else
        return 0 and **stop**
  for p prime not dividing $n\ell$ and $p \leq B(n,k)$ **do**
    if $f(T_p) \neq g(T_p)$ **then**
      return 0 and **stop**
  for p prime dividing n **do**
    Let p_1 and p_2 be respectively the valuation at p of n and m
    if $p_2 = 0$ **then**
      Let $\{\overline{\alpha}, \overline{\beta}\}$ be the set of roots of $x^2 - g(T_p)x + g(\langle p \rangle)p^{k-1}$

      if $p_1 = 1$ **then**

```
                    if f(T_p) ∉ {ᾱ, β̄} then
                        return 0 and stop
                else
                    if f(T_p) ∉ {0, ᾱ, β̄} then
                        return 0 and stop
            else
                if g(T_p) = 0 and f(T_p) ≠ 0 then
                    return 0 and stop
                else if g(T_p) ≠ 0 and f(T_p) ≠ 0 then
                    if f(T_p) ≠ g(T_p) then
                        return 0 and stop
        return 1
```

Theorem 6.3.8. *Algorithm* 6.3.7 *is correct.*

Proof. If the two representations are isomorphic then their determinants are equal, therefore $\overline{\psi} = \mathrm{Res}^{\mathbb{Z}/m\mathbb{Z}}_{\mathbb{Z}/n\mathbb{Z}}(\overline{\epsilon})$.

If $\rho_f \cong \rho_g$ then by Theorem 6.3.6 f is in the subspace of the old-space given by g at level n if the representation ρ_f is ramified at ℓ. Otherwise, if ρ_f is unramified at ℓ it could be in the old-space given by the form g or in the one given by g', form such that $g'(T_p) = g(T_p)$ for all primes p different from ℓ and $g'(T_\ell)$ satisfies:

$$x^2 - \mathrm{Trace}(\rho_f(\mathrm{Frob}_\ell))x + \det(\rho_f(\mathrm{Frob}_\ell)) = (x - g(T_\ell))(x - g'(T_\ell)).$$

This means that the form g comes from weight 1, see [Edi06, Section 4] and [Wie05, Section 4.5, Section 4.6], and we check it using, for example, Algorithm 4.3.4 and Algorithm 4.6.1 in [Wie05] since we are only looking at eigenforms.

The form f is in the subspace of the old-space given by g at level n through the degeneracy maps from level m to level n. Moreover, g is such that the representation ρ_g does not arise from lower level. Therefore, we apply Theorem 6.3.5: for all p prime dividing the level n, the value of $f(T_p)$ is among the eigenvalues in the old-space given by g at level n. □

Remark 6.3.9. In the previous theorem and algorithm we are assuming that the representation ρ_g does not arise from lower level. This condition can be verified through a bottom-up approach: given a level n it is needed to compute all data coming from lower level (or compare with data stored in a database). In particular, this means that the information about the level of first appearance of a system of eigenvalues is stored in the database.

Remark 6.3.10. I would like to thank Professor Kevin Buzzard for the correspondence we had on this topic, which has been a motivating starting point for the theorems and the algorithm that we presented in this section.

6.4 Algorithm: bottom-up approach

The goal of the Part II of this thesis is to outline an algorithm, which receives as input: n and k positive integers, a prime ℓ not dividing n and such that $2 \leq k \leq \ell + 1$, a character $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ and a morphism of rings $f : \mathbb{T}_\epsilon(n,k) \to \overline{\mathbb{F}}_\ell$, and which gives as output the image of the Galois representation ρ_f, given by Corollary 4.0.5, up to conjugation, as a subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$.

In this section we give a first description of the algorithm, explaining one of the main ideas in it.

As explained in the introduction, the Hecke algebra $\mathbb{T}_\epsilon(n,k)$ is free of finite rank as $\mathbb{Z}$-module, hence, a morphism of rings $f : \mathbb{T}_\epsilon(n,k) \to \overline{\mathbb{F}}_\ell$ can be expressed, using the module structure and the relative multiplication table, giving the image of a basis.

Given this data we compute the system of eigenvalues $f_{n,k}$ associated to the morphism f:

$$\begin{aligned} f_{n,k}\colon \mathcal{P} &\to \overline{\mathbb{F}}_\ell \times \overline{\mathbb{F}}_\ell \\ p &\mapsto (f(T_p), f(\langle p \rangle)) \end{aligned}$$

Since we use the system of eigenvalues to check equalities between mod ℓ modular forms, it is not needed to know the full system, it is enough to know it for primes up to a certain bound: we will denote as

$$\begin{aligned} f^{(*)}_{n,k} = f_{n,k}|_{\mathcal{P}\leq(*)}\colon \{\mathcal{P} \leq (*)\} &\to \overline{\mathbb{F}}_\ell \times \overline{\mathbb{F}}_\ell \\ p &\mapsto (f(T_p), f(\langle p \rangle)) \end{aligned}$$

the system of eigenvalues truncated at $(*)$. Usually, $(*)$ will be the Sturm bound of a certain level and weight as explained in the previous section.

The algorithm that we are constructing is associated to a database which stores the data obtained.

For any new level n, we store in the database the system of eigenvalues at levels dividing n and weights smaller than the weight considered, so that there is no need to re-do the computations if the representation arises from lower level or weight. Indeed, if the representation arises from lower level or weight we will have directly the image right after the preliminary steps that we are going to describe.

The first reduction step is a weight reduction. Given a system of eigenvalues, it could happen that it also occurs also at lower weight, see [Edi92, Proposition 3.3 and Theorem 3.4]. Since we are assuming that the weight is between 2 and $\ell+1$, then it is possible that the same system of eigenvalues appears in weight 2 and $\ell+1$. In particular, if this is the case the two system will be equal for all operators T_p for p prime, according to [Edi92, Theorem 3.4]. The equality can be checked for p up to $B(n,\ell+1)$, i.e. the Sturm bound for modular forms for $\Gamma_0(n)$ and weight $\ell+1$. Indeed, since the systems (i.e. the corresponding modular form) in weight 2 and level n can be mapped to weight $\ell+1$ using the Hasse invariant, the equality is checked between forms of level n and weight $\ell+1$ with given character, therefore we apply Corollary 6.1.3.

Algorithm 6.4.1 (Reduction on the weight)**.** Let n be a positive integer, let ℓ be a prime not dividing n and let $k=\ell+1$. Let $\epsilon\colon (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character. Let $f\colon \mathbb{T}_\epsilon(n,\ell+1) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings and let $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the representation attached to f in Corollary 4.0.5. Let $\bar{\epsilon} : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ be the character defined by $\bar{\epsilon}(a) = f(\langle a\rangle)$ for all $a \in \mathbb{Z}/n\mathbb{Z}^*$.

Input: n, ℓ, ϵ, $f(T_p)$ for p prime $p \le B(n,\ell+1)$, i.e. the Sturm bound for modular forms for $\Gamma_0(n)$ and weight $\ell+1$;
Output: return 0 if there exist no form g of weight 2 and level n such that $\rho_f \cong \rho_g$; otherwise return g.

---

for $g \in S(n,2,\bar{\epsilon})_{\overline{\mathbb{F}}_\ell}$ **do**
  if $g(T_p) = f(T_p)$ for all primes p with $p \le B(n,\ell+1)$ and $p \neq \ell$ **then**
    return g and **stop**
return 0

The second reduction step regards the level: the representation can arise from lower level than the one given. Applying Lemma 4.2.2, the system of eigenvalues $f_{n,k}$ can occur only in level m dividing n, this because the representation ρ_f has conductor dividing n. This check is done in Algorithm 6.3.7, computing the image of Hecke operators T_p for p prime less than $B(n,k)$, the Sturm Bound for modular forms for $\Gamma_0(n)$ and weight k, since the character is fixed and so we can apply Corollary 6.1.3. In fact, for the primes dividing n we have prescribed values.

After these preliminary steps we have computed the minimal level and weight for which the representation ρ_f occurs:

Definition 6.4.2. Let n and k be two positive integers, let ℓ be a prime such that $(n,\ell)=1$ and $2 \le k \le \ell+1$, and let $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character.

Let $f : \mathbb{T}_\epsilon(n,k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings and let $\rho_f : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the representation attached to f in Corollary 4.0.5. We say that ρ_f is *minimal* with respect to *level* if it does not arise from any mod ℓ modular form of level lower than n. We say that ρ_f is *minimal* with respect to *weight* if it does not arise from any mod ℓ modular form of weight lower than k.

Remark 6.4.3. It is clear that if the representation ρ_f is minimal with respect to level and irreducible then the level is equal to $\mathrm{N}(\rho_f)$ by Khare-Wintenberger Theorem, see Remark 4.2.3.

With the data obtained by the algorithm we will construct a database. For any new level n for which the algorithm compute the image, we store in the database the data coming from systems of eigenvalues of levels dividing n.

Let us suppose that we run the algorithm for a given input. The output of the algorithm can be used to fill in the database at higher levels and weights. If the weight is 2 then we do know that the same system of eigenvalues occur in weight $\ell+1$ by multiplication with the Hasse invariant. Analogously, we can list all the systems of eigenvalue at a higher level coming from the given one and so we have the following algorithm which is correct, since Algorithm 6.3.7 is correct.

Algorithm 6.4.4 (Old-space from a given mod ℓ form)**.** Let n, m, k be positive integers with n a multiple of m. Let ℓ be a prime not dividing n such that $2 \leq k \leq \ell + 1$. Let $g : \mathbb{T}_\psi(m,k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings and let $\rho_g : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the representation attached to g in Corollary 4.0.5.

Input: n, m, k, ℓ, $g(T_p)$ for p prime $p \leq B(n,k)$ where $B(n,k)$ is the Sturm bound for modular forms for $\Gamma_0(n)$ and weight k;
Output: list of systems of eigenvalue in the subspace of the old-space given by g at level n.

Set $v \leftarrow [\,]$
for $f \in S(n,k)_{\overline{\mathbb{F}}_\ell}$ **do**
    Run Algorithm 6.3.7 for f and g
    if the output of Algorithm 6.3.7 is 1 **then**
        store f in v
return v

Chapter 7

Reducible representations

In this chapter we study reducible 2-dimensional representations of the absolute Galois group $G_{\mathbb{Q}}$ of an algebraic closure of $\mathbb{Q}$ which are modular. We recall some results about Eisenstein series and generalized Bernoulli numbers in order to state an algorithm to check reducibility of a 2-dimensional semi-simple modular representation.

The interplay between reducible representations, Bernoulli numbers and Eisenstein series can be underlined through the Herbrand-Ribet Theorem, see [Rib76b] and [Maz11].

Let B_k be the k-th Bernoulli number, defined in *Ars Conjectandi* by Bernoulli, see [Ber06]. It is the coefficient of $x^k/k!$ in the power series expansion

$$\frac{x}{e^x - 1} = \sum_{k=0}^{\infty} B_k \frac{x^k}{k!}.$$

Therefore, $B_0 = 1$ and $B_1 = -1/2$. As the function $x/(e^x-1) - 1 + x/2$ is even, i.e. invariant under the map $x \mapsto -x$, we have that B_k vanishes for odd integers $k > 1$. Ken Ribet managed to pass from properties of Bernoulli numbers to note a consequence about Eisenstein series. This allowed him to construct certain cuspidal modular forms related to these Eisenstein series:

Proposition 7.0.5 ([Rib76b, Proposition 3.5]). *Suppose that ℓ divides B_k for some even integer k such that $2 \leq k \leq p-3$. Then there exists a normalized, weight k, level 1, cuspidal eigenform $f = \sum_{n>0} a_n q^n \in S(1,k)_{\mathbb{C}}$ and a prime λ, dividing ℓ, of the number field generated by the coefficients of the q-expansion of f, such that for every prime $p \neq \ell$ the coefficient a_p is λ-integral and*

$$a_p \equiv 1 + p^{k-1} \bmod \lambda.$$

This leads to the construction of an abelian extension of the cyclotomic field $\mathbb{Q}(\zeta_\ell)$ which is unramified and cyclic of degree ℓ but non-abelian over $\mathbb{Q}$. In fact, a way to construct these extensions is through non-abelian reducible indecomposable representation of $G_{\mathbb{Q}}$ into $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$.

Herbrand-Ribet Theorem ([Rib76b]). *Let ℓ be a prime number and k an integer greater than 2 and smaller than $\ell-3$. The following are equivalent:*

1. *The numerator of the Bernoulli number $B_{2k}/4k$ is divisible by ℓ.*

2. *Let K be the cyclotomic field $K = \mathbb{Q}(\zeta_\ell)$. There is a field extension L/K that is cyclic of degree ℓ, that is everywhere unramified, and that has the further property that $L/\mathbb{Q}$ is Galois.*

7.1 Generalized Bernoulli numbers and Eisenstein series

Let n be a positive integer. A Dirichlet character modulo n is a multiplicative homomorphism from $(\mathbb{Z}/n\mathbb{Z})^*$ to $\mathbb{C}^*$. In particular, using Fourier theory for finite abelian groups, any function on $(\mathbb{Z}/n\mathbb{Z})^*$ can be written as a linear combination of Dirichlet characters, see [Ser78, Section 6]. Since Dirichlet characters are multiplicative, the L-series of a Dirichlet character admits an Euler product. Let us remark that it is possible to compute the order and the conductor of a Dirichlet character, for example using [Ste07, Algorithm 4.14] and [Ste07, Algorithm 4.19].

Let χ be a Dirichlet character modulo n, we define the k-th generalized Bernoulli number B_k^χ attached to χ as the coefficient of $x^k/k!$ in the following identity of formal series:

$$\sum_{j=1}^{n} \frac{\chi(j) x e^{jx}}{e^{nx} - 1} = \sum_{k=0}^{\infty} B_k^\chi \frac{x^k}{k!}.$$

If χ is the trivial character then $B_k^\chi = B_k$ for $k > 1$ and $B_1^\chi = -B_1 = 1/2$. The generalized Bernoulli numbers are algebraic numbers in the number field obtained adjoining to $\mathbb{Q}$ all values of χ, for further details see [Car59a] and [Car59b]. Algorithm [Ste07, Algorithm 5.2] computes generalized Bernoulli numbers attached to a given character with high precision.

Let us recall that a Dirichlet character modulo n is called primitive if n is equal to the conductor of the character, see [Ste07, Definition 4.18].

We have the following result which identifies the denominator of a generalized Bernoulli number:

Proposition 7.1.1 ([Ste07, Theorem 5.7]). *Let k be an integer and χ be a non-trivial primitive Dirichlet character. Let us define the integer d as follows:*

$$d := \begin{cases} 1 & \text{if } \operatorname{cond}(\chi) \text{ is divisible by two distinct primes,} \\ 2 & \text{if } \operatorname{cond}(\chi) = 4, \\ 1 & \text{if } \operatorname{cond}(\chi) = 2^m,\ m > 2, \\ kp & \text{if } \operatorname{cond}(\chi) = p,\ \text{prime, } p > 2, \\ (1 - \chi(1+p)) & \text{if } \operatorname{cond}(\chi) = p^m,\ \text{prime } p > 2 \text{ and } m > 1. \end{cases}$$

Then $dk^{-1}B_k^\chi$ is integral.

From this Proposition we immediately deduce the following Corollary:

Corollary 7.1.2. *Let k be an integer and χ be a non-trivial primitive Dirichlet character. Let d be as in Proposition* 7.1.1. *Then d is not divisible by any odd prime number not dividing the conductor of χ and k.*

Proof. The possible values of d are given in Proposition 7.1.1. Under our assumptions, we need to prove the statement only when $\mathrm{cond}(\chi) = p^m$, where p is an odd prime and $m > 1$. If $\chi(1+p) = 1$ then χ is trivial on $1 + p\mathbb{Z}/p^m\mathbb{Z}$ and, hence, it factors through $\mathbb{F}_p^*$. Meanwhile, if $\chi(1+p) \neq 1$ then the order of $\chi(1+p)$ is a positive power of p. Given that by hypothesis $p \neq \ell$, the valuation at ℓ of $1 - \chi(1+p)$ is zero. □

Generalized Bernoulli numbers are linked to Eisenstein series. Indeed, in the next theorem we will see that they occur in the constant term of the q-expansion of certain Eisenstein series which are elements of a basis for the Eisenstein subspace of the space of modular forms, for a proof see [Miy06, Section 7].

Let χ_1 and χ_2 be Dirichlet characters and let k be a positive integer such that $\chi_1(-1)\chi_2(-1) = (-1)^k$. Let ρ be the 2-dimensional, semi-simple, odd, Galois representation given by $\rho \cong \chi_1\chi_\ell^{k-1} \oplus \chi_2$, where χ_ℓ is the ℓ-adic cyclotomic character. The L-function associated to the representation ρ is the product of the L-functions associated at the two characters in which the representation split:

$$L(\rho, s) = L(\chi_1, s - k + 1)L(\chi_2, s).$$

Hence, we have that:

$$L(\rho, s) = \prod_p \left(1 - \chi_1(p) \cdot p^{k-1} \cdot p^{-s}\right)^{-1} \cdot \left(1 - \chi_2(p) \cdot p^{-s}\right)^{-1} = \sum_{m=1}^{\infty} c_m m^{-s}$$

where

$$c_m := \sum_{0<d|m} \chi_1(d)\, \chi_2\left(\frac{m}{d}\right)\, d^{k-1}.$$

Under suitable conditions on χ_1 and χ_2, the Dirichlet series that we have just computed is associated with a modular form:

Theorem 7.1.3 ([Ste07, Theorem 5.8])**.** *Let χ_1 and χ_2 be primitive Dirichlet characters and let k be a positive integer such that $\chi_1(-1)\chi_2(-1) = (-1)^k$. Let t be a positive integer. Let $E_k^{\chi_1,\chi_2}(q)$ be the power series:*

$$E_k^{\chi_1,\chi_2}(q) := c_0 + \sum_{m\geq 1} \left(\sum_{0<d|m} \chi_1(d)\chi_2(\frac{m}{d})d^{k-1} \right) q^m \in \mathbb{Q}\left(\chi_1, \chi_2\right)[[q]]$$

where

$$c_0 = \begin{cases} 0 & \text{if } \operatorname{cond}(\chi_2) > 1, \\ -B_k^{\chi_1}/2k & \text{if } \operatorname{cond}(\chi_2) = 1. \end{cases}$$

Then, except when $k = 2$ *and* $\chi_1 = \chi_2 = 1$*, the power series* $E_k^{\chi_1,\chi_2}(q^t)$ *belongs to* $M(t\operatorname{cond}(\chi_1)\cdot\operatorname{cond}(\chi_2), k, \chi_1/\chi_2)_{\mathbb{C}}$.

If $k = 2$ *and* $\chi_1 = \chi_2 = 1$*, let* $t \in \mathbb{Z}_{>1}$*, then* $E_2^{1,1}(q) - tE_2^{1,1}(q^t)$ *is a modular form in* $M(\Gamma_0(t), 2)_{\mathbb{C}}$.

Let us remark that the modular forms $E_k^{\chi_1,\chi_2}$, for a given integer k and characters χ_1 and χ_2, are Eisenstein series and are normalized. Analogously, for all positive integer $t > 1$ the series $E_2^{1,1}(q) - tE_2^{1,1}(q^t)$ is a normalized Eisenstein series.

Theorem 7.1.4 ([Ste07, Theorem 5.9]). *Let* n *and* k *be positive integers. The Eisenstein series of the form* $E_k^{\chi_1,\chi_2}(q^t)$*, with* $\operatorname{cond}(\chi_1)\cdot\operatorname{cond}(\chi_2)t$ *dividing* n*, where* t *is a positive integer, and* $\chi_1/\chi_2 = \epsilon$*, and of the form* $E_2^{1,1}(q) - tE_2^{1,1}(q^t)$ *for all* t *dividing* n*, give a basis for the Eisenstein subspace of* $M(n, k, \epsilon)_{\mathbb{C}}$.

Moreover, the Eisenstein series $E_k^{\chi_1,\chi_2}(q) \in M(\operatorname{cond}(\chi_1)\cdot\operatorname{cond}(\chi_2), k)_{\mathbb{C}}$ and the ones of the form $E_2^{1,1}(q) - tE_2^{1,1}(q^t)$ for $t > 1$ are eigenforms for all Hecke operators.

It is possible to enumerate Eisenstein series in $M(n, k, \epsilon)_{\mathbb{C}}$, for a given Dirichlet character ϵ form $(\mathbb{Z}/n\mathbb{Z})^*$ to $\mathbb{C}^*$, see [Ste07, Algorithm 5.11].

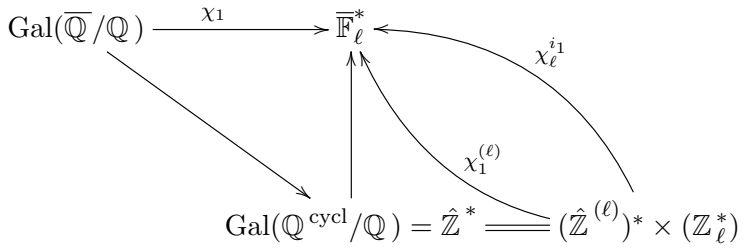
7.2 Checking reducibility

Let n, k be positive integers, let $f\colon \mathbb{T}_\epsilon(n,k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings from the Hecke algebra of level n, weight k and character $\epsilon\colon (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ to an algebraic closure of $\mathbb{F}_\ell$, where ℓ is a prime not dividing n and such that $2 \le k \le \ell+1$. Let $\overline{\epsilon}\colon (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ be the character defined by $a \mapsto f(\langle a\rangle)$ for all $a \in (\mathbb{Z}/n\mathbb{Z})^*$. Let us suppose that ρ_f is absolutely reducible:

$$\rho_f \otimes \overline{\mathbb{F}}_\ell \cong \chi_1 \oplus \chi_2$$

where χ_1 and χ_2 are characters from $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to $\overline{\mathbb{F}}_\ell^*$. We decompose the character χ_1 into its part at ℓ and its part away from ℓ, according to the

following diagram:



where $i_1 \in \mathbb{Z}/(\ell-1)\mathbb{Z}$. So we have $\chi_1 = \chi_1^{(\ell)} \cdot \chi_\ell^{i_1}$ and analogously $\chi_2 = \chi_2^{(\ell)} \cdot \chi_\ell^{i_2}$. The determinant of $\rho_f \otimes \overline{\mathbb{F}}_\ell$ is $\overline{\epsilon}\chi_\ell^{k-1}$, where χ_ℓ is the mod ℓ cyclotomic character. Since $\rho_f \otimes \overline{\mathbb{F}}_\ell$ is isomorphic to $\chi_1 \oplus \chi_2$ it follows that the determinants are equal and so

$$\begin{aligned} &\chi_1^{(\ell)}\chi_2^{(\ell)} = \overline{\epsilon}, \\ &i_1 + i_2 = k - 1 \in \mathbb{Z}/(\ell-1)\mathbb{Z}. \end{aligned}$$

In particular, twisting by the j-th power of the mod ℓ cyclotomic character, where $j := i_1 + 1 - k \in \mathbb{Z}/(\ell-1)\mathbb{Z}$, the representation is isomorphic to:

$$\chi_\ell^j \otimes (\rho_f \otimes \overline{\mathbb{F}}_\ell) \cong \begin{pmatrix} \chi_1^{(\ell)}\chi_\ell^{i_1-i_2} & 0 \\ 0 & \chi_2^{(\ell)} \end{pmatrix}.$$

Hence, if the representation ρ_f is absolutely reducible then its image can be described in terms of the characters $\chi_1^{(\ell)}$, $\chi_2^{(\ell)}$, up to twisting. We will see in Chapter 8 that twisting by the (j)-th power of the mod ℓ cyclotomic character corresponds to apply θ_ℓ^j to the corresponding form. Indeed, the Galois representation associated to $\theta_\ell^j(f)$ satisfies $\rho_{\theta_\ell^j(f)} \cong \chi_1^{(\ell)}\chi_\ell^{i_1-i_2} \oplus \chi_2^{(\ell)}$.

The following proposition describes the structure of a 2-dimensional semi-simple reducible Galois representation under the restriction we are imposing on the level and the weight.

Proposition 7.2.1. *Let n, k be positive integers. Let ℓ be a prime not dividing n and such that $2 \leq k \leq \ell + 1$. Let $f\colon \mathbb{T}_\epsilon(n,k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings from the Hecke algebra of level n, weight k and character $\epsilon\colon (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$. Assume that $\rho_f : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$, the representation attached to f in Corollary 4.0.5, is reducible. Then there exists a pair of Dirichlet characters χ_1 and χ_2 of $(\mathbb{Z}/n\mathbb{Z})^*$ with values in $\overline{\mathbb{F}}_\ell^*$, such that*

$$\rho_f \cong \chi_1\chi_\ell^{k-1} \oplus \chi_2,$$

where χ_ℓ is the mod ℓ cyclotomic character.

Proof. The representation ρ_f is semi-simple and reducible by hypothesis, hence it is decomposable. Let χ_1' and χ_2' be two Dirichlet characters from $(\mathbb{Z}/n\ell\mathbb{Z})^*$ to $\overline{\mathbb{F}}_\ell^*$ such that $\rho_f \cong \chi_1' \oplus \chi_2'$. Then, as in the beginning of this section, using the Chinese remainder Theorem and the hypothesis that ℓ does not divide n, we decompose each character into a character of $(\mathbb{Z}/n\mathbb{Z})^*$ and a power of the mod ℓ cyclotomic character. Let χ_1 and χ_2 be two Dirichlet characters from $(\mathbb{Z}/n\mathbb{Z})^*$ to $\overline{\mathbb{F}}_\ell^*$ such that $\chi_1' = \chi_1 \cdot \chi_\ell^{i_1}$ and $\chi_2' = \chi_2 \cdot \chi_\ell^{i_2}$. Therefore, we have $\rho_f \cong \chi_1 \cdot \chi_\ell^{i_1} \oplus \chi_2 \cdot \chi_\ell^{i_2}$.

The two representations are isomorphic, so they are isomorphic also restricted to the decomposition group at ℓ. If $f(T_\ell) = 0$ then Theorem 6.3.2 states that the representation restricted to the decomposition group is irreducible. Since we are supposing ρ_f to be reducible, then we have $f(T_\ell) \neq 0$. Therefore, we can apply Theorem 6.3.1: the representation ρ_f restricted to the decomposition at ℓ is reducible and of the form

$$\begin{pmatrix} \chi_\ell^{k-1}\lambda(\epsilon(\ell)/f(T_\ell)) & * \\ 0 & \lambda(f(T_\ell)) \end{pmatrix}$$

where $\lambda(f(T_\ell))$ is an unramified character of the decomposition group at ℓ. This means that there exists an unramified quotient line for the representation, hence restricting the representations ρ_f and $\chi_1 \cdot \chi_\ell^{i_1} \oplus \chi_2 \cdot \chi_\ell^{i_2}$ to the inertia at ℓ, we have that $\chi_2 \cdot \chi_\ell^{i_2}$ has to be unramified at ℓ, so we have $i_2 = 0$ and $i_1 = k - 1$. □

Remark 7.2.2. The restriction on the weight, $2 \leq k \leq \ell + 1$, is a crucial hypothesis. In fact, the twist of the representation ρ_f, as in the previous proposition, by the mod ℓ cyclotomic character is isomorphic to the representation $\rho_{\theta_\ell f}$, as already remarked in Chapter 1. If ρ_f is reducible then also $\rho_{\theta_\ell f}$ is reducible, but $\theta_\ell f(T_\ell) = 0$ while $f(T_\ell) \neq 0$ as observed in the proof of the previous proposition.

Theorem 7.2.3. *Let n, k be positive integers, let ℓ be a prime not dividing n and such that $2 \leq k \leq \ell + 1$. Let $f\colon \mathbb{T}_\epsilon(n,k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings. Assume that $\rho_f : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$, the representation attached to f in Corollary 4.0.5, is reducible and does not arise from lower level or weight. Assume that ℓ is odd, $k \neq \ell$ and that we are neither in the case $k = 2$ and $\rho_f \cong 1 \oplus 1$ nor in the case $k = \ell - 1$ and $\rho_f \cong \chi_\ell^{-1} \oplus 1$. Then f is the mod ℓ reduction of an Eisenstein series coming from Theorem 7.1.3.*

Proof. If the representation ρ_f is reducible then there exists a pair of Dirichlet characters χ_1 and χ_2 of $(\mathbb{Z}/n\mathbb{Z})^*$, such that $\rho_f \cong \chi_1\chi_\ell^{k-1} \oplus \chi_2$ by Proposition 7.2.1. Let $\bar{\epsilon} : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ be the character defined by $a \mapsto f(\langle a \rangle)$ for all $a \in (\mathbb{Z}/n\mathbb{Z})^*$.

Since $\rho_f \cong \chi_1\chi_\ell^{k-1} \oplus \chi_2$, the determinants of the two representations have to be equal, then $\chi_1\chi_2 = \bar{\epsilon}$.

The field of definition of the representation $\chi_1\chi_\ell^{k-1} \oplus \chi_2$ is the compositum of the fields of definition of χ_1 and χ_2, since it is the smallest field containing all the traces of the representation. Let us denote this field by $\mathbb{F}$. Let K be a finite extension of $\mathbb{Q}_\ell$ with residue field $\mathbb{F}$ and let us fix an ideal λ in the ring of integers of K such that $(\ell) \supset \lambda$. Let $\widetilde{\chi}_1, \widetilde{\chi}_2$ be λ-adic lifts of χ_1 and χ_2, obtained via a Teichmüller lift, and let χ_ℓ denote the ℓ-adic cyclotomic character which lifts the mod ℓ cyclotomic character by its definition. Therefore, the representation $\widetilde{\rho} \cong \widetilde{\chi}_1\chi_\ell^{k-1} \oplus \widetilde{\chi}_2$ is a lift of the representation ρ_f to characteristic zero. Since the representation ρ_f does not arise from lower level and weight then the conductor of $\widetilde{\rho}$ is n. In fact, if this is not the case, the conductor of $\widetilde{\rho}$ is a divisor of n, so the reduction modulo ℓ of $\widetilde{\rho}$ is isomorphic to $\chi_1\chi_\ell^{k-1} \oplus \chi_2$ and comes from lower level by construction, hence we get a contradiction. Moreover, we can suppose the characters primitive.

The L-function associated to the representation $\widetilde{\rho}$ is the product of the L-functions associated to the two characters in which the representation splits:

$$L(\widetilde{\rho}, s) = \prod_{\substack{p \\ \text{prime}}} L_p(\widetilde{\rho}, s) = \prod_p \left(1 - \widetilde{\chi}_1(p) \cdot p^{k-1} \cdot p^{-s}\right)^{-1} \cdot \left(1 - \widetilde{\chi}_2(p) \cdot p^{-s}\right)^{-1}.$$

Hence, we have that:

$$\begin{aligned}
L(\widetilde{\rho}, s) &= \prod_p \sum_{j \geq 0} \widetilde{\chi}_1(p)^j \, p^{j(k-1)} \, p^{-js} \cdot \prod_p \sum_{i \geq 0} \widetilde{\chi}_2(p)^i p^{-is} = \\
&= \sum_{m=1}^{\infty} \widetilde{\chi}_1(m) \, m^{k-1-s} \cdot \sum_{m'=1}^{\infty} \widetilde{\chi}_2(m') \, m'^{-s} = \\
&= \sum_{m=1}^{\infty} \sum_{0<d|m} \widetilde{\chi}_1(d) \, d^{k-1-s} \, \widetilde{\chi}_2\left(\frac{m}{d}\right) \left(\frac{m}{d}\right)^{-s} = \\
&= \sum_{m=1}^{\infty} \left(\sum_{0<d|m} \widetilde{\chi}_1(d) \, \widetilde{\chi}_2\left(\frac{m}{d}\right) \, d^{k-1} \right) m^{-s} = \sum_{m=1}^{\infty} c_m m^{-s}
\end{aligned}$$

where

$$c_m := \sum_{0<d|m} \widetilde{\chi}_1(d) \, \widetilde{\chi}_2\left(\frac{m}{d}\right) \, d^{k-1}.$$

The expansion of $L(\widetilde{\rho}, s)$ and the expansion of the L-series attached to the Eisenstein series $E_k^{\widetilde{\chi}_1, \widetilde{\chi}_2}$ coincide, except in the case when both characters are trivial and $k = 2$. See [Hid93, Section 5.5] or [DS05, Section 5.9] for a definition of L-series attached to an Eisenstein series.

Let us remark that $\widetilde{\chi}_1(-1)\widetilde{\chi}_2(-1) = (-1)^k$ from the construction of the lift.

The equality of the L-series implies that the Galois representation associated to $E_k^{\widetilde{\chi}_1,\widetilde{\chi}_2}$ in characteristic zero is equivalent to the representation $\widetilde{\rho}$. Hence, if there exists a mod ℓ modular form which is the reduction mod ℓ of $E_k^{\widetilde{\chi}_1,\widetilde{\chi}_2}$, then this form has representation isomorphic to ρ_f. Moreover, since we are supposing that the representation is reducible and does not arise from lower level or weight, then this form has to be equal to f.

Theorem 7.1.3 gives the coefficient c_m of the q-expansion of $E_k^{\widetilde{\chi}_1,\widetilde{\chi}_2}$. For $m \geq 1$ the coefficient c_m is reducible mod ℓ since it is expressed in terms of $\widetilde{\chi}_1$ and $\widetilde{\chi}_2$ and by construction the characters reduce to χ_1 and χ_2. The possible values of c_0 are listed in Theorem 7.1.3.

Let us suppose that $c_0 = 0$, i.e. that χ_1 and χ_2 are both non-trivial, then let us denote by $\overline{E}$ the eigenform obtained by reduction modulo ℓ of the Eisenstein series $E_k^{\widetilde{\chi}_1,\widetilde{\chi}_2}$. If f and $\overline{E}$ are equal then ρ_f is reducible and $\rho_f \cong \chi_1\chi_\ell^{k-1} \oplus \chi_2$.

Let suppose $c_0 \neq 0$, then at least one between χ_1 and χ_2 is trivial. Suppose that χ_1 is trivial, and so $\chi_2 = \overline{\epsilon}$.

If $\overline{\epsilon}$ is non-trivial, then multiplying the Eisenstein series $E_k^{\widetilde{\chi}_1,\widetilde{\chi}_2}$ by $2d$, where d is given in Proposition 7.1.1, we obtain a form whose constant term is an algebraic integer. Therefore, we reduce the series $2dE_k^{\widetilde{\chi}_1,\widetilde{\chi}_2}$ modulo ℓ and we obtain an eigenform $\overline{E}$.

If $\overline{\epsilon}$ is trivial, then the constant term of the Eisenstein series can be expressed using ordinary Bernoulli numbers, as remarked at the beginning of this chapter. The von Staudt Theorem, see [Lan76, Chapter X, Theorem 2.1], states that the denominator of B_k is given by the product over the primes p such that $p-1$ divides k. Since χ_1 and χ_2 are trivial, we are checking if ρ_f is equivalent to $\chi_\ell^{k-1} \oplus 1$. Let us recall that the representation attached to the reduction of $E_k^{1,1}$ for k odd integer $2 < k \leq \ell + 1$ and $k \neq \ell - 1$ is equivalent to $1 \oplus \chi_\ell^{k-1}$, see [EC11, Chapter 14]. Indeed, $c_1(E_k^{1,1}) = 1$ and $E_k^{1,1}$ is an eigenform such that $c_p(E_k^{1,1}) = 1 + p^{k-1}$ for all prime p. If k is different from 2 and $\ell-1$, in order to check if ρ_f is equivalent to one of these representations or not we check if f is equal to the correspondent form. □

In the rest of this chapter we describe an algorithm which checks reducibility for a residual modular Galois representation and we prove that it is correct.

Algorithm 7.2.4 (Reducible representations)**.** Let n, k be positive integers, let ℓ be a prime such that $(n, \ell) = 1$ and $2 \leq k \leq \ell + 1$. Let $f : \mathbb{T}_\epsilon(n, k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings from the Hecke algebra of level n, weight k and character $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$. Let $\overline{\epsilon} : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ be the character defined by $a \mapsto f(\langle a \rangle)$ for all $a \in (\mathbb{Z}/n\mathbb{Z})^*$. Suppose that $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$, the representation attached to f in Corollary 4.0.5, does not arise from lower

level or weight. We this using Algorithm 6.3.7.

Input: n, k, ℓ, $f(T_p)$ for p prime $p \leq B(n,k)$, where $B(n,k)$ is the Sturm bound for modular forms for $\Gamma_0(n)$ and weight k;
Output: if ρ_f is reducible then return χ_1 and χ_2; otherwise return 0.

---

if $f(T_\ell) = 0$ **then**
  return 0
else
  Set q = the smallest odd prime not dividing n and different from ℓ
  List all the possible pairs of primitive Dirichlet characters χ_1, χ_2 from $(\mathbb{Z}/n\mathbb{Z})^*$ to $\overline{\mathbb{F}}_\ell^*$ such that: $\chi_1\chi_2 = \bar{\epsilon}$ and $\mathrm{cond}(\chi_1) \cdot \mathrm{cond}(\chi_2)$ divides n
  for (χ_1, χ_2) in the list **do**
    Preliminary check:
    for p prime, $p \leq B(n,k)$, and $p \neq \ell, q$ **do**
      Compute $c_p = \sum_{0<d|p} \chi_1(d)\chi_2\left(\frac{p}{d}\right) d^{k-1}$
      if $f(T_p) \neq c_p$ **then**
        Change the pair and if no pair is left **return** 0
    For every pair which pass the preliminary check
    Compute $c_p = \sum_{0<d|p} \chi_1(d)\chi_2\left(\frac{p}{d}\right) d^{k-1}$ for $p \in \{\ell, q\}$
    if χ_1 and χ_2 are not trivial **then**
      if $f(T_p) = c_p$ for all p prime, $p \leq B(n,k)$ **then**
        return χ_1 and χ_2;
      else
        Change pair and if no pair is left **return** 0
    else if at least one among χ_1 and χ_2 is trivial **then**
      if one of the following conditions holds: $k = \ell$ or $\ell = 2$ or both characters are trivial and $k = 2$ or both characters are trivial and $k = \ell - 1$ or $kq(q+1) \leq k + \ell + 1$ **then**
        Compute $f(T_p)$ for all p prime with $p \neq q$ and $p \leq B(nq^2, k)$, where $B(nq^2, k)$ is the Sturm bound for modular forms for $\Gamma_0(nq^2)$ and weight k;
        Compute c_p for all p prime with $p \neq q$ and $p \leq B(nq^2, k)$;

        if $f(T_p) = c_p$ for all p prime with $p \neq q$ and $p \leq B(nq^2, k)$; **then**
          return χ_1 and χ_2;
        else
          Change pair and if no pair is left **return** 0
      else
        Compute $f(T_p)$ for all p prime with $p \neq q$ and $p \leq B(n, k+\ell+1)$, where $B(n, k+\ell+1)$ is the Sturm

bound for modular forms for $\Gamma_0(n)$ and weight $k+\ell+1$;

Compute c_p for all p prime with $p \neq q$ and $p \leq B(n, k+\ell+1)$;

if $f(T_p) = c_p$ for all p prime with $p \neq \ell$ and $p \leq B(n, k+\ell+1)$; **then**
    return χ_1 and χ_2;
else
    Change pair and if no pair is left **return** 0

Theorem 7.2.5. *Algorithm* 7.2.4 *is correct.*

Proof. If the representation ρ_f is reducible then by Proposition 7.2.1 there exists a pair of Dirichlet characters χ_1 and χ_2 of $(\mathbb{Z}/n\mathbb{Z})^*$, such that

$$\rho_f \cong \chi_1 \chi_\ell^{k-1} \oplus \chi_2.$$

Let $\overline{\epsilon} : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ be the character defined by $a \mapsto f(\langle a \rangle)$ for all $a \in (\mathbb{Z}/n\mathbb{Z})^*$. Given that ρ_f is isomoprhic to $\chi_1\chi_\ell^{k-1} \oplus \chi_2$, then $\chi_1\chi_2 = \overline{\epsilon}$. Moreover, as remarked in Proposition 7.2.1 we have that $f(T_\ell) \neq 0$, otherwise the representation is not reducible.

As stated in Thoerem 7.2.3, if the representation attached to f in Corollary 4.0.5 is reducible and does not arise from lower level or weight, and we are not in one of the cases excluded by the theorem, then f is the mod ℓ reduction of an Eisenstein series coming from Theorem 7.1.3. In those cases, we check equalities between mod ℓ eigenforms.

If the characters χ_1 and χ_2 are both non-trivial, then let us denote by $\overline{E}$ the eigenform obtained by reduction modulo ℓ of the Eisenstein series in characteristic zero described in the proof of Thoerem 7.2.3. If f and $\overline{E}$ are equal then ρ_f is reducible and $\rho_f \cong \chi_1\chi_\ell^{k-1} \oplus \chi_2$. Using the Sturm bound, more precisely Corollary 6.1.3, it is enough to check the equality $f(T_m) = c_m$, where c_m denotes the m-th coefficient of the q-expansion of $\overline{E}$, for all $m \leq B(n,k)$, where $B(n,k)$ is the Sturm bound relative to $M(\Gamma_0(n), k)_{\overline{\mathbb{F}}_\ell}$.

Assume that at least one between χ_1 and χ_2 is trivial. For simplicity let us suppose that χ_1 is trivial, and so $\chi_2 = \overline{\epsilon}$.

Let q be the smallest odd prime not dividing n and different from ℓ.

In the following cases:
- $k = \ell$;
- $\ell = 2$;
- both characters are trivial and $k = 2$;
- both characters are trivial and $k = \ell - 1$;

– $kq(q+1) \leq k+\ell+1$;
we use the following procedure: twisting by a character.

The inequality $kq(q+1) \leq k+\ell+1$ is obtained comparing the Sturm bound $B(nq^2,k)$ for modular forms for $\Gamma_0(nq^2)$ and weight k with the Sturm bound $B(n,k+\ell+1)$ for modular forms for $\Gamma_0(n)$ and weight $k+\ell+1$. In fact we have

$$\begin{aligned} B(nq^2,k) &= B(n,k)q(q+1), \\ B(n,k+\ell+1) &= B(n,k)+B(n,\ell+1), \end{aligned}$$

then $B(nq^2,k) \leq B(n,k+\ell+1)$ if $kq(q+1) \leq k+\ell+1$.

Let τ be a non-trivial Dirichlet character from $(\mathbb{Z}/q\mathbb{Z})^*$ to $\overline{\mathbb{F}}_\ell^*$ of conductor q. Let $\rho_f \otimes \tau$ be the twist of the representation ρ_f by the character τ. To prove that ρ_f is equivalent to $\chi_1\chi_\ell^{k-1} \oplus \chi_2$ is equivalent to prove that $\rho_f \otimes \tau$ is equivalent to $(\chi_1\chi_\ell^{k-1} \oplus \chi_2) \otimes \tau$. If at least one between χ_1 and χ_2 is trivial, then twisting by τ, we get a couple of non-trivial characters. Therefore, the Eisenstein series $E_k^{\widetilde{\tau}\widetilde{\chi}_1,\widetilde{\tau}\widetilde{\chi}_2}$, where $\widetilde{\tau}$ is a Teichmüller lift of τ, has constant coefficient zero. Let us denote by $\overline{E}$ the eigenform obtained by its reduction modulo ℓ. The representation $\rho_f \otimes \tau$ is modular and it is equivalent to the representation associated to the mod ℓ modular form h whose q-expansion at the cusp ∞ is given by $\sum_m \tau(m)a_m q^m$ while the q-expansion of f is given by $\sum_m a_m q^m$, see [Shi71, Proposition 3.64]. If h and $\overline{E}$ are equal then ρ_f is reducible and $\rho_f \cong \overline{\chi}_1\chi_\ell^{k-1} \oplus \overline{\chi}_2$. Let us remark that $\overline{E}$ belongs to $M(nq^2,k,\epsilon\tau)_{\overline{\mathbb{F}}_\ell}$ since by Theorem 7.1.3 we have $E_k^{\widetilde{\tau}\widetilde{\chi}_1,\widetilde{\tau}\widetilde{\chi}_2}$ is an Eisenstein series in $M(\mathrm{cond}(\bar{\epsilon})\,\mathrm{cond}(\tau)^2,k,\epsilon\tau)_{\mathbb{C}}$, analogously by [Shi71, Proposition 3.64] the form h belongs to $M(nq^2,k,\epsilon\tau)_{\overline{\mathbb{F}}_\ell}$. By Corollary 6.1.3, it is enough check the equality $f(T_m) = c_m$, where c_m denotes the m-th coefficient of the q-expansion of $\overline{E}$, for all m prime, $m \neq q$ and $m \leq B(nq^2,k)$.

If $kq(q+1) > k+\ell+1$ and we are not in the cases listed before, then we follow a different procedure to optimize the computations.

If $\bar{\epsilon}$ is non-trivial, by Thoerem 7.2.3, we obtain a mod ℓ eigenform $\overline{E}$ which has constant coefficient a priori different from zero. Hence, if $\theta_\ell(f)$ and $\theta_\ell\overline{E}$ are equal then $\rho_f \cong \overline{\chi}_1\chi_\ell^{k-1} \oplus \overline{\chi}_2$. This is equivalent to check if $f(T_m) = c_m$ for all m prime, $m \neq \ell$ and $m \leq B(n,k+\ell+1)$.

If $\bar{\epsilon}$ is trivial, then by Thoerem 7.2.3, we need to check equality between f the reduction of $E_k^{1,1}$ for k odd integer $2 < k \leq \ell+1$ and $k \neq \ell-1$ is equivalent to $1 \oplus \chi_\ell^{k-1}$, see [EC11, Chapter 14]: indeed $c_1(E_k^{1,1}) = 1$ and $E_k^{1,1}$ is an eigenform such that $c_p(E_k^{1,1}) = 1+p^{k-1}$ for all prime p. By Sturm's Theorem, this is equivalent to check equality of the coefficients for all primes m different from ℓ and $m \leq B(n,k+\ell+1)$: the constant term of the mod ℓ forms obtained can be different from zero, hence we need to apply the theta operator, and so the weight increases to $k+\ell+1$. □

Remark 7.2.6. Let ℓ be a prime, the Eisenstein series $E_{\ell-1}^{1,1}$ has constant term equal to the ordinary Bernoulli number $B_{\ell-1}$. The von Staudt Theorem implies that ℓ divides the denominator of $B_{\ell-1}$. Hence, multiplying by the denominator of $B_{\ell-1}$ the series $E_{\ell-1}^{1,1}$, we obtain an Eisenstein series whose reduction modulo ℓ, denoted by $\overline{E}$, has $c_1(\overline{E}) = 0$. Then $c_n(\overline{E}) = 0$ for all $n \in \mathbb{Z}_{>0}$. Hence, the q-expansion of $\overline{E}$ is the constant power series $c_0(\overline{E})$, a constant multiple of the Hasse invariant, and it is not normalized. For this reason when $k = \ell - 1$ and both characters are trivial we use the first procedure. If we use the second procedure, then we would check equality between the $\ell - 1$ power of the theta operator applied to f and to the reduction of the Eisenstein series $E_{\ell+1}^{1,1}$ and so it would require to use the Sturm bound $B(n, \ell^2 + \ell)$.

When $k = 2$ and both characters are trivial the Eisenstein series $E_2^{1,1}$ is not a modular form, so we use the first procedure.

Chapter 8

Twist

Twisting a representation by a character is a basic operation in representation theory. In the context of Part II this thesis, twisting, keeping low bounds on the required number of operators, is a fundamental feature of the algorithm we want to outline.

On the one hand, this allows to speed up the computation of the image of a residual modular 2-dimensional Galois representation by using the data coming from lower levels. On the other hand, we can easily fill in the database at higher level using the information obtained at the given level by twisting.

In this chapter we collect several useful result in order to describe the twist of a modular representation with a Dirichlet character: see Proposition 8.2.1, Proposition 8.2.4 and Proposition 8.2.6. We show that it is possible to determine whether the representation restricted to the decomposition group at a ramified prime is irreducible or reducible, and in the latter case we study its splitting. Moreover, we outline an algorithm which returns the local description of the representation at the primes dividing the level and the characteristic, see Algorithm 8.2.9.

In particular, we investigate the conductor of the twist and we obtain results which allows us to use better bounds than the classical given by Shimura in [Shi71, Proposition 3.64]: the bound given by Shimura is an upper bound for the conductor of the twist. In this chapter we also address the problem of twisting by powers of the mod ℓ cyclotomic character.

8.1 Local representation and conductor

Lemma 8.1.1. *Let G be a group and N a normal subgroup. Let V be a 2-dimensional representation of G. Suppose that $V|_N = V_1 \oplus V_2$, i.e. V is decomposable for the action of N, and that the action of N on V_1 and V_2 is given by the restriction of characters χ_1, χ_2 of G such that $\chi_1|_N \neq \chi_2|_N$. Then V decomposes as $V_1 \oplus V_2$ for the action of G.*

Proof. For every $\sigma \in G$ we have the following commutative diagram:

$$\begin{array}{ccc} G \times V & \longrightarrow & G \times V \\ \downarrow & & \downarrow \\ V & \xrightarrow{\sigma} & V \end{array} \qquad \begin{array}{ccc} (g, v) & \longmapsto & (\sigma g \sigma^{-1}, \sigma v) \\ \downarrow & & \downarrow \\ gv & \longmapsto & \sigma g v, \end{array}$$

where in the first row the action of σ on $G \times V$ is given by conjugation on G and on V by the action of G on V. Let n be an element of N, and let v_1 be an element of V_1. From the previous diagram we have:

$$\begin{array}{ccc} (n, v_1) & \longmapsto & (\sigma n \sigma^{-1}, \sigma v_1) \\ \downarrow & & \downarrow \\ nv_1 & \longmapsto & \sigma n v_1. \end{array}$$

The action of N on V_1 is given by the character χ_1, hence $nv_1 = \chi_1(n)v_1$. Let us denote by $(\sigma v_1)_1$, $(\sigma v_1)_2$ the projections of σv_1 on V_1 and V_2. We have $\sigma n v_1 = \sigma(nv_1) = \sigma(\chi_1(n)v_1)$. Therefore, on the one hand we have:

$$\sigma(\chi_1(n)v_1) = \chi_1(n)\sigma v_1 = \chi_1(n)(\sigma v_1)_1 + \chi_1(n)(\sigma v_1)_2,$$

and on the other hand

$$\sigma n v_1 = \sigma n \sigma^{-1} \sigma v_1 = \sigma n \sigma^{-1}((\sigma v_1)_1 + (\sigma v_1)_2) = \chi_1(n)(\sigma v_1)_1 + \chi_2(n)(\sigma v_1)_2.$$

Hence, $(\chi_1(n) - \chi_2(n))(\sigma v_1)_2 = 0$. By hypothesis, for some $n \in N$ we have $\chi_1(n) \neq \chi_2(n)$, then $(\sigma v_1)_2 = 0$. This means that V_1 and V_2 are stable under the action of G. □

Remark 8.1.2. Let us underline that the hypotheses about the characters χ_1 and χ_2 in the previous lemma are crucial. If these characters are characters of N and not of G, then it is not possible to have the same conclusion of the lemma. For example, take G to be $\mathfrak{S}_3$, the symmetric group on 3 elements, and its representation to $\mathrm{GL}_2(\mathbb{C})$ given by:

$$\begin{aligned} &\rho : \mathfrak{S}_3 \to \mathrm{GL}_2(\mathbb{C}) \\ &\rho(\tau) = \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}, \ \rho(\epsilon) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \end{aligned}$$

where $\mathfrak{S}_3 \cong C_3 \rtimes C_2 \cong \langle \tau \rangle \rtimes \langle \epsilon \rangle$, and ω is a fixed third root of unity. The subgroup C_3 is normal in $\mathfrak{S}_3$ and the representation ρ restricted to C_3 is decomposable meanwhile ρ is not reducible. In fact, the characters which give the action of C_3 on the representation are not characters of $\mathfrak{S}_3$.

Proposition 8.1.3. *Let n and k be two positive integers, let ℓ be a prime such that $(n,\ell)=1$ and $2\leq k\leq \ell+1$, and let $\epsilon:(\mathbb{Z}/n\mathbb{Z})^*\to\mathbb{C}^*$ be a character. Let $f:\mathbb{T}_\epsilon(n,k)\to\overline{\mathbb{F}}_\ell$ be a morphism of rings. Let $\rho_f:G_{\mathbb{Q}}\to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the representation attached to f in Corollary 4.0.5. Assume that ρ_f is irreducible and it does not arise from lower level. Let p be a prime dividing n such that $f(T_p)\neq 0$. Then $\rho_f|_{G_p}$ is decomposable if and only if $\rho_f|_{I_p}$ is decomposable.*

Proof. If $\rho_f|_{G_p}$ is decomposable then $\rho_f|_{I_p}$ is decomposable.

Let us assume that $\rho_f|_{I_p}$ is decomposable. By hypothesis $f(T_p)\neq 0$, hence the representation is ramified at p, since it does not arise from lower level, and by Theorem 6.3.3 the representation restricted to G_p, the decomposition at p, is reducible. Moreover, there exists a stable line $D\subset V$ for the action of G_p, such that the inertia group at p acts trivially on V/D. This means that the two characters which describe the action of G_p on the line and its quotient are distinct once restricted to the inertia. The inertia I_p is normal in G_p, so we apply Lemma 8.1.1. Therefore, if $\rho_f|_{I_p}$ is decomposable then $\rho_f|_{G_p}$ is decomposable. □

Remark 8.1.4. If the Galois representation ρ_f as in the previous proposition is reducible then it is decomposable since it is semi-simple. The representation restricted to the decomposition group at p is reducible but the two characters which describe the action of G_p on the line and its quotient are not a priori distinct once restricted to the inertia.

Proposition 8.1.5. *Let n and k be two positive integers, let ℓ be a prime such that $(n,\ell)=1$ and $2\leq k\leq \ell+1$, and let $\epsilon:(\mathbb{Z}/n\mathbb{Z})^*\to\mathbb{C}^*$ be a character. Let $f:\mathbb{T}_\epsilon(n,k)\to\overline{\mathbb{F}}_\ell$ be a morphism of rings and let $\rho_f:G_{\mathbb{Q}}\to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the representation attached to f in Corollary 4.0.5. Let $\overline{\epsilon}:(\mathbb{Z}/n\mathbb{Z})^*\to\overline{\mathbb{F}}_\ell^*$ be the character defined by $\overline{\epsilon}(a)=f(\langle a\rangle)$ for all $a\in(\mathbb{Z}/n\mathbb{Z})^*$.*

Assume that ρ_f is irreducible and it does not arise from lower level. Let p be a prime dividing n, such that $f(T_p)\neq 0$. Then:
(a) $\rho_f|_{I_p}$ is decomposable if and only if $\mathrm{N}_p(\rho_f)=\mathrm{N}_p(\overline{\epsilon})$;
(b) $\rho_f|_{I_p}$ is indecomposable if and only if $\mathrm{N}_p(\rho_f)=1+\mathrm{N}_p(\overline{\epsilon})$.

Proof. The formula $(*)$ for the Artin conductor of a representation given in Chapter 4 can be re-written in the following way:

$$\mathrm{N}_p(\rho_f)=\sum_{i\geq 0}\frac{1}{[G_{0,p}:G_{i,p}]}\dim(V/V^{G_{i,p}})=\dim(V/V^{I_p})+b(V),$$

where V is a 2-dimensional $\overline{\mathbb{F}}_\ell$-vector space underlying the representation and

$$b(V)=\sum_{i\geq 1}\frac{1}{[G_{0,p}:G_{i,p}]}\dim(V/V^{G_{i,p}})$$

is called the wild part of the conductor. By hypothesis $f(T_p) \neq 0$, then the representation restricted to the decomposition group at p is reducible. Let ϵ_1 and ϵ_2 be the characters of G_p with values in $\overline{\mathbb{F}}_\ell^*$ which describe the action of G_p respectively on D, stable line in V for the action of G_p, and on V/D, unramified quotient for the action of I_p. The character ϵ_2 is an unramified character of G_p by Theorem 6.3.3. Hence,after conjugation, we have

$$\rho_f|_{G_p} \cong \begin{pmatrix} \epsilon_1\chi_\ell^{k-1} & * \\ 0 & \epsilon_2 \end{pmatrix}, \quad \rho_f|_{I_p} \cong \begin{pmatrix} \epsilon_1|_{I_p} & * \\ 0 & 1 \end{pmatrix},$$

where χ_ℓ is the mod ℓ cyclotomic character and $*$ belongs to $\overline{\mathbb{F}}_\ell$.

Let us first suppose that $\rho_f|_{I_p}$ is indecomposable. Then V^{I_p} is either $\{0\}$ if ϵ_1 is ramified, or $\overline{\mathbb{F}}_\ell \cdot \binom{1}{0}$ if ϵ_1 is unramified. The wild part of the conductor is equal to the wild part of the conductor of ϵ_1. Hence,

$$\mathrm{N}_p(\rho_f) = \begin{cases} 1 = 1 + \mathrm{N}_p(\epsilon_1) & \text{if } \epsilon_1 \text{ is unramified,} \\ 2 + b(\epsilon_1) = 1 + \mathrm{N}_p(\epsilon_1) & \text{if } \epsilon_1 \text{ is ramified.} \end{cases}$$

The determinant of the representation is given by $\det(\rho_f) = \bar{\epsilon}\chi_\ell^{k-1}$. Since p and ℓ are co-prime, then $\det(\rho_f)|_{I_p} = \bar{\epsilon}|_{I_p}$. This implies that $\epsilon_1|_{I_p} = \bar{\epsilon}|_{I_p}$, so $\mathrm{N}_p(\epsilon_1) = \mathrm{N}_p(\bar{\epsilon})$. Therefore, if $\rho_f|_{I_p}$ is indecomposable then $\mathrm{N}_p(\rho_f) = 1 + \mathrm{N}_p(\bar{\epsilon})$.

Let us suppose that $\rho_f|_{I_p}$ is decomposable. Then V^{I_p} is either $\overline{\mathbb{F}}_\ell \cdot \binom{0}{1}$ if ϵ_1 is ramified, or 2-dimensional if ϵ_1 is unramified. Therefore,

$$\mathrm{N}_p(\rho_f) = \begin{cases} 0 = \mathrm{N}_p(\epsilon_1) & \text{if } \epsilon_1 \text{ is unramified,} \\ 1 + b(\epsilon_1) = \mathrm{N}_p(\epsilon_1) & \text{if } \epsilon_1 \text{ is ramified.} \end{cases}$$

Given that $\epsilon_1|_{I_p} = \bar{\epsilon}|_{I_p}$, we have $\mathrm{N}_p(\rho_f) = \mathrm{N}_p(\bar{\epsilon})$.

□

Remark 8.1.6. Let n and k be two positive integers, let ℓ be a prime such that $(n, \ell) = 1$ and $2 \leq k \leq \ell + 1$, and let $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character. Let $f : \mathbb{T}_\epsilon(n, k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings and let $\rho_f : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the representation attached to f in Corollary 4.0.5. Assume that ρ_f is irreducible. Let p be a prime dividing n, such that $f(T_p) \neq 0$. Proposition 8.1.5 gives a criterion to decide if $\rho_f|_{I_p}$ is decomposable or not. By [Dia97, Proposition 2.2], if $\rho_f|_{I_p}$ is indecomposable then the image of inertia at p is of order divisible by ℓ and so the image cannot be exceptional.

8.2 Twisting by Dirichlet characters

Let n be a positive integer. Suppose that it is given a factorization of n as $\prod_{i=0}^m p_i^{e_i}$ where $p_0 < p_1 < \ldots < p_m$ are primes and $e_i \in \mathbb{Z}_{>0}$. Each $(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^*$ is

a cyclic group, unless $p_0 = 2$ and $e_0 \geq 3$ in which case $(\mathbb{Z}/2^{e_0}\mathbb{Z})^* \cong C_{0,0} \times C_{0,1}$ where $C_{0,0}$ is a cyclic group of order 2, for example $C_{0,0} \cong \langle -1 \rangle$, and $C_{0,1}$ is a cyclic group of order 2^{e_0-2}, for example $C_{0,1} \cong \langle 5 \rangle$. Using [Ste07, Algorithm 4.4], we determine the minimal generators for each $(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^*$ and thorough the Chinese reminder Theorem we lift each generator to an element g_i in $(\mathbb{Z}/n\mathbb{Z})^*$, for the case $p_0 = 2$ and $e_0 \geq 3$ we have two elements $g_{0,0}$ and $g_{0,1}$ instead of a single g_0. Any Dirichlet character χ from $(\mathbb{Z}/n\mathbb{Z})^*$ to $\overline{\mathbb{F}}_\ell^*$ is then represented giving a list $[\chi(g_0), \chi(g_1) \ldots, \chi(g_m)]$ of the images of the minimal generators g_i, with $i = 0, \ldots, m$, where g_0 is replaced by the couple $g_{0,0}$, $g_{0,1}$ in the case $p_0 = 2$ and $e_0 \geq 3$. In particular any Dirichlet character can be decomposed into local characters, one for each prime divisor of n, using [Ste07, Algorithm 4.16].

This means that, with no loss of generality, we can reduce ourselves to study twists of modular Galois representations with Dirichlet characters with prime power conductor. In fact, the general case is deduced from this combining the local characters in which the character decomposes.

Let p be a prime and let $\chi : (\mathbb{Z}/p^i\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$, for $i > 0$, be a non-trivial character. By definition χ is ramified only at p and its conductor at p is positive. The Galois representation $\rho_f \otimes \chi$ is a 2-dimensional odd continuous representation: let c be a complex conjugation then

$$\det(\rho_f \otimes \chi)(c) = \det(\rho_f(c))\chi^2(-1) = -1.$$

Moreover, it is modular and if it is irreducible then by Khare-Wintenberger Theorem there exists a mod ℓ modular form g of level $\mathrm{N}(\rho_f \otimes \chi)$ and weight k such that $\rho_g \cong \rho_f \otimes \chi$. If the weight is ℓ then there could exist two such forms, this follows from the fact that we are restricting ourselves to weight between 2 and $\ell+1$ and that there exist two different embeddings from weight 1 to weight ℓ, see [Edi06, Section 4.1] and [Wie05, Section 4.5].

It is natural to wonder about the conductor of $\rho_f \otimes \chi$. The next propositions settle the problem.

Proposition 8.2.1. *Let n and k be two positive integers, let ℓ be a prime such that $(n, \ell) = 1$ and $2 \leq k \leq \ell+1$, and let $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character. Let $f : \mathbb{T}_\epsilon(n, k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings and let $\rho_f : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the representation attached to f in Corollary 4.0.5. Suppose that ρ_f does not arise from lower level and let p be a prime not dividing $n\ell$. Let $\chi : (\mathbb{Z}/p^i\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$, for $i > 0$, be a non-trivial character. Then*

$$\mathrm{N}_p(\rho_f \otimes \chi) = 2\mathrm{N}_p(\chi).$$

Proof. The representation ρ_f is unramified at p since p does not divide $n\ell$. Therefore we have that

$$(\rho_f \otimes \chi)|_{I_p} \cong \begin{pmatrix} \chi|_{I_p} & 0 \\ 0 & \chi|_{I_p} \end{pmatrix},$$

since χ is non-trivial and ramified at p. This means that $\mathrm{N}_p(\rho_f \otimes \chi) = 2\mathrm{N}_p(\chi)$. □

Remark 8.2.2. In the hypotheses of Proposition 8.2.1 if in addition ρ_f is irreducible then let g be a mod ℓ modular form of level $\mathrm{N}(\rho_f \otimes \chi)$ and minimal weight such that $\rho_g \cong \rho_f \otimes \chi$. Since χ is not ramified at prime where ρ_f is ramified, then it follows that $g(T_q) = \chi(q) f(T_q)$ for all primes q. If the representation is reducible, the analogous result holds true, see [Shi71, Proposition 3.64]. Moreover, $\rho_f \otimes \chi$ restricted to G_p does not admit any stable line with unramified quotient.

Remark 8.2.3. If we twist by characters which ramifies at the primes where the representation is unramified, then the conductor increases. On the other hand, twisting by characters ramified at primes where the representation is ramified allows us to detect representations which arises as twist of others of lower conductor. In order to fill in the database at levels multiple of the given one we will, instead, twist by characters ramified also at primes where the representation is unramified.

Proposition 8.2.4. *Let n and k be two positive integers, let ℓ be a prime such that $(n, \ell) = 1$ and $2 \leq k \leq \ell+1$, and let $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character. Let $f : \mathbb{T}_\epsilon(n, k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings and let $\rho_f : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the representation attached to f in Corollary 4.0.5. Let $\overline{\epsilon} : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ be the character defined by $\overline{\epsilon}(a) = f(\langle a \rangle)$ for all $a \in (\mathbb{Z}/n\mathbb{Z})^*$.*

Assume that ρ_f is irreducible and it does not arise from lower level. Let p be a prime dividing n and suppose that $f(T_p) \neq 0$.

Let $\chi : (\mathbb{Z}/p^i\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$, for $i > 0$, be a non-trivial character. Then

$$\mathrm{N}_p(\rho_f \otimes \chi) = \mathrm{N}_p(\chi\overline{\epsilon}) + \mathrm{N}_p(\chi).$$

Proof. Let us remark that, being twist of each other, ρ_f and $\rho_f \otimes \chi$ have the same projective image. Hence, also restricted to the inertia they have the same projective representation. From this, it is clear that $\rho_f|_{I_p}$ is decomposable if and only if $(\rho_f \otimes \chi)|_{I_p}$ is decomposable.

Suppose that $\rho_f|_{I_p}$ is decomposable. Proposition 8.1.3 implies that $\rho_f|_{G_p}$ is decomposable. By Theorem 6.3.3, since $f(T_p) \neq 0$, the representation restricted to the decomposition group at p is equivalent to $\epsilon_1 \chi_\ell^{k-1} \oplus \epsilon_2$, where ϵ_1 and ϵ_2 are characters of G_p, with ϵ_2 unramified. The equality of the determinants restricted to I_p leads to $\epsilon_1|_{I_p} = \overline{\epsilon}|_{I_p}$. Therefore, $\rho_f|_{I_p} = \overline{\epsilon} \oplus 1$ and so

$$(\rho_f \otimes \chi)|_{I_p} \cong \rho_f|_{I_p} \otimes \chi|_{I_p} \cong \begin{pmatrix} (\chi\overline{\epsilon})|_{I_p} & 0 \\ 0 & \chi|_{I_p} \end{pmatrix}.$$

This implies that $\mathrm{N}_p(\rho_f \otimes \chi) = \mathrm{N}_p(\chi\overline{\epsilon}) + \mathrm{N}_p(\chi)$.

If $\rho_f|_{I_p}$ is indecomposable, then

$$(\rho_f \otimes \chi)|_{I_p} \cong \begin{pmatrix} (\chi\overline{\epsilon})|_{I_p} & \chi|_{I_p} \cdot * \\ 0 & \chi|_{I_p} \end{pmatrix},$$

with $* \neq 0$. Hence, we have that

$$\mathrm{N}_p(\rho_f \otimes \chi) = \begin{cases} 1 + b(\chi) & \text{if } \chi\overline{\epsilon} \text{ is unramified,} \\ 2 + b(\chi\overline{\epsilon}) + b(\chi) & \text{if } \chi\overline{\epsilon} \text{ is ramified.} \end{cases}$$

Given that $\mathrm{N}_p(\chi) = 1 + b(\chi)$, because χ is non-trivial and ramified at p, it follows that $\mathrm{N}_p(\rho_f \otimes \chi) = \mathrm{N}_p(\chi\overline{\epsilon}) + \mathrm{N}_p(\chi)$. □

Proposition 8.2.5. *Let n and k be two positive integers, let ℓ be a prime such that $(n, \ell) = 1$ and $2 \leq k \leq \ell+1$, and let $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character. Let $f : \mathbb{T}_\epsilon(n, k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings and let $\rho_f : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the representation attached to f in Corollary 4.0.5.*

Suppose that ρ_f is irreducible and that $\mathrm{N}(\rho_f) = n$. Let p be a prime dividing n and suppose that $f(T_p) \neq 0$. Let χ from $(\mathbb{Z}/p^i\mathbb{Z})^*$ to $\overline{\mathbb{F}}_\ell^*$, with $i > 0$, be a non-trivial character. Then

(a) if $\rho_f|_{I_p}$ is decomposable then the representation $\rho_f \otimes \chi$ restricted to G_p, the decomposition group at p, admits a stable line with unramified quotient if and only if $\mathrm{N}_p(\rho_f \otimes \chi) = \mathrm{N}_p(\rho_f)$;

(b) if $\rho_f|_{I_p}$ is indecomposable then the representation $\rho_f \otimes \chi$ restricted to G_p does not admit any stable line with unramified quotient.

Proof. Since $f(T_p) \neq 0$, we have that $\mathrm{N}_p(\rho_f \otimes \chi) = \mathrm{N}_p(\chi\overline{\epsilon}) + \mathrm{N}_p(\chi)$ by Proposition 8.2.4. Let us first suppose that $\rho_f|_{I_p}$ is decomposable. By Proposition 8.1.5 this is equivalent to $\mathrm{N}_p(\rho_f) = \mathrm{N}_p(\overline{\epsilon})$. Theorem 6.3.3 states that, since $f(T_p) \neq 0$, the representation ρ_f restricted to the decomposition group at p is, after conjugation, of the form:

$$\rho_f|_{G_p} \cong \begin{pmatrix} \chi_\ell^{k-1}\epsilon_1 & 0 \\ 0 & \epsilon_2 \end{pmatrix},$$

where ϵ_1 and ϵ_2 are the characters of G_p with values in $\overline{\mathbb{F}}_\ell^*$, with ϵ_2 unramified. Hence, after conjugation, we have:

$$(\rho_f \otimes \chi)|_{G_p} \cong \begin{pmatrix} \chi_\ell^{k-1}\epsilon_1\chi & 0 \\ 0 & \epsilon_2\chi \end{pmatrix}.$$

If $\epsilon_1\chi$ and $\epsilon_2\chi$ are both ramified at p then $\rho_f \otimes \chi$ restricted to G_p does not admit any stable line with unramified quotient. If at least one of the two characters is unramified then such a line exists. Since ϵ_2 is unramified at p and χ is ramified, then $\epsilon_2\chi$ is ramified, hence, there exists a stable line with

unramified quotient if and only if $\epsilon_1\chi$ is unramified at p. We have already shown, in the proof of Proposition 8.2.4, that $\epsilon_1|_{I_p} = \overline{\epsilon}|_{I_p}$. This implies that $\mathrm{N}_p(\chi\epsilon_1) = \mathrm{N}_p(\chi\overline{\epsilon}) = 0$, hence that $\mathrm{N}_p(\rho_f \otimes \chi) = \mathrm{N}_p(\chi)$. Since $\chi\overline{\epsilon}$ is unramified then $\mathrm{N}_p(\overline{\epsilon}) = \mathrm{N}_p(\chi)$. Therefore $\mathrm{N}_p(\rho_f \otimes \chi) = \mathrm{N}_p(\rho_f)$.

Moreover, the trace of the representation $\rho_f \otimes \chi$ at p is equal to the scalar which gives the action of Frob_p on the unramified line, hence, by Theorem 6.3.3, it is equal to $\chi_\ell^{k-1}(\epsilon_1\chi)(\mathrm{Frob}_p)$.

Let us suppose that $\rho_f|_{I_p}$ is indecomposable. In [Dia97, Proposition 2.2] it is stated that the representation $\rho_f|_{G_p}$ after twisting is either of the form $\left(\begin{smallmatrix} 1 & \phi \\ 0 & 1 \end{smallmatrix}\right)$ if $p \equiv 1 \bmod \ell$, where ϕ is an additive ramified character of G_p, or is equivalent to $\left(\begin{smallmatrix} \chi_\ell & * \\ 0 & 1 \end{smallmatrix}\right)$ if $p \not\equiv 1 \bmod \ell$, where $*$ is non-trivial. Being twist of each other, ρ_f and $\rho_f \otimes \chi$ restricted to the inertia at p have the same projective image. There exists a stable line with unramified quotient for the action of the projective image of $\rho_f|_{G_p}$ on $\mathbb{P}^1(\overline{\mathbb{F}}_\ell)$ since $f(T_p) \neq 0$ and the representation ρ_f is ramified at p. If we twist such line by a character ramified at p, since the extension is non-trivial in the indecomposable case, then the representation $\rho_f \otimes \chi$ restricted to G_p does not admit any stable line with unramified quotient. □

Proposition 8.2.6. *Let n and k be two positive integers, let ℓ be a prime such that $(n, \ell) = 1$ and $2 \leq k \leq \ell+1$, and let $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character. Let $f : \mathbb{T}_\epsilon(n, k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings and let $\rho_f : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the representation attached to f in Corollary 4.0.5. Let $\overline{\epsilon} : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ be the character defined by $\overline{\epsilon}(a) = f(\langle a \rangle)$ for all $a \in (\mathbb{Z}/n\mathbb{Z})^*$.*

Suppose that ρ_f is irreducible and that $\mathrm{N}(\rho_f) = n$. Let p be a prime dividing n and suppose that $f(T_p) = 0$. Then:

(a) if $\rho_f|_{G_p}$ is reducible then there exists a mod ℓ modular form g of weight k and level at most np and a non-trivial character $\chi : (\mathbb{Z}/p^i\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ with $i > 0$ such that $g(T_p) \neq 0$ and $\rho_g \cong \rho_f \otimes \chi$;

(b) if $\rho_f|_{G_p}$ is irreducible then for any non-trivial character $\chi : (\mathbb{Z}/p^i\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ with $i > 0$ the representation $\rho_f \otimes \chi$ restricted to G_p does not admit any stable line with unramified quotient.

Proof. By hypothesis $f(T_p) = 0$, hence the representation ρ_f restricted to the decomposition group at p does not admit any stable line with unramified quotient. The representation, restricted to the decomposition group at p, can be either reducible or irreducible.

In the irreducible case, since for any non-trivial character $\chi : (\mathbb{Z}/p^i\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ with $i > 0$ the representations $\rho_f \otimes \chi$ and ρ_f have the same projective image, then there exists no stable line with unramified quotient for $\rho_f \otimes \chi$.

Let us assume that ρ_f restricted to G_p is reducible and indecomposable. Then, by Theorem 6.3.3, the representation is of the form:

$$\rho_f|_{G_p} \cong \begin{pmatrix} \epsilon_1 \chi_\ell^{k-1} & * \\ 0 & \epsilon_2 \end{pmatrix}$$

where ϵ_2 is a ramified character of G_p with values in $\overline{\mathbb{F}}_\ell^*$ and $* \in \overline{\mathbb{F}}_\ell^*$. If ϵ_1 is unramified, then $\rho_f|_{I_p} \cong \left(\begin{smallmatrix} 1 & * \\ 0 & \epsilon_2|_{I_p} \end{smallmatrix}\right)$. Hence, $V^{I_p} = \overline{\mathbb{F}}_\ell \cdot \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$. Meanwhile, if ϵ_1 is ramified, $V^{I_p} = \{0\}$. Therefore, the conductor at p of ρ_f is given by

$$\mathrm{N}_p(\rho_f) = \begin{cases} 1 + b(\epsilon_2) = \mathrm{N}_p(\epsilon_2) & \text{if } \epsilon_1 \text{ is unramified,} \\ 2 + b(\epsilon_1) + b(\epsilon_2) = \mathrm{N}_p(\epsilon_1) + \mathrm{N}_p(\epsilon_2) & \text{if } \epsilon_1 \text{ is ramified.} \end{cases}$$

Hence, we have that $\mathrm{N}_p(\rho_f) = \mathrm{N}_p(\epsilon_1) + \mathrm{N}_p(\epsilon_2)$.

A stable line with unramified quotient for a twist of ρ_f exists if and only if the twist is given by the inverse of ϵ_2. The conductor at p of $\rho_f \otimes \epsilon_2^{-1}$ is given by:

$$\mathrm{N}_p(\rho_f \otimes \epsilon_2^{-1}) = \mathrm{N}_p \begin{pmatrix} \epsilon_1 \epsilon_2^{-1} \chi_\ell^{k-1} & * \\ 0 & 1 \end{pmatrix} = \begin{cases} 1 & \text{if } \epsilon_1 \epsilon_2^{-1} \text{ is unramified,} \\ 1 + \mathrm{N}_p(\epsilon_1 \epsilon_2^{-1}) & \text{if } \epsilon_1 \epsilon_2^{-1} \text{ is ramified,} \end{cases}$$

so $\mathrm{N}_p(\rho_f \otimes \epsilon_2^{-1}) = 1 + \mathrm{N}_p(\epsilon_1 \epsilon_2^{-1})$.

Let us remark that the conductor of $\epsilon_1 \epsilon_2^{-1}$ is less or equal to the maximum between $\mathrm{cond}(\epsilon_1)$ and $\mathrm{cond}(\epsilon_2)$. Therefore, if ϵ_1 is ramified, then $\mathrm{N}_p(\rho_f \otimes \epsilon_2^{-1})$ is less or equal to $\mathrm{N}_p(\rho_f)$: this follows since $\mathrm{N}_p(\epsilon_1 \epsilon_2^{-1}) \leq \max\{\mathrm{N}_p(\epsilon_1), \mathrm{N}_p(\epsilon_2)\}$ and $\mathrm{N}_p(\epsilon_1)$, $\mathrm{N}_p(\epsilon_2)$ are both positive since both characters are ramified. If ϵ_1 is unramified, then $\mathrm{N}_p(\rho_f \otimes \epsilon_2^{-1}) = \mathrm{N}_p(\rho_f) + 1$ from the previous computations. This means that there exists a mod ℓ modular form g of weight k and level at most np such that $\rho_g \cong \rho_f \otimes \epsilon_2^{-1}$ and $g(T_p) \neq 0$ since $\rho_f \otimes \epsilon_2^{-1}$ admits a stable line with unramified quotient.

If ρ_f restricted to G_p is reducible and decomposable we obtain the same result. □

Remark 8.2.7. Proposition 8.2.6 gives us a criterion to decide whether an irreducible representation ρ_f restricted to the decomposition at p, prime dividing $\mathrm{N}(\rho)$, with $\mathrm{Trace}(\rho_f(\mathrm{Frob}_p)) = 0$, is irreducible or not. Let us remark that if $\rho_f|_{G_p}$ is reducible then the splitting of $\rho_f|_{G_p}$ is also determined once computed the mod ℓ modular form g of weight k and level $\mathrm{N}(\rho_f \otimes \chi)$ such that $g(T_p) \neq 0$ and $\rho_g \cong \rho_f \otimes \chi$. Indeed, by Proposition 8.1.5 the projective image does not change.

The proof of Proposition 8.2.6 implies that if $\mathrm{N}_p(\rho_f \otimes \chi) \geq \mathrm{N}_p(\rho_f)$ and $\rho_f \otimes \chi$ admits a stable line with unramified quotient, then χ is the inverse

of the component at p of the character $\overline{\epsilon}$: this case can occur only if ϵ_1 is unramified, hence, by the equality of the determinants $\epsilon_2|_{I_p} = \overline{\epsilon}|_{I_p}$ and ϵ_2 is ramified since $f(T_\ell) = 0$.

Let n and k be two positive integers, let ℓ be a prime such that $(n, \ell) = 1$ and $2 \leq k \leq \ell + 1$, and let $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character. Let $f : \mathbb{T}_\epsilon(n, k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings and let $\rho_f : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the representation attached to f in Corollary 4.0.5.

Suppose that ρ_f is irreducible and that it does not come from lower level or weight. Then for any Dirichlet character χ there exists a mod ℓ modular form g of level $\mathrm{N}(\rho_f \otimes \chi)$ and weight k such that $\rho_g \cong \rho_f \otimes \chi$. As we have already remarked, the form g does not need to be unique since we are restricting ourselves to weight between 2 and ℓ+1.

For any unramified prime q for ρ_f we have that $g(T_q) = \chi(q)f(T_q)$. Analogously, if r is a prime dividing $\mathrm{N}(\rho_f)$ and the component at r of χ is trivial we have that $g(T_r) = f(T_r)$, since the $\rho_f|_{G_r}$ and $\rho_f \otimes \chi|_{G_r}$ are equivalent in this case.

Let p be a prime dividing $\mathrm{N}(\rho_f)$, and suppose that the component at p of χ is non trivial.

If $f(T_p) \neq 0$ then Proposition 8.1.5 give us a criterion to decide about the splitting of $\rho_f|_{G_p}$. Proposition 8.2.5 states that if $\rho_f|_{I_p}$ is decomposable and the twist occur at level n then $g(T_p) \neq 0$, since there exists a stable line with unramified quotient for $\rho_f \otimes \chi$. It also follows that if $\rho_f|_{I_p}$ is indecomposable then $g(T_p) = 0$.

If $f(T_p) = 0$ then Proposition 8.2.6 give us a criterion to decide if $\rho_f|_{G_p}$ is irreducible or not. If $\rho_f|_{G_p}$ is irreducible then $g(T_p) = 0$. Meanwhile, if $\rho_f|_{G_p}$ is reducible then the form g of level $\mathrm{N}(\rho_f \otimes \chi)$ is such that $g(T_p) \neq 0$. Proposition 8.1.5 applied to g give us the splitting of $\rho_f|_{G_p}$.

The previous propositions and the discussion carried on in this chapter motivate the following definition:

Definition 8.2.8. Let n and k be two positive integers, let ℓ be a prime such that $(n, \ell) = 1$ and $2 \leq k \leq \ell + 1$, and let $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character. Let $f : \mathbb{T}_\epsilon(n, k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings and let $\rho_f : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the representation attached to f in Corollary 4.0.5. We say that f is *minimal up to twisting* if for any Dirichlet character $\chi : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$, and for any prime p dividing n

$$\mathrm{N}_p(\rho_f) \leq \mathrm{N}_p(\rho_f \otimes \chi).$$

The definition of minimality up to twisting is equivalent to require that ρ_f is not isomorphic to a twist of a representation of lower conductor. Can

we determine when a representation is twist of a representation of lower conductor?

The following algorithms answer to this question.

Algorithm 8.2.9 (Local description at the prime p dividing the level)**.** Let n and k be positive integers. Let ℓ be a prime not dividing n such that $2 \leq k \leq \ell + 1$. Let $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character. Let $f : \mathbb{T}_\epsilon(n,k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings and let $\rho_f : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the representation attached to f in Corollary 4.0.5.

Assume that Algorithm 6.3.7 and Algorithm 7.2.4 certify that ρ_f is irreducible and $\mathrm{N}(\rho_f) = n$. Let p be a prime dividing n. Let $\overline{\epsilon} : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ be the character defined by $\overline{\epsilon}(a) = f(\langle a \rangle)$ for all $a \in (\mathbb{Z}/n\mathbb{Z})^*$.

Input: n, p, k, ℓ, $\overline{\epsilon}$, $f(T_q)$ for q prime $q \leq B(n,k)$ where $B(n,k)$ is the Sturm bound for cusp forms for $\Gamma_0(n)$ and weight k;
Output: return the list [is_reducible, is_decomposable, v] where
- is_reducible=true if $\rho_f|_{G_p}$ is reducible, otherwise it is set to false;
- is_decomposable=true if $\rho_f|_{G_p}$ is decomposable, otherwise it is set to false;
- v is a list and it is non-empty if and only if $f(T_p) = 0$ and $\rho_f|_{G_p}$ is reducible in which case $v = [g, \chi]$ where g and χ are the form and the character as in Proposition 8.2.6.

Set $v \leftarrow []$; is_reducible=false; is_decomposable=false;
if $f(T_p) \neq 0$ **then**
    Set is_reducible=true
    if $\mathrm{N}_p(n) \neq \mathrm{N}_p(\overline{\epsilon}) + 1$ **then**
        Set is_decomposable=true
else if $f(T_p) = 0$ **then**
    for χ non-trivial Dirichlet character from $(\mathbb{Z}/p^i\mathbb{Z})^*$ to $\overline{\mathbb{F}}_\ell^*$ with $i > 0$ and $i \leq \mathrm{N}_p(n)$ **do**
        Set $j \leftarrow 0$
        while $j \leq \mathrm{N}_p(n)$ **do**
            for $g \in S(np^{-j}, k)_{\overline{\mathbb{F}}_\ell}$ such that ρ_g is irreducible and $\mathrm{N}(\rho_g) = np^{-j}$ **do**
                if $g(T_p) = 0$ **then**
                    Change g and continue
                else
                    if $f(T_q) \neq \chi(q)g(T_q)$ for q prime different from p and $q \leq B(n,k)$ **then**
                        Pass to the next g
                    else

Set $v \leftarrow [g, \chi]$ and **stop** the cycle and the while iteration

Set $j \leftarrow j + 1$

if $v = []$ **then**

Let $\overline{\epsilon}^{(p)}$ be the component at p of $\overline{\epsilon}$

for $g \in S(np, k, \overline{\epsilon}(\overline{\epsilon}^{(p)})^{-2})_{\overline{\mathbb{F}}_\ell}$ such that ρ_g is irreducible and $\mathrm{N}(\rho_g) = np$ **do**

if $g(T_p) = 0$ **then**

Change g and continue

else

if $f(T_q) \neq \overline{\epsilon}^{(p)}(q)g(T_q)$ for q prime different from p and $q \leq B(n,k)$ **then**

Pass to the next g

else

Set $v \leftarrow [g, \overline{\epsilon}^{(p)}]$ and **stop** the cycle

if $v \neq []$ **then**

if $\mathrm{N}_p(\rho_g) \neq \mathrm{N}_p(\epsilon_g) + 1$ where ϵ_g is the character of g **then**

Set is_decomposable=true

Theorem 8.2.10. *Algorithm* 8.2.9 *is correct.*

Proof. The first part of the algorithm follows from Theorem 6.3.3: the representation is ramified at p and if $f(T_p) \neq 0$ then $\rho_f|_{G_p}$ is reducible. Proposition 8.1.5 give us a criterion to decide about the splitting of $\rho_f|_{G_p}$.

If $f(T_p) = 0$ then by Proposition 8.2.6 we can distinguish whether $\rho_f|_{G_p}$ is reducible or not. In the algorithm we determine if the representation is reducible, checking if it is twist by a character ramified only at p of a modular forms of lower level or of level np. The hypotheses on the forms we are twisting, i.e. irreducibility and the fact that the associate representation does not arise from lower level, are checked using Algorithm 7.2.4 and Algorithm 6.3.7 respectively. For the forms of lower level the bounds for the conductor of χ comes from the proof of Proposition 8.2.6. Analogously, we know that the level of the twist admitting a stable line with unramified quotient can be np only if the twist is done using $(\overline{\epsilon}^{(p)})^{-1}$, the component at p of $\overline{\epsilon}$, see Remark 8.2.7. The splitting in the reducible case is given by the splitting of $\rho_g|_{G_p}$, see Remark 8.2.7. □

Algorithm 8.2.11 (Check if two representations are twist by a given character)**.** Let n, m, k be positive integers, such that m is a multiple of n. Let ℓ be a prime not dividing m and n such that $2 \leq k \leq \ell + 1$.

Let $\psi : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$ be a character. Let $g : \mathbb{T}_\psi(m,k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings and let $\rho_g : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the representation attached to g in Corollary 4.0.5. Suppose that ρ_g is irreducible and $\mathrm{N}(\rho_g) = m$: Algorithm 6.3.7 and Algorithm 7.2.4 perform the respective checks.

Let $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character. Let $f : \mathbb{T}_\epsilon(n,k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings and let $\rho_f : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the representation attached to f in Corollary 4.0.5. Suppose that ρ_f is irreducible and $\mathrm{N}(\rho_f) = n$.

Let $\overline{\epsilon} : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ be the character defined by $\overline{\epsilon}(a)=f(\langle a \rangle)$ for all $a \in (\mathbb{Z}/n\mathbb{Z})^*$ and let $\overline{\psi} : (\mathbb{Z}/m\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ be the character defined by $\overline{\psi}(b)=g(\langle b \rangle)$ for all $b \in (\mathbb{Z}/m\mathbb{Z})^*$. Let χ be a Dirichlet character, represented giving a list $\chi^{(p)}$ for all p prime dividing the conductor of χ.

Input: n, m, k, ℓ, χ, $\overline{\epsilon}$, $\overline{\psi}$, $f(T_p)$ and $g(T_p)$ for p prime $p \leq B(m,k)$ where $B(m,k)$ is the Sturm bound for cusp forms for $\Gamma_0(m)$ and weight k;
Output: if $\rho_g \cong \rho_f \otimes \chi$ return true; otherwise return false.

Set twist=false;
if $\chi^2\overline{\epsilon} = \overline{\psi}$ **then**
  if $g(T_q) = \chi(q)f(T_q)$ for all q prime, $q \leq B(m,k)$ and $q \nmid n\,\mathrm{cond}(\chi)$ **then**
    Set $v \leftarrow 0$; list$\leftarrow [q$ prime, $q \leq B(m,k)$ and $q \mid n\,\mathrm{cond}(\chi)]$
    while p in list **do**
      if $p \mid \mathrm{cond}(\chi)$ and $p \nmid n$ **then**
        if $\mathrm{N}_p(m) = 2\mathrm{N}_p(\mathrm{cond}(\chi))$ and $g(T_p) = 0$ **then**
          $v = v + 1$ and pass to the next prime
      else
        if $f(T_p) \neq 0$ **then**
          Compute the characters of G_p in Theorem 6.3.3 for f i.e. compute ϵ_1 and ϵ_2 where $\epsilon_1 = \epsilon_2^{-1}\overline{\epsilon}$ and ϵ_2 is unramified at p and $\epsilon_2(\mathrm{Frob}_p) = f(T_p)$.

          if $\mathrm{N}_p(n) = \mathrm{N}_p(\overline{\epsilon}) + 1$ and $g(T_p) = 0$ **then**
            $v = v + 1$ and pass to the next prime
          else if $\mathrm{N}_p(m) = \mathrm{N}_p(n)$ **then**
            if $g(T_p) = p^{k-1}(\epsilon_1\chi^{(p)})(\mathrm{Frob}_p)$ **then**
              $v = v + 1$ and pass to the next prime
          else if $g(T_p) = 0$ **then**
            $v = v + 1$ and pass to the next prime
        else
          Run Algorithm 8.2.9 for f and p, let $v = [h, \tau]$ be the list in the output
          if $\tau = \chi^{(p)}$ and $h(T_p) = g(T_p)$ **then**

$v = v + 1$ and pass to the next prime
if v is equal to the length of list **then**
Set twist=true
return twist

Theorem 8.2.12. *Algorithm* 8.2.11 *is correct.*

Proof. To decide if ρ_g is equivalent to $\rho_f \otimes \chi$ or not, we check a relation in the space of modular forms at level m, given that ρ_g is irreducible with $\mathrm{N}(\rho_g) = m$ and weight k. Hence, it is enough to check equalities up to $B(m,k)$ where B is the Sturm bound for cusp forms for $\Gamma_0(m)$ and weight k since ρ_f and ρ_g are irreducible by hypothesis. The equality between the determinant of ρ_g and $\rho_f \otimes \chi$ leads to the equality $\chi^2\overline{\epsilon} = \overline{\psi}$.

For all primes q not dividing $n\,\mathrm{cond}(\chi)$ and $q \leq B(m,k)$ we have:

$$g(T_q) = \chi(q) f(T_q),$$

since these primes are unramified primes for ρ_g.

Similarly, for all primes r dividing $\mathrm{cond}(\chi)$ but not n we have that $\mathrm{N}_r(m)$ is equal to $2\mathrm{N}_r(\mathrm{cond}(\chi))$ by Proposition 8.2.1. Moreover, since in this case the twist restricted to the decomposition group at r does not admit a stable line with unramified quotient, then $g(T_r) = 0$.

Let p be a prime dividing n and $\mathrm{cond}(\chi)$.

If $f(T_p) \neq 0$ then we can compute the characters of G_p in Theorem 6.3.3 for f i.e. compute ϵ_1 and ϵ_2 where $\epsilon_1 = \epsilon_2^{-1}\overline{\epsilon}$ and ϵ_2 is unramified at p and $\epsilon_2(\mathrm{Frob}_p) = f(T_p)$.

If ρ_f restricted to G_p is indecomposable then $\mathrm{N}_p(n) = \mathrm{N}_p(\overline{\epsilon})+1$ and in Proposition 8.2.5 we have shown that there exist no stable line with unramified quotient for the twist, hence $g(T_p)$ is zero.

If ρ_f restricted to G_p is decomposable then $\mathrm{N}_p(n) = \mathrm{N}_p(\overline{\epsilon})$ and in Proposition 8.2.5 we have proved that there exist a stable line with unramified quotient for the twist if and only if the twist as the same conductor of the representation. Hence, $g(T_p)$ is non zero and equal to $p^{k-1}(\epsilon_1\chi^{(p)})(\mathrm{Frob}_p)$ if and only if $\mathrm{N}_p(m) = \mathrm{N}_p(n)$.

If $f(T_p) = 0$ then by Proposition 8.2.6 we have that there exist a stable line with unramified quotient for the twist if and only if the representation is reducible. Hence, $g(T_p) = 0$ unless Algorithm 8.2.9 returns in the output a non-empty list as third argument. In this case $g(T_p)$ has to be equal to the value at T_p of the form stored. □

In the next Algorithm we suppose that the character of the twist is not given and we check if there exist one.

Algorithm 8.2.13 (Check if two representations are twists)**.** Let n, m, k be positive integers, with n dividing m. Let ℓ be a prime not dividing m and n such that $2 \leq k \leq \ell + 1$.

Let $\psi : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$ be a character. Let $g : \mathbb{T}_\psi(m,k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings and let $\rho_g : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the representation attached to g in Corollary 4.0.5. Suppose that ρ_g is irreducible and $\mathrm{N}(\rho_g) = m$: Algorithm 6.3.7 and Algorithm 7.2.4 perform the respective checks.

Let $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character. Let $f : \mathbb{T}_\epsilon(n,k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings and let $\rho_f : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the representation attached to f in Corollary 4.0.5. Suppose that ρ_f is irreducible and $\mathrm{N}(\rho_f) = n$.

Let $\overline{\epsilon} : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ be the character defined by $\overline{\epsilon}(a)=f(\langle a \rangle)$ for all $a \in (\mathbb{Z}/n\mathbb{Z})^*$ and let $\overline{\psi} : (\mathbb{Z}/m\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ be the character defined by $\overline{\psi}(b)=g(\langle b \rangle)$ for all $b \in (\mathbb{Z}/m\mathbb{Z})^*$.

Input: n, m, k, ℓ, $\overline{\epsilon}$, $\overline{\psi}$, $f(T_p)$ and $g(T_p)$ for p prime $p \leq B(m,k)$ where $B(m,k)$ is the Sturm bound for cusp forms for $\Gamma_0(m)$ and weight k;
Output: if $\rho_g \cong \rho_f \otimes \chi$ for a Dirichlet character χ return χ; otherwise return 0.

$v \leftarrow [\ ]$;
for p prime dividing n **do**
  if $f(T_p) \neq 0$ **then**
    Let $\chi^{(p)}$ be the Dirichlet character from $(\mathbb{Z}/p^i\mathbb{Z})^*$ to $\overline{\mathbb{F}}_\ell^*$, for $i > 0$, such that $\mathrm{N}_p(\chi^{(p)}\overline{\epsilon}) + \mathrm{N}_p(\chi^{(p)}) = \mathrm{N}_p(m)$.
    Compute the characters of G_p in Theorem 6.3.3 i.e. compute ϵ_1 and ϵ_2 where we have that $\epsilon_1 = \epsilon_2^{-1}\overline{\epsilon}$, the character ϵ_2 is unramified at p and $\epsilon_2(\mathrm{Frob}_p) = f(T_p)$.
    if $\mathrm{N}_p(n) = \mathrm{N}_p(m)$ **then**
      if $g(T_p) = p^{k-1}(\epsilon_1\chi^{(p)})(\mathrm{Frob}_p)$ **then**
        Store $\chi^{(p)}$ in v
      else
        return 0 and **exit**
    else
      if $g(T_p) = 0$ **then**
        Store $\chi^{(p)}$ in v
      else
        return 0 and **exit**
  else if $f(T_p) = 0$ **then**
    Run Algorithm 8.2.9 for f at p, let v be the output obtained
    if is_reducible=false **then**

```
                    if g(T_p) = 0 then
                        Store χ^(p) = 1 in v
                    else
                        return 0 and exit
                else
                    if g(T_p) = 0 then
                        Store χ^(p) = 1 in v
                    else
                        if m ≠ np then
                            return 0 and exit
                        else
                            Let v = [h, ψ]
                            if h(T_q) ≠ g(T_q) for all q prime q ≤ B(m, k)
                            then
                                return 0 and stop
                            else
                                Store χ^(p) = ψ in v
Set χ ← ∏ χ^(p) for χ^(p) in v
if χ^2 ε̄ = ψ̄ then
    if g(T_q) = χ(q)f(T_q) for all q prime, q ≤ B(m, k), and q not dividing
    cond(χ) then
        return χ
    else
        return 0
else
    return 0
```

Theorem 8.2.14. *Algorithm* 8.2.13 *is correct.*

Proof. For all primes p dividing n we compute the local component $\chi^{(p)}$ of the character χ. If $f(T_p) \neq 0$ then, from Proposition 8.2.4 and from the hypothesis $\mathrm{N}(\rho_g) = m$, it follows that $\chi^{(p)}$ is the character such that $\mathrm{N}_p(\chi^{(p)}\overline{\epsilon}) + \mathrm{N}_p(\chi^{(p)})$ is equal to $\mathrm{N}_p(m)$. We compute the characters of G_p in Theorem 6.3.3 for ρ_f: let us denote them by ϵ_1 and ϵ_2 where $\epsilon_1 = \epsilon_2^{-1}\overline{\epsilon}$, the character ϵ_2 is unramified at p and $\epsilon_2(\mathrm{Frob}_p) = f(T_p)$. If ρ_f restricted to G_p is decomposable, then by Theorem 8.2.5 we have $g(T_p) \neq 0$ and $g(T_p) = p^{k-1}(\epsilon_1\chi^{(p)})(\mathrm{Frob}_p)$ if and only if $\mathrm{N}_p(n) = \mathrm{N}_p(m)$. If ρ_f restricted to G_p is indecomposable, then by Proposition 8.2.5 we have $g(T_p) = 0$. If $f(T_p) = 0$ then then by Proposition 8.2.6 we have $g(T_p) = 0$ unless $m = np$. In this last case, we run Algorithm 8.2.9 and we use the output to check equality between mod ℓ modular forms.

The character χ given by the product of the $\chi^{(p)}$ has to satisfy $\chi^2\overline{\epsilon} = \overline{\psi}$.

Moreover, for all primes q not dividing $\mathrm{cond}(\chi)$ and smaller than $B(m,k)$ the equality $g(T_q) = \chi(q)f(T_q)$ must hold. □

Algorithm 8.2.15 (Check minimality up to twisting)**.** Let n and k be positive integers. Let ℓ be a prime not dividing n such that $2 \leq k \leq \ell + 1$. Let $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character. Let $f : \mathbb{T}_\epsilon(n,k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings and let $\rho_f : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the representation attached to f in Corollary 4.0.5. Assume that Algorithm 6.3.7 and Algorithm 7.2.4 certify that ρ_f is irreducible and $\mathrm{N}(\rho_f) = n$. Let $\bar{\epsilon} : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ be the character defined by $\bar{\epsilon}(a) = f(\langle a \rangle)$ for all $a \in (\mathbb{Z}/n\mathbb{Z})^*$.

Input: n, k, ℓ, $\bar{\epsilon}$, $f(T_p)$ for p prime $p \leq B(n,k)$ where $B(n,k)$ is the Sturm bound for cusp forms for $\Gamma_0(n)$ and weight k;
Output: return 1 if f is minimal up to twisting; otherwise return the form g and the character such that $\rho_g \otimes \chi \cong \rho_f$.

---

for p prime dividing n **do**
  if $f(T_p) \neq 0$ **then**
    for $1 \leq i \leq \mathrm{N}_p(n)$ **do**
      for $g \in S(np^{-i}, k)_{\overline{\mathbb{F}}_\ell}$ **do**
        for χ Dirichlet character from $(\mathbb{Z}/p^j\mathbb{Z})^*$ to $\overline{\mathbb{F}}_\ell^*$ with $j > 0$ and such that $\mathrm{N}_p(\chi\epsilon_g) + \mathrm{N}_p(\chi) = \mathrm{N}_p(n)$, where ϵ_g is the character of g **do**
          if Algorithm 8.2.11 returns true **then**
            return g and χ and **stop**
  else
    Run Algorithm 8.2.9 for f and p, let v be the list in the output obtained
    if $v[2] = [h, \chi]$ with h of level dividing n **then**
      return h and χ and **stop**
return 1

Theorem 8.2.16. *Algorithm* 8.2.15 *is correct.*

Proof. Minimality up to twisting is a local condition: we need to verify it for every prime dividing the conductor of the representation. Let p be a prime dividing n, the conductor of ρ_f.

If $f(T_p) \neq 0$ then by Proposition 8.2.4 we compute the conductor of the twist and, hence, the set of characters for which we need to perform a check is known.

If $f(T_p) = 0$ then Algorithm 8.2.9 returns the form given in Proposition 8.2.6 and if such form exists and it is of level smaller than n, then f is not minimal up to twisting. □

8.3 Twisting by the mod ℓ cyclotomic character

Let n and k be positive integers. Let ℓ be a prime not dividing n such that $2 \leq k \leq \ell + 1$. Let $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character. Let $f : \mathbb{T}_\epsilon(n, k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings and let $\rho_f : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the representation attached to f in Corollary 4.0.5. Assume that Algorithm 6.3.7 and Algorithm 7.2.4 certify that ρ_f is irreducible and $\mathrm{N}(\rho_f) = n$. The twist of the Galois representation ρ_f by the mod ℓ cyclotomic character is isomorphic to the Galois representation associated to $\theta_\ell(f)$ by [Edi92, Section 3.1]:

$$\rho_{\theta_\ell(f)} \cong \rho_f \otimes \chi_\ell.$$

Hence, the representation obtained by twisting with powers of the mod ℓ cyclotomic character is isomorphic to the representation attached to the mod ℓ modular form obtained applying the same power of θ_ℓ to the form. Anyway this form could not be the minimal one giving rise to the twist. Suppose that the representation ρ_f has weight k, then the representation $\rho_f \otimes \chi_\ell^a$ for $a \in \mathbb{Z}$ has weight $k(\rho_f \otimes \chi_\ell^a)$: the weight is given by the theory of θ_ℓ-cycles, see [Edi92, Proposition 3.3].

Let us remark that the coefficients of the twist are given by the coefficients of $\theta_\ell^a f$, and that twisting by powers of the mod ℓ cyclotomic character does not change the field of definition of the representation.

Chapter 9

Fields of definition

The goal of this thesis is to give the outline of an algorithm which gives as output the image of a semi-simple residual modular Galois representation, up to conjugation, as a subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$. After checking whether the representation is reducible or not, the next step towards our aim is to determine the field of definition of the representation.

The field of definition of the representation is the smallest field $\mathbb{F} \subset \overline{\mathbb{F}}_\ell$ over which ρ_f is equivalent to all its conjugate. In this case, since the Brauer group of a finite field is trivial, the field of definition and the field of realization are the same field: see [DS74, Lemme 6.13] and [EC11, p.56]. Hence, the representation is equivalent to a representation whose image is made of matrices with entries in the field of definition. The image of the representation ρ_f is then a subgroup of $\mathrm{GL}_2(\mathbb{F})$.

Let $\mathbb{P}\rho_f : G_\mathbb{Q} \to \mathrm{PGL}_2(\mathbb{F})$ be the projective representation associated to the representation ρ_f through the quotient map $\mathrm{GL}_2(\mathbb{F}) \overset{\pi}{\twoheadrightarrow} \mathrm{PGL}_2(\mathbb{F})$. The representation $\mathbb{P}\rho_f$ can be defined on a different field than the field of definition of the representation. This field is the Dickson's field for the representation, as explained in Chapter 5.

The aim of this chapter is to describe the fields of definition of the representation and of the projective representation. These are fundamental ingredients in the description of the image of the representation. Related results has been proved by Ribet, see [Rib85], our main contribution is the use of the Sturm bound, which we have not seen in the literature before.

9.1 Linear representation

Let n and k be positive integers, and let ℓ be a prime not dividing n such that $2 \leq k \leq \ell+1$. Let $\epsilon\colon (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character and let $f\colon \mathbb{T}_\epsilon(n,k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings.

As explained in [EC11, Chapter 2, Section 2.5], the field of definition for the representation ρ_f is the smallest extension of $\mathbb{F}_\ell$ which contains the traces and the determinants of $\rho_f(\mathrm{Frob}_p)$ for all p not dividing $n\ell$ and it is the minimal field over which all conjugates are isomorphic. We want to make the result effective, using the local description of the representation given in Chapter 6.

Proposition 9.1.1. *Let n and k be positive integers and let ℓ be a prime such that $(n,\ell)=1$ and $2 \leq k \leq \ell+1$. Let $\epsilon\colon (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character and let $f\colon \mathbb{T}_\epsilon(n,k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings. Let us suppose that the representation $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$, given in Corollary 4.0.5, is irreducible and does not arise from lower level or weight. Let S be the set:*

$$S := \{f(T_p) | \, p \text{ prime}, \, p \neq \ell \text{ and } p \leq B(n,k)\} \cup \{f(\langle d \rangle) | \, d \in (\mathbb{Z}/n\mathbb{Z})^*\},$$

where $B(n,k)$ is the Sturm bound for cusp forms for $\Gamma_0(n)$.

Then the field of definition of ρ_f is $\mathbb{F}_\ell(S)$: the smallest extension of $\mathbb{F}_\ell$ containing the elements of the set S.

Proof. Let $\mathbb{F}$ be the field of definition of ρ_f. It is the smallest extension of $\mathbb{F}_\ell$ containing $f(T_p)$ for p prime, not dividing $n\ell$, and $f(\langle d \rangle)$ for $d \in (\mathbb{Z}/n\mathbb{Z})^*$, as proved in [EC11, Chapter 2, Section 2.5]. The statement is equivalent to prove that $\mathbb{F} = \mathbb{F}_\ell(S)$.

Let S' be the set

$$S' := \{f(T_p) | \, p \text{ prime}, \, p \leq B(n,k)\} \cup \{f(\langle d \rangle) | \, d \in (\mathbb{Z}/n\mathbb{Z})^*\} \supseteq S$$

and let us denote by $\mathbb{F}' := \mathbb{F}_\ell(S')$ the smallest extension of $\mathbb{F}_\ell$ containing all elements of S'. For all $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}')$ we have that, for all primes p less than $B(n,k)$, the conjugate of $f(T_p)$ by σ, which we will denote by $f(T_p)^\sigma$, is equal to $f(T_p)$ by definition of $\mathbb{F}'$. Corollary 6.1.3 implies that, since $f(T_p)^\sigma = f(T_p)$ for all primes up to the Sturm bound for cusp forms for $\Gamma_0(n)$, then $f^\sigma = f$. Therefore, the Galois representations attached to f^σ and f are isomorphic: they are both semi-simple and they have the same characteristic polynomials, hence the result follows by a theorem of Brauer-Nesbitt, see [CR06, Theorem 30.16]. For the same reason we have that the representations ρ_f and ρ_{f^σ} are isomorphic, so that ρ_f is isomorphic to ρ_f^σ.

Since $\mathbb{F}$ is the field of definition for the representation, we have that $\mathbb{F} \subseteq \mathbb{F}'$. Indeed, the field of definition is the smallest extension of $\mathbb{F}_\ell$ for which, for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F})$, the representation ρ_f^σ is isomorphic to ρ_f. Theorem 6.3.3 implies that $f(T_p)$ belongs to $\mathbb{F}$ for all primes p dividing n: by hypotheses ρ_f is irreducible and $n = \mathrm{cond}(\rho_f)$, so if $f(T_p)$ is non-zero then the Frobenius at p acts on a line over $\mathbb{F}$ with eigenvalue equal to $f(T_p)$. If the representation at ℓ is ramified then $f(T_\ell)$ belongs to $\mathbb{F}_\ell(S)$ by Theorem 6.3.1 and 6.3.2. If, instead, the representation is unramified at ℓ, which means that the weight is ℓ, then there are two possible eigenvalue of Frob_ℓ and this values are conjugated over a quadratic extension of $\mathbb{F}$. From this it follows that $\mathbb{F}' = \mathbb{F}(f(T_\ell))$. Hence, $\mathbb{F} = \mathbb{F}_\ell(S)$. □

Remark 9.1.2. In Proposition 9.1.1, we have shown that $\mathbb{F}$ the field of definition for the representation ρ_f is such that either $\mathbb{F}(f(T_\ell)) \cong \mathbb{F}$ or $\mathbb{F}(f(T_\ell))$

is quadratic over $\mathbb{F}$. The second case can occurs only if $k(\rho_f) = \ell$ and it corresponds to an embedding of mod ℓ modular form from weight one to weight ℓ. Hence, this is not the minimal weight in which the representation does occur.

Remark 9.1.3. In Proposition 9.1.1, the representation ρ_f is assumed to be irreducible. Let us recall that in the reducible case, the field of definition of the representation is the compositum of the fields of definition of the characters in which the representation decomposes.

9.2 Projective representation

Let ρ_f be the residual Galois representation as in Corollary 4.0.5, and let $\mathbb{F}$ be the field of definition for the representation. Let $\mathbb{P}\rho_f : G_{\mathbb{Q}} \to \mathrm{PGL}_2(\mathbb{F})$ be the projective representation obtained by composition with the quotient map $\mathrm{GL}_2(\mathbb{F}) \overset{\pi}{\twoheadrightarrow} \mathrm{PGL}_2(\mathbb{F})$.

Proposition 9.2.1. *Let n and k be two positive integers, let ℓ be a prime such that $(n, \ell) = 1$ and $2 \leq k \leq \ell+1$, and let $\epsilon\colon (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character. Let $f\colon \mathbb{T}_\epsilon(n, k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings and let $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the representation attached to f in Corollary* 4.0.5. *Assume that ρ_f is irreducible, it does not arise from lower level or weight and it is realized over $\mathbb{F}$. Then $\mathbb{P}\rho_f$ is realized over the subfield of $\mathbb{F}$ fixed by*

$$A\colon = \left\{\sigma \in \mathrm{Aut}(\mathbb{F}) |\ \exists \tau : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}^* : \rho_f^\sigma \cong \rho_f \otimes \tau\right\}.$$

Proof. Let $\mathbb{F}' \subset \overline{\mathbb{F}}_\ell$ be the subfield fixed (point-wise) by all $\sigma \in \mathrm{Aut}(\overline{\mathbb{F}}_\ell)$ such that $(\mathbb{P}\rho_f)^\sigma$ is isomorphic to $\mathbb{P}\rho_f$, therefore $\mathbb{F}'$ is the field of definition of the projective representation. Note that $(\mathbb{P}\rho_f)^\sigma = \mathbb{P}(\rho_f^\sigma)$, so we have $\mathbb{F}' \subseteq \mathbb{F}$, field of definition of the representation. Hence, $\mathbb{F}' \subseteq \mathbb{F}$ is the subfield fixed by the $\sigma \in \mathrm{Aut}(\mathbb{F})$ such that $\mathbb{P}(\rho_f^\sigma) \cong \mathbb{P}\rho_f$. This implies that for each choice of $\sigma \in \mathrm{Aut}(\mathbb{F})$ there exists a character $\tau : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}^*$ such that ρ_f^σ and ρ_f are twist.

Let σ be the Frobenius element of $\mathrm{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}')$, and let s be an element of $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$ such that for all g in the image of $\mathbb{P}\rho_f$ we have $\sigma(g) = sgs^{-1}$. Since $\mathrm{PGL}_2(\mathbb{F}')$ is a connected group, then by Lang's Theorem, see [Sri79, Theorem 2.4], there exists t in $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$ such that $s = \sigma(t)^{-1}t$. Then all tgt^{-1} are in $\mathrm{PGL}_2(\mathbb{F}')$, so the realization over $\mathbb{F}'$ is unique. □

What is $\mathrm{Aut}(\mathbb{P}\rho_f)$? The representation ρ_f is an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the $\mathbb{F}$-vector space $\mathbb{F}^2$, in the same way the projective representation $\mathbb{P}\rho_f$ is an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the projective line $\mathbb{P}^1_{\mathbb{F}}$, regarded as $\mathbb{F}$-scheme. Then $\mathrm{Aut}(\mathbb{P}\rho_f)$ is the group of elements of $\mathrm{Aut}(\mathbb{P}^1_{\mathbb{F}}) \cong \mathrm{GL}_2(\mathbb{F})/\mathbb{F}^*$ that commute with all elements in the image.

Proposition 9.2.2. *Let n and k be two positive integers, let ℓ be a prime such that $(n,\ell)=1$ and $2\leq k\leq \ell+1$, and let $\epsilon\colon (\mathbb{Z}/n\mathbb{Z})^*\to\mathbb{C}^*$ be a character. Let $f\colon \mathbb{T}_\epsilon(n,k)\to\overline{\mathbb{F}}_\ell$ be a morphism of rings and let $\rho_f : G_{\mathbb{Q}}\to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the representation attached to it in Corollary 4.0.5. Assume that ρ_f is irreducible, does not arise from lower level or weight and is realized over $\mathbb{F}$. Then the field of definition of $\mathbb{P}\rho_f$ is the smallest extension of $\mathbb{F}_\ell$ containing $(f(T_p))^2/f(\langle p\rangle)p^{k-1}$ for all primes p not dividing $n\ell$.*

Proof. Let $\mathbb{F}'$ denote the field of definition of the projective representation. As shown in Proposition 9.2.1, the field $\mathbb{F}'$ is the fixed field of $\mathbb{F}$, the field of definition of the representation, under the group of automorphism of $\mathbb{F}$ for which the representation and its conjugate are twist.

We have the following diagram of algebraic groups:

$$\begin{array}{ccccc} \mathrm{GL}_2(\overline{\mathbb{F}}_\ell) & \xrightarrow{\pi} & \mathrm{PGL}_2(\overline{\mathbb{F}}_\ell) & \xrightarrow{\sim} & \mathrm{SO}_3(\overline{\mathbb{F}}_\ell) \\ & \searrow^{\mathrm{Sym}^2\otimes\det^{-1}} & & & \downarrow \\ & & & & \mathrm{GL}_3(\overline{\mathbb{F}}_\ell) \end{array}$$

where π is the natural quotient map, the group homeomorphism from $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ to $\mathrm{GL}_3(\overline{\mathbb{F}}_\ell)$ is defined as follows:

$$\begin{array}{rccc} \mathrm{Sym}^2\otimes\det^{-1}\colon & \mathrm{GL}_2(\overline{\mathbb{F}}_\ell) & \to & \mathrm{GL}_3(\overline{\mathbb{F}}_\ell) \\ & \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \mapsto & \begin{pmatrix} a^2 & ab & b^2 \\ 2ac & ad{+}bd & 2bd \\ c^2 & cd & d^2 \end{pmatrix}\cdot\begin{pmatrix} 1 \\ \hline ad{-}bd \end{pmatrix} \end{array}$$

In particular, given a diagonal matrix $D=\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)\in \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$, then we have that

$$(\mathrm{Sym}^2\otimes\det^{-1})(D)=\begin{pmatrix} a/b & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & b/a \end{pmatrix}.$$

Hence, by simple computations it follows that $\ker(\mathrm{Sym}^2\otimes\det^{-1})\cong\overline{\mathbb{F}}_\ell^*$ is given by the scalar matrices. Moreover, each matrix in the image of $\mathrm{Sym}^2\otimes\det^{-1}$ has determinant 1 and it preserves q, the quadratic form on $\mathbb{P}^2_{\overline{\mathbb{F}}_\ell}$ defined by $q(x,y,z)=4xz-y^2$. Then $\mathrm{Sym}^2\otimes\det^{-1}(\mathrm{GL}_2(\overline{\mathbb{F}}_\ell))$ is isomorphic to $\mathrm{SO}_3(\overline{\mathbb{F}}_\ell,q)$.

The groups $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$ and $\mathrm{SO}_3(\overline{\mathbb{F}}_\ell,\overline{q})$ are isomorphic, where $\overline{q}$ is the standard quadratic form on $\mathbb{P}^2_{\overline{\mathbb{F}}_\ell}$, see [Die71, Section 9, Chapter II] or [FH91, p.273]. This isomorphism gives an injection of $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$ in $\mathrm{GL}_3(\overline{\mathbb{F}}_\ell)$.

If $\ell\neq 2$, the quadratic forms q and $\overline{q}$ are equivalent over $\overline{\mathbb{F}}_\ell$, see [Ser77a, pp.34-35], and in characteristic 2 they are equivalent because they are both

degenerate and both equivalent to the form x^2. Hence, from now on we will drop the reference to the quadratic form in the notation of the special orthogonal group.

Let us claim that conjugation in $\mathrm{SO}_3(\overline{\mathbb{F}}_\ell)$ by element of $\mathrm{GL}_3(\overline{\mathbb{F}}_\ell)$ is the same as conjugation in $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$. The automorphism group of the image of the map φ from $\mathbb{P}^1_{\overline{\mathbb{F}}_\ell}$ to $\mathbb{P}^2_{\overline{\mathbb{F}}_\ell}$ given by $(x : y) \mapsto (x^2 : 2xy : y^2)$ is a subgroup of $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$: the map φ is a closed embedding, and its image is the zero locus of the quadratic form q. Any matrix in $\mathrm{GL}_3(\overline{\mathbb{F}}_\ell)$ acting as conjugation on the image of φ corresponds to an automorphism of the image, so to conjugation in $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$. Hence, the claim holds true.

In conclusion, any 2-dimensional projective representation is a linear representation to $\mathrm{GL}_3(\overline{\mathbb{F}}_\ell)$. In particular, the representation $\mathbb{P}\rho_f$ corresponds to the representation $\mathrm{Sym}^2 \otimes \det^{-1}(\rho_f)$ in $\mathrm{GL}_3(\overline{\mathbb{F}}_\ell)$. The representation ρ_f is semi-simple, then $\mathrm{Sym}^2(\rho_f)$ is semi-simple: since ρ_f is 2-dimensional, this follows from [Ser94, Théorème 2]. Therefore, the representation $\mathrm{Sym}^2 \otimes \det^{-1}(\rho_f)$ is semi-simple.

For any $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}')$ the conjugate of $\mathrm{Sym}^2 \otimes \det^{-1}(\rho_f)$ by σ and the representation $\mathrm{Sym}^2 \otimes \det^{-1}(\rho_f)$ are semi-simple and they give the same characteristic polynomials as functions on $\mathrm{Gal}(\overline{\mathbb{Q}}\,/\mathbb{Q}\,)$.

Therefore, the representation $\mathrm{Sym}^2 \otimes \det^{-1}(\rho_f)$ is isomorphic to all its conjugates over $\mathbb{F}'$ by [CR06, Theorem 30.16]. By the Brauer-Nesbitt Theorem combined with the Chebotarev density Theorem, the field $\mathbb{F}'$ contains all the traces of the representation $\mathrm{Sym}^2 \otimes \det^{-1}(\rho_f)$ at the unramified prime. This means that $\mathbb{F}'$ is the smallest extension of $\mathbb{F}_\ell$ containing $(f(T_p))^2/f(\langle p\rangle)p^{k-1}$ for all primes p, not dividing $n\ell$, since for the unramified primes we have:

$$\mathrm{Trace}(\mathrm{Sym}^2 \otimes \det^{-1}(\rho_f(\mathrm{Frob}_p))) = \frac{(f(T_p))^2}{f(\langle p\rangle)p^{k-1}} - 1.$$

□

The previous proposition is not effective: there is no bound for the number of traces needed. Anyway we can compute $\mathbb{F}'$, the Dickson's field of the representation, using the following observation.

Let n and k be two positive integers, let ℓ be a prime such that $(n, \ell) = 1$ and $2 \leq k \leq \ell+1$, and let $\epsilon\colon (\mathbb{Z}\,/n\mathbb{Z}\,)^* \to \mathbb{C}^*$ be a character. Let $f : \mathbb{T}_\epsilon(n, k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings and $\rho_f : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ the representation attached to it in Corollary 4.0.5. Assume that ρ_f is irreducible, it does not arise from lower level or weight and it is realized over $\mathbb{F}$. Moreover, assume that f is minimal up to twisting: we can check this using Algorithm 8.2.15.

In Proposition 9.2.1 we have proved that $\mathbb{F}' = \mathbb{F}^A$ where

$$A\colon = \left\{\sigma \in \mathrm{Aut}(\mathbb{F}) |\ \exists \tau : \mathrm{Gal}(\overline{\mathbb{Q}}\,/\mathbb{Q}\,) \to \mathbb{F}^* : \rho_f^\sigma \cong \rho_f \otimes \tau\right\}.$$

The condition $\rho_f^\sigma \cong \rho_f \otimes \tau$ is equivalent to the equality between f^σ and the mod ℓ modular form of minimal level and weight associated to $\rho_f \otimes \tau$, since f is minimal up to twisting and the representation ρ_f does not arise from lower level or weight. Algorithm 8.2.13 checks if two representation are twist of each other and, if it is the case, it returns the character which gives the twist. Hence, once f^σ is computed we can run such algorithm and find $\mathbb{F}'$.

To speed up computations, instead of trying all subfields of the field of definition of the representation, we compute the smallest extension of $\mathbb{F}_\ell$ containing $(f(T_p))^2/f(\langle p\rangle)p^{k-1}$ for all primes p, not dividing $n\ell$, up to the Sturm bound for cusp forms for $\Gamma_0(n)$ and weight k. Let us denote this extension by $\mathbb{F}''$.

This field is a subfield of the field of definition of the projective representation, so we run Algorithm 8.2.13 for f^σ and f with $\sigma \in \mathrm{Gal}(\mathbb{F}/\mathbb{F}'')$. We used coefficients only up to the Sturm bound for cusp forms for $\Gamma_0(n)$ and weight k because these are needed to run Algorithm 8.2.13. What we have just described is the following algorithm:

Algorithm 9.2.3 (Field of definition of the projective representation)**.** Let n and k be positive integers. Let ℓ be a prime not dividing n such that $2 \leq k \leq \ell + 1$. Let $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character. Let $f : \mathbb{T}_\epsilon(n,k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings and let $\rho_f : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the representation attached to f in Corollary 4.0.5. Suppose that ρ_f is irreducible and $\mathrm{N}(\rho_f) = n$. Let $\mathbb{F}$ be the field of definition of the representation, it can be computed using Proposition 9.1.1. Let $\overline{\epsilon} : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ be the character defined by $\overline{\epsilon}(a) = f(\langle a\rangle)$ for all $a \in \mathbb{Z}/n\mathbb{Z}^*$.

Input: n, k, ℓ, $\overline{\epsilon}$, $\mathbb{F}$ field of definition of the representation, $f(T_p)$ for p prime $p \leq B(n,k)$ where $B(n,k)$ is the Sturm bound for cusp forms for $\Gamma_0(n)$ and weight k;
Output:$\mathbb{F}'$ field of definition of the projective representation.

Set $\mathbb{F}'$ equal to the smallest extension of $\mathbb{F}_\ell$ containing $(f(T_p))^2/f(\langle p\rangle)p^{k-1}$ for all p prime, $p \nmid n\ell$, $p \leq B(n,k)$.
if $\mathbb{F}' \neq \mathbb{F}$ **then**
  for $\sigma \in \mathrm{Gal}(\mathbb{F}/\mathbb{F}')$ such that $\langle\sigma\rangle \cong \mathrm{Gal}(\mathbb{F}/\mathbb{F}')$ **do**
    Compute the system of eigenvalues $f_{n,k}^\sigma$
    Run Algorithm 8.2.13 for and $f_{n,k}$ with $f_{n,k}^\sigma$
    if The output of Algorithm 8.2.13 is not 0 **then**
      Set $\mathbb{F}' = \mathbb{F}^\sigma$ and restart the cycle with this new choice of $\mathbb{F}'$

Theorem 9.2.4. *Algorithm* 9.2.3 *is correct.*

Proof. This follows from Proposition 9.2.1 and 9.2.2. □

Remark 9.2.5. Twisting ρ_f does not change the image of $\mathbb{P}\rho_f$. This means that if f is not minimal up to twisting then the projective image of f and the one of the form of smaller level of which f is twist are isomorphic. Hence, we run Algorithm 8.2.15 and if the form is not minimal we get that its projective image is already in the database at a smaller level.

Chapter 10

Irreducible representations

In this chapter we study irreducible 2-dimensional residual modular Galois representations with exceptional image. This means that projective image is either isomorphic to a dihedral group or projectively exceptional. Indeed, if the representation does not have projective image isomorphic to a dihedral group or projectively exceptional then by Dickson's Theorem it has "big" image, i.e. the image contains $\mathrm{SL}_2(\mathbb{F})$, where $\mathbb{F}$, finite extension of $\mathbb{F}_\ell$, is the Dickson's field of the representation.

In the first section we study the case of projective image isomorphic to a dihedral group. Analogously, in the second section we describe the case of image projectively exceptional. Let ℓ be a prime larger than 3 (respectively different from 5), we link modular forms mod ℓ with projectively exceptional image to modular forms in characteristic 3 (respectively 2 and 5) with octahedral and tetrahedral (respectively icosahedral) projective image.

In addition, in the tetrahedral and octahedral case, let f be a form with projectively exceptional image in characteristic 3 (respectively 5 in the icosahedral case). We describe a construction that gives a form in characteristic zero whose reduction mod 3 (respectively mod 5) is the form f and such that its reduction modulo any other odd prime is projectively exceptional. We also study the image of the reduction mod 2 of this characteristic zero form.

The results of the first section are essentially known in the literature, and are due to Serre, Wiese and Dieulefait-Billerey. We give a different argument from the one presented in [BD12] about the ramification of the quadratic character. On the other hand, the results of the second section give a new contribution towards a better comprehension of projectively exceptional modular Galois representations.

10.1 Dihedral case

Let us suppose that the representation ρ_f, defined as in Corollary 4.0.5, is an irreducible representation. If the projective image of ρ_f is isomorphic to a dihedral group D_{2n}, with ℓ not dividing n, then by Dickson's Theorem there exists a Cartan subgroup $C \subseteq \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$, that is the group of points of a split or non-split maximal torus, such that $G := \rho_f(G_{\mathbb{Q}})$ is contained in the

normalizer N of C, but not in C. Let $\alpha : G_{\mathbb{Q}} \to \mathbb{Z}/2\mathbb{Z}$ be the composition:

$$G_{\mathbb{Q}} \longrightarrow G \subseteq N \overset{\alpha}{\twoheadrightarrow} N/C \cong \mathbb{Z}/2\mathbb{Z}\,.$$

The kernel of α is an open subgroup of $G_{\mathbb{Q}}$ of index 2, so its fixed field K is quadratic and unramified outside $n\ell$, where $n = \mathrm{cond}(\rho_f)$ by construction.

Let $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}/K) \subset G_{\mathbb{Q}}$, then $\mathbb{P}\rho_f(G_K) = C$ and ρ_f restricted to G_K is reducible:

$$\rho_f|_{G_K} = \chi \oplus \chi',$$

where χ, χ' are characters such that, denoted by σ the non trivial element of $\mathrm{Gal}(K/\mathbb{Q})$, the character $\chi' = \chi^\sigma$ where for all $\gamma \in G_K$ we have $\chi^\sigma(\gamma) = \chi(\sigma\gamma\sigma^{-1})$. Hence, ρ_f is the representation of $G_{\mathbb{Q}}$ induced by χ.

Moreover, the order of a maximal cyclic subgroup contained in the projective image is given by the order of the character $\chi^{-1}\chi^\sigma$, according to [Ser77b, (7.2.1)(d)], and the character χ can be computed using the statements in [Ser77b, (7.2.1)] if the quadratic character α is known.

Proposition 10.1.1. *Let n and k be positive integers, let ℓ be a prime not dividing n and such that $2 \leq k \leq \ell + 1$. Let $\epsilon\colon (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character and $f\colon \mathbb{T}_\epsilon(n,k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings. Let us suppose that the representation $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$, given in Corollary* 4.0.5, *does not arise from lower level or weight, it is realized over $\mathbb{F}$ and it is irreducible. Then $\mathbb{P}\rho_f(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ is dihedral if and only if there exists a quadratic character $\alpha\colon (\mathbb{Z}/n\mathbb{Z})^* \to \{\pm 1\}$ such that $\rho_f \cong \alpha \otimes \rho_f$.*

Proof. If $\mathbb{P}\rho_f(G_{\mathbb{Q}})$ is dihedral then the existence of the character follows from the description above. Vice versa let suppose there exists a character $\alpha\colon (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{F}^*$ such that $\rho_f \cong \alpha \otimes \rho_f$. Then for all unramified prime p the traces of the two representations are equal: $f(T_p) = \alpha(p)f(T_p)$, and also the determinant $f(\epsilon(p))p^{k-1} = \alpha(p)^2 f(\epsilon(p))p^{k-1}$. Hence by the Chebotarev density Theorem the character α has to be a quadratic character. Moreover, by [Ser77b, (7.2.1), p.337], we have that the projective image is dihedral. □

Corollary 10.1.2. *In the same hypotheses of Proposition* 10.1.1*, if the character α is ramified at a prime p dividing n, then p^2 divides n. If the character α ramifies at ℓ then either $f(T_\ell) \neq 0$ and $k = (\ell+1)/2$ or $f(T_\ell) = 0$ and $k = (\ell+3)/2$.*

Proof. The character α in unramified outside $n\ell$ because the representation ρ_f is in unramified outside $n\ell$. Let p be a prime dividing n. Since $\rho_f \cong \alpha\otimes\rho_f$ then $\mathrm{N}_p(\rho_f) = \mathrm{N}_p(\alpha\otimes\rho_f)$. Suppose that α is ramified at p. The result follows from [BD12, Proposition 3.1, 1].

Let us suppose that α is ramified at ℓ.

If $f(T_\ell) \neq 0$ then by Theorem 6.3.1 we have that ρ_f restricted to the inertia subgroup at ℓ is reducible. By [Dia97, Proposition 2.2], it is decomposable. Since α is a quadratic character ramified at ℓ, then, once restricted to the inertia at ℓ, it is equivalent to $\chi_\ell^{(\ell-1)/2}$. Given that $\rho_f \cong \alpha \otimes \rho_f$, we have that:

$$\rho_f|_{I_\ell} \cong \begin{pmatrix} \chi_\ell^{k-1} & 0 \\ 0 & 1 \end{pmatrix} \cong (\alpha \otimes \rho_f)|_{I_\ell} \cong \begin{pmatrix} \chi_\ell^{(\ell-1)/2}\chi_\ell^{k-1} & 0 \\ 0 & \chi_\ell^{(\ell-1)/2} \end{pmatrix},$$

and this is possible only if $k = (\ell+1)/2$.

If $f(T_\ell) = 0$ then by Theorem 6.3.2 we have that $\rho_f|_{I_\ell}$ is reducible and equivalent to $\varphi'^{k-1} \oplus \varphi^{k-1}$, where φ', φ are the two fundamental characters of level 2. Since $\rho_f \cong \alpha \otimes \rho_f$, then using that $\varphi\varphi' = \chi_\ell|_{I_\ell}$ and that $\chi_\ell|_{I_\ell} = \varphi^{\ell+1}$ we have that

$$\ell(k-1) = (k-1) + \frac{\ell^2-1}{2} \quad \text{in } \mathbb{Z}/(\ell^2-1)\mathbb{Z}$$

this is impossible for $\ell = 2$ and if ℓ is odd then it is equivalent to

$$k-1 \equiv \frac{\ell+1}{2} \bmod \ell+1.$$

Therefore, this is possible if and only if $k = (\ell+3)/2$. □

Algorithm 10.1.3 (Check dihedral projective image)**.** Let n, k be positive integers. Let ℓ be a prime not dividing n such that $2 \leq k \leq \ell+1$. Let $\epsilon\colon (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character. Let $f\colon \mathbb{T}_\epsilon(n,k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings and let ρ_f be the representation attached to f in Corollary 4.0.5. Suppose that ρ_f is irreducible and $\mathrm{N}(\rho_f) = n$: Algorithm 6.3.7 and Algorithm 7.2.4 perform the respective checks.

Input: n, k, ℓ, $f(T_p)$ for p prime $p \leq B(n,k)$ where $B(n,k)$ is the Sturm bound for cusp forms for $\Gamma_0(n)$ and weight k;
Output: if $\mathbb{P}\rho_f(G_\mathbb{Q})$ is dihedral return α such that $\rho_f \cong \rho_f \otimes \alpha$; otherwise return 0.

$D \leftarrow [\ ]$;
if $k \notin \{(\ell+1)/2, (\ell+3)/2\}$ **then**
    Set D to be the list of all the possible quadratic characters α of $(\mathbb{Z}/q\mathbb{Z})^*$, where q is the product of all primes dividing n such that their square divides n;
else

Set D to be the list of all the possible quadratic characters α of $(\mathbb{Z}/q'\mathbb{Z})^*$, where $q' = \ell q$ where q is the product of all primes dividing n such that their square divides n;
for $\alpha \in D$ **do**
  if $f(T_p) = \alpha(p)f(T_p)$ for all primes p with $p \leq B(n,k)$ **then**
    return α and **stop**
return 0 and **stop**

Theorem 10.1.4. *Algorithm* 10.1.3 *is correct.*

Proof. Proposition 10.1.1 states that the projective image is dihedral if and only if there exists a quadratic character α such that $\rho_f \cong \alpha \otimes \rho_f$. The set of characters is described in Corollary 10.1.2. Since $\rho_f \cong \alpha \otimes \rho_f$ then their conductor are the same, so the representation $\alpha \otimes \rho_f$ has conductor n by hypothesis on ρ_f. The representation $\alpha \otimes \rho_f$ arises from a form at level n and weight k: this follows from the hypotheses and the equivalence of the representations. Such form has q-expansion given by $\sum \alpha(n)f(T_n)q^n$. Hence, it is enough to check equalities up to $B(n,k)$, the Sturm bound for cusp forms for $\Gamma_0(n)$ and weight k since ρ_f is irreducible. □

10.2 Exceptional groups case

Let the representation ρ_f, defined as in Corollary 4.0.5, be irreducible and projectively exceptional.

Let us recall that the following isomorphisms hold: $\mathfrak{A}_4 \cong \mathrm{SL}_2(\mathbb{F}_3)/\{\pm 1\}$ and $\mathfrak{S}_4 \cong \mathrm{PGL}_2(\mathbb{F}_3)$, while $\mathfrak{A}_5 \cong \mathrm{SL}_2(\mathbb{F}_4)$ and also $\mathfrak{A}_5 \cong \mathrm{SL}_2(\mathbb{F}_5)/\{\pm 1\}$.

This implies that in characteristic 3 if a representation has projective image isomorphic to $\mathfrak{A}_4$ or $\mathfrak{S}_4$ then its image contains $\mathrm{SL}_2(\mathbb{F}_3)$ so it is not exceptional. Analogously, in characteristic 5 and 2 if the projective image is isomorphic to $\mathfrak{A}_5$ then the image is not exceptional.

Let ℓ be a prime greater than 3 (respectively different from 5), in the following proposition we link modular forms mod ℓ with projectively exceptional image to modular forms in characteristic 3 (respectively 2 and 5) with octahedral and tetrahedral (respectively icosahedral) projective image.

Proposition 10.2.1. *Let n and k be two positive integers. Let ℓ be a prime not dividing n such that $2 \leq k \leq \ell + 1$. Let $\epsilon\colon (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character and let $f\colon \mathbb{T}_\epsilon(n,k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings. Let us suppose that the representation $\rho_f : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$, attached to f in Corollary* 4.0.5*, does not arise from lower level or weight, it is irreducible, minimal up to twisting*

and projectively exceptional. Let us assume that $\ell > 3$ if the projective image is octahedral or tetrahedral otherwise let us assume $\ell \neq 5$.

Then there exists a characteristic zero, weight one cuspidal eigenform such that the reduction mod ℓ of the associated Artin representation is equivalent to ρ_f.

Moreover, if the projective image is octahedral or tetrahedral then the reduction modulo 3 of the Artin representation is not exceptional. Analogously, if the projective image is icosahedral then the reductions modulo 2 and 5 of the Artin representation are not exceptional.

Proof. Let $G = \rho_f(G_{\mathbb{Q}})$ and H be its projective image. Let us suppose that H is an icosahedral group. The case of octahedral and tetrahedral projective image are completely analogous and, hence, we will not discuss them.

Since the representation ρ_f is irreducible and minimal up to twisting then its determinant is a character of 2-power order, otherwise the twist of ρ_f with a power of the determinant would have lower conductor.

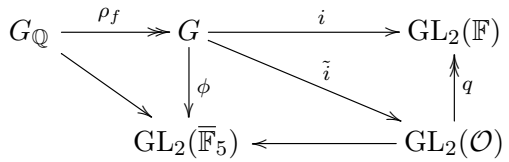
The group G is a finite group and it surjects to a group isomorphic to $\mathfrak{A}_5$, hence to $\mathrm{SL}_2(\mathbb{F}_5)/\{\pm 1\}$. The kernel of the projection is given by a cyclic group of 2-power order since the determinant is a character of 2-power order. Hence, G does admit a faithful representation $\phi\colon G \to \mathbb{F}' \cdot \mathrm{GL}_2(\mathbb{F}_5)$, where $\mathbb{F}'$ is a finite extension of $\mathbb{F}_5$. Indeed the map ϕ is injective because $\mathfrak{A}_5$ is a simple group and only elements of 5-power order can be in the kernel, while the kernel is cyclic of 2-power order.

The group G is by construction contained in $\mathrm{GL}_2(\mathbb{F})$, where $\mathbb{F}$ is the field of definition of the representation ρ_f. Let W be the ring of Witt vectors over $\mathbb{F}$, see [Ser95, Section I.6], and let us denote by $q : W \to \mathbb{F}$ the quotient map. Let i denote the inclusion, then there exist, up to conjugation, a unique map $\tilde{i}$ which lifts the representation i of G to $\mathrm{GL}_2(W)$ by the Schur-Zassenhaus Theorem, see [Rob96, (9.1.2)]. The following diagram summarizes the setting:

$$\begin{array}{ccccc} G_{\mathbb{Q}} & \xrightarrow{\rho_g} & G & \xrightarrow{\quad i \quad} & \mathrm{GL}_2(\mathbb{F}) \\ & & \downarrow{\scriptstyle \phi} & \searrow^{\tilde{i}} & \uparrow{\scriptstyle q} \\ & & \mathbb{F}' \cdot \mathrm{GL}_2(\mathbb{F}_5) & & \mathrm{GL}_2(W). \end{array}$$

Since $G_{\mathbb{Q}}$ is compact and ρ_f is continuous, $\tilde{i}(G)$ is a compact subgroup of $\mathrm{GL}_2(W)$. Moreover, G is a finite group, hence $\tilde{i}(G)$ is finite. Therefore by representation theory, see [Ser78, Section 12], there exist a number field such that the representation is realized over the ring of integer $\mathcal{O}$ herein. The ring

$\mathcal{O}$ admits a residue field at 5, hence we have the following:



where the representation ϕ is lifted from $\mathrm{GL}_2(\mathbb{F}')$ to $\mathrm{GL}_2(\overline{\mathbb{F}}_5)$ according to [EC11, Lemma 7.2.3 and Theorem 7.2.2].

Then by [KW09a, Corollary 10.2] there exists a cuspidal eigenform with coefficients in $\mathcal{O}$ and of weight one whose associated representation is equivalent to $\tilde{i} \circ \rho_f$. So its reduction mod ℓ is equivalent to ρ_f. Moreover, this form can be reduced modulo 5. Since the group G has a faithful representation in $\mathrm{GL}_2(\overline{\mathbb{F}}_5)$ and projective image isomorphic to $\mathfrak{A}_5$ then the representation given by composition with the reduction map has not exceptional image. This means that, by Khare-Wintenberger Theorem, there exists a mod 5 modular form h with minimal level and weight such that the associated representation ρ_h is equivalent to the given one and and it has big image.

Since $\mathfrak{A}_5 \cong \mathrm{SL}_2(\mathbb{F}_5)/\{\pm 1\}$ and $\mathfrak{A}_5 \cong \mathrm{SL}_2(\mathbb{F}_4)$, then we repeat the same argument to prove the existence of a mod 2 modular form with non-exceptional image using that $\mathrm{SL}_2(\mathbb{F}_4) \cong \mathfrak{A}_5$. □

Remark 10.2.2. Icosahedral representations in characteristic 2 have a specific characterization. Indeed, up to $\mathbb{F}_4/\mathbb{F}_2$-automorphisms, the trace of an element in $\mathrm{SL}_2(\mathbb{F}_4)$ depends only on its order. The possible orders of elements in $\mathrm{SL}_2(\mathbb{F}_4)$ are 2, 3 and 5. If an element has order 2, it must have characteristic polynomial $x^2 - 1 = (x-1)^2$ and so has trace 0. Similarly, every nontrivial element of order 3 has characteristic polynomial $x^2 + x + 1$ and so has trace 1. Finally, the nontrivial elements of order 5 have as characteristic polynomial a degree 2, monic polynomial over $\mathbb{F}_4$ dividing $x^4+x^3+x^2+x+1$, and the unique two such polynomials are $\mathrm{Gal}(\mathbb{F}_4/\mathbb{F}_2)$-conjugate as claimed. Therefore, if f is a mod 2 modular form of odd level such that the representation ρ_f given in Corollary 4.0.5 is irreducible and with icosahedral projective image, then

$$f(T_p) = \begin{cases} 0 & \text{if } \mathrm{ord}(\mathrm{Frob}_p) = 1 \text{ or } 2 \\ 1 & \text{if } \mathrm{ord}(\mathrm{Frob}_p) = 3 \\ \omega \text{ or } \omega^2 & \text{if } \mathrm{ord}(\mathrm{Frob}_p) = 5 \end{cases}$$

where ω, ω^2 are the distinct roots of $x^2 + x + 1$ in $\mathbb{F}_4$. Moreover, the form f^σ, where $\langle\sigma\rangle \cong \mathrm{Gal}(\mathbb{F}_4/\mathbb{F}_2)$, is a mod 2 modular form with the same level and weight of f and the associated representation has icosahedral projective image.

Proposition 10.2.1 is a statement about existence of a characteristic zero modular form with certain properties and it is not constructive. In the tetrahedral and octahedral case, let f be a form with projectively exceptional image in characteristic 3 (respectively 5 in the icosahedral case). In the next section we describe a construction that gives a form in characteristic zero whose reduction mod 3 (respectively mod 5) is the form f and such that the residual representation modulo any other odd prime is projectively exceptional. We also study the image of the reduction mod 2 of this characteristic zero form.

10.3 Construction for the exceptional cases

– Projective image isomorphic to $\mathfrak{S}_4$ in characteristic 3

Let f be a mod 3 cuspidal eigenform of level n, not divisible by 3, weight k, with $2 \leq k \leq 4$, and let $\overline{\epsilon} : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ be the unique character such that $f \in S(n, k, \overline{\epsilon})_{\overline{\mathbb{F}}_\ell}$.

Let us suppose that the representation ρ_f, attached to f as in Corollary 4.0.5, is irreducible with projective image isomorphic to $\mathrm{PGL}_2(\mathbb{F}_3) \cong \mathfrak{S}_4$, and it is minimal with respect to level, weight and twisting.

Let $\mathbb{F}$ be the field of definition of the representation. The field of definition of the projective representation is $\mathbb{F}_3$ since all octahedral groups are conjugated by [Fab11, Proposition 4.17]. By Proposition 5.2.2 the image of the representation: $\rho_f(G_{\mathbb{Q}}) \subseteq \mathbb{F}^* \cdot \mathrm{GL}_2(\mathbb{F}_3)$.

Let ρ_2 be the 2-dimensional faithful representation of $\mathrm{GL}_2(\mathbb{F}_3)$ in Table 5.2. The intersection $\mathbb{F}^* \cap \mathrm{GL}_2(\mathbb{F}_3)$ is given by $\{\pm 1\}$, hence, a representation of $\mathbb{F}^* \cdot \mathrm{GL}_2(\mathbb{F}_3)$, with $\mathbb{F}^*$ acting by scalars, is given by a character of $\mathbb{F}^*$ and a representation of $\mathrm{GL}_2(\mathbb{F}_3)$ such that the two representations are compatible, i.e. they have the same image for -1.

Let $\beta : \mathbb{F}^* \cdot \mathrm{GL}_2(\mathbb{F}_3) \to \mathrm{GL}_2(\mathcal{O}_K)$ be the irreducible 2-dimensional representation given by the choice of ρ_2 as representation of $\mathrm{GL}_2(\mathbb{F}_3)$ and a compatible character $\tau : \mathbb{F}^* \to \mathbb{Z}[\zeta]^*$, where $\zeta \in \mathbb{C}$ is a root of unity of order equal to the cardinality of $\mathbb{F}^*$. The representation β is realized over $\mathcal{O}_K$, which is the ring of integers of a number field which contains the field of definition of ρ_2, which is $\mathbb{Q}(\sqrt{2})$, as shown in Table 5.2, and the cyclotomic extension of $\mathbb{Q}$ given by the image of τ. Let us remark that the field K is completely determined from the choice of β.

Let ρ be the composition:

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow[\rho_f]{} \mathbb{F}^* \mathrm{GL}_2(\mathbb{F}_3) \xrightarrow[\beta]{} \mathrm{GL}_2(\mathcal{O}_K), \qquad \text{with } \rho = \beta \circ \rho_f.$$

By Langlands-Tunnell theorem, or equivalently by [KW09a, Corollary 10.2], there exist a weight one cuspidal eigenform of minimal level and weight, that we will denote as f_β, such that ρ_{f_β} is equivalent to ρ. Moreover, this form has octahedral projective image by construction.

Can we determine the level of f_β?

The representation ρ_f is unramified outside $3n$ by Corollary 4.0.5, hence also the representation ρ_{f_β} is unramified outside $3n$. The level of the form f_β is the conductor of the representation ρ_{f_β} by Khare-Wintenberger Theorem.

Let p be a prime dividing n (let us recall that n is not divisible by 3 by hypothesis), and assume that $f(T_p) \neq 0$. Proposition 8.1.5 gives us a criterion to decide whether the representation restricted to the decomposition group at p is decomposable or not. The representation restricted to the decomposition group at p is such that:

$$\rho_f|_{G_p} \cong \begin{pmatrix} \epsilon_1 \chi_3^{k-1} & * \\ 0 & \epsilon_2 \end{pmatrix} \cong \epsilon_2 \begin{pmatrix} \theta & * \\ 0 & 1 \end{pmatrix},$$

where ϵ_1 and ϵ_2 are characters of G_p with values in $\overline{\mathbb{F}}_3^*$ with ϵ_2 unramified as in Theorem 6.3.3, and θ is a characters of G_p such that $\epsilon_1\, \chi_\ell^{k-1} = \epsilon_2\, \theta$. Let us recall that in this case $\epsilon_2(\mathrm{Frob}_p) = f(T_p)$. Since $\overline{\epsilon}|_{G_p} = \epsilon_1\, \epsilon_2$, then

$$\overline{\epsilon}|_{G_p}\, \chi_3^{1-k} = \epsilon_2^2\, \theta,$$

hence the character θ is explicitly determined in terms of $\overline{\epsilon}$ and ϵ_2.

The image of the decomposition group at p, for p odd prime, can be either dihedral or cyclic since the group G_p is solvable. For $p = 2$ the image of the decomposition group is either cyclic, either dihedral, either octahedral or tetrahedral (icosahedral images are not possible since $\mathfrak{A}_5$ is not solvable).

The representation ρ_{f_β}, which is equivalent to $\beta \circ \rho_f$, restricted to the decomposition group at p is such that:

$$\rho_{f_\beta}|_{G_p} \cong \beta \left(\epsilon_2 \begin{pmatrix} \theta & * \\ 0 & 1 \end{pmatrix} \right) = \tau(\epsilon_2) \cdot \rho_2 \begin{pmatrix} \theta & * \\ 0 & 1 \end{pmatrix}.$$

If the image of ρ_f restricted to the decomposition group at p is not abelian, then the representation ρ_{f_β} restricted to the decomposition group at p does not admit any stable line with unramified quotient since the representation ρ_2 is faithful and irreducible. Therefore, in this case $f_\beta(T_p) = 0$.

If ρ_f restricted to the decomposition group at p is reducible and decomposable, it is abelian and $f_\beta(T_p)$ is equal to the eigenvalue of Frob_p which acts on the quotient given by a stable line, so it is equal to $\tau(\epsilon_2(\mathrm{Frob}_p))$. Therefore, $f_\beta(T_p) = \tau(f(T_p))$.

Since $f(T_p) \neq 0$ and p divides n, if ρ_f restricted to the decomposition group at p is decomposable then the character θ is ramified and the conductor of the representation ρ_{f_β} at p is the same as the conductor of the representation ρ_f at p.

Meanwhile, if ρ_f restricted to the decomposition group at p is indecomposable then two different cases can occur. If the character θ is trivial then

$$\rho_{f_\beta}|_{G_p} \cong \tau(\epsilon_2) \cdot \rho_2 \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \cong \tau(\epsilon_2) \cdot \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}$$

where $*$ is a ramified character and α is a character of the decomposition group at p of order 3: this follows applying the representation ρ_2. Hence, we have that $\mathrm{N}_p(\rho_{f_\beta}) = 2$ while $\mathrm{N}_p(\rho_f) = 1$. If the character θ is not trivial then the conductor of the representation ρ_{f_β} at p is the same as the conductor of the representation ρ_f at p.

Let p be a prime dividing n and assume that $f(T_p) = 0$. Then ρ_f restricted to the decomposition group at p is irreducible, so also ρ_{f_β} restricted to the decomposition group at p is irreducible. The image of the representation is not abelian, hence $f_\beta(T_p) = 0$. The conductor of the representation ρ_{f_β} at p is the same as the conductor of the representation ρ_f at p: the stable subspaces for the ramification groups can be either 0-dimensional or 2-dimensional and the representation ρ_2 is faithful.

The only case left is $p = 3$.

If ρ_f restricted to the decomposition group at 3 is unramified then ρ_{f_β} restricted to the decomposition group at 3 is unramified. In this case $f(T_3) \neq 0$ by Theorem 6.3.1 and $\rho_f(\mathrm{Frob}_3)$ has eigenvalues $f(T_3)$ and $\overline{\epsilon}(3)f(T_3)^{-1}$ so

$$f_\beta(T_3) = \tau(f(T_3)) + \tau(\overline{\epsilon}(3)f(T_3)^{-1}),$$

since ρ_{f_β} is unramified at 3. Let us remark that if $f(T_3)$ does not belong to $\mathbb{F}$, the field of definition of the representation, then ρ_f is unramified at 3.

If ρ_f restricted to the decomposition group at 3 is reducible and tamely ramified, that is equivalent to say that ρ_f restricted to G_3 is ramified and decomposable, then $f(T_3) \neq 0$ by Theorem 6.3.1 and

$$\rho_f|_{G_3} \cong \begin{pmatrix} \epsilon_2\theta & 0 \\ 0 & \epsilon_2 \end{pmatrix}$$

with ϵ_2 and θ defined as before. The "peu ramifié" case, see [Ser87, p.186], cannot occur since ρ_f is suppose to be minimal with respect to weight. The character θ is ramified and the weight can only be 2: in this case, in fact, there exists a companion form for f, see [Gro90, Proposition 13.2, 3)]. As in the previous case, we conclude that $f_\beta(T_3) = \tau(f(T_3))$. The valuation of

the conductor of ρ_{f_β} at 3 is then equal to 1 because there exists a stable line for the action of the inertia with unramified quotient.

If ρ_f restricted to the decomposition group at 3 is reducible and wildly ramified, then $f(T_3) \neq 0$ by Theorem 6.3.1 and

$$\rho_f|_{G_3} \cong \epsilon_2 \cdot \begin{pmatrix} \theta & * \\ 0 & 1 \end{pmatrix}$$

with ϵ_2 and θ defined as before. Define $b \in \{1, 2\}$ be the integer such that $\theta|_{I_3} = \chi_3^b$, then by [Edi92, Defiition 4.3, 2(b)] we have that $b = 1$ if $k = 4$ and $b = 2$ if $k = 3$. The image of the representation ρ_f restricted to the decomposition group at 3 is not abelian, then $f_\beta(T_3) = 0$. Moreover, the conductor of the representation ρ_{f_β} at 3 is such that $\mathrm{N}_p(\rho_{f_\beta}) = 2$.

If ρ_f restricted to the decomposition group at 3 is irreducible then $f(T_3) = 0$ by Theorem 6.3.2. The image of the representation ρ_f restricted to the decomposition group at 3 is not abelian, then $f_\beta(T_3) = 0$. The valuation of conductor of the representation ρ_{f_β} at 3 is equal to 2.

From what we have described so far we deduce the following proposition:

Proposition 10.3.1. *Let n and k be two positive integers such that n is not divisible by 3 and $2 \leq k \leq 4$. Let $\epsilon\colon (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character and let $f\colon \mathbb{T}_\epsilon(n, k) \to \overline{\mathbb{F}}_3$ be a morphism of rings. Let us suppose that the representation $\rho_f : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_3)$, attached to f in Corollary 4.0.5, does not arise from lower level or weight, it is irreducible, minimal up to twisting and with octahedral projective image.*

Then there exists a characteristic zero, weight one cuspidal eigenform of level n' such that the reduction mod 3 of the associated Artin representation is equivalent to ρ_f, where n' divides

$$3^i \cdot n \cdot \prod p$$

where the product is taken over the primes p dividing n, such that $f(T_p) \neq 0$ and $\mathrm{N}_p(n) = 1$, and if $f(T_3) \neq 0$ then $i = 0, 1$ or 2 according to $\rho_f|_{G_3}$ being unramified, tamely ramified or wildly ramified otherwise, if $f(T_3) = 0$ then $i = 2$.

Until now we have studied the traces of the representation ρ_{f_β} at the ramified primes. For the unramified primes, we cannot a priori determine uniquely the coefficient, we cannot distinguish elements in $\mathrm{GL}_2(\mathbb{F}_3)$ using only traces and determinants: for example, we cannot distinguish the identity from an element of order 3.

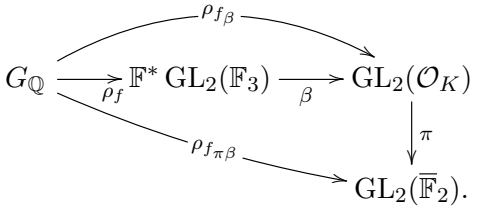
To solve this problem we will list all modular forms with weight one and level given in Proposition 10.3.1 over $\mathcal{O}_K$, the ring of integers of the number fields

where the representation β is defined, and check which one has reduction equal to f. This is possible using [Sch12, Algorithm 7.2.6] which allow us to list a basis for the space of weight one modular forms over $\mathcal{O}_K$ of a given level. To check whether the reduction is the correct one it is enough to check equalities between $f(T_p)$ and the reduced coefficients up to the Sturm bound for cusp forms on $\Gamma_0(n')$ where n' is the level of the characteristic zero form: in this case the reduction is a mod 3 modular form by [Edi97, Lemma 1.9].

The characteristic zero form we obtain in this way can be reduced modulo any odd prime and the image of the Galois representation associated is projectively octahedral.

Let us study the reduction in characteristic 2: we will give a method that can be used instead of [Sch12, Algorithm 7.2.6].

Let π be the reduction map from $\mathcal{O}_K$ to the residue field at 2. By [KW09a, Corollary 10.2], we have that the representation obtained composing ρ_{f_β} with the reduction map π is modular since it is an irreducible continuous representation. Hence, there exist a mod 2 Katz cuspidal eigenform $f_{\pi\beta}$ with associated Galois representation equivalent to $\pi \circ \rho_{f_\beta}$. The following diagram summarizes the setting:



The representation is irreducible, the projective image of ρ_{f_β} is isomorphic to $\mathfrak{S}_4$ and so the kernel of its reduction modulo 2 can only be a 2-power order normal subgroup of $\mathfrak{S}_4$. Therefore, the projective image of $\rho_{f_{\pi\beta}}$ is such that $\mathbb{P}\rho_{f_{\pi\beta}}(G_{\mathbb{Q}}) \cong \mathfrak{S}_3$. Since $\mathfrak{S}_3 \cong \operatorname{GL}_2(\mathbb{F}_2) \cong \operatorname{PGL}_2(\mathbb{F}_2)$, we have that the representation $\rho_{f_{\pi\beta}}$ has not exceptional image, so by Proposition 5.2.2 the image of this representation is a subgroup of $\mathbb{F}'^* \times \operatorname{GL}_2(\mathbb{F}_2)$ where $\mathbb{F}'$ is the field of definition of the representation. By construction it is the field containing the image of the reduction of the character τ through π. Let us remark that, since $\mathcal{O}_K$ is completely explicit once fixed β, also $\mathbb{F}'$ is explicitly computable.

The level of the form $f_{\pi\beta}$ divides the level of the form f_β, see [Car89]. Hence, we can list all forms with the given image and check if the characteristic zero form we have found in the previous step has the desired reduction modulo 2.

In particular, the representation in characteristic 2 distinguishes the conjugacy classes for which it is not possible to decide in characteristic 3: the identity and the Jordan block are sent respectively to a matrix with trace

zero and a matrix with non-zero trace. Since we do not know what is the right choice, we list all possibilities. For each one we get a q-power series expansion in characteristic zero: only one of those is a modular form. We list all systems of eigenvalues in the smallest characteristic co-prime with the level of the form and we exclude all q-power series expansion which do not give by reduction a system of eigenvalues. If the process do not give a unique q-power series expansion then we proceed to the next prime and repeat. We claim that this process concludes. If we are not able to decide then we apply [Sch12, Algorithm 7.2.6] and proceed as explained before.

The following algorithms summarize the construction we have described in this section.

Algorithm 10.3.2 (Companion form for Algorithm 10.3.4)**.** Let n, k be positive integers with 3 not dividing n and $2 \leq k \leq 4$. Let $\epsilon\colon (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character. Let $f\colon \mathbb{T}_\epsilon(n,k) \to \overline{\mathbb{F}}_3$ be a morphism of rings and let $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_3)$ be the representation attached to f in Corollary 4.0.5. Suppose that ρ_f is irreducible, $\mathrm{N}(\rho_f) = n$, minimal with respect to weight and twisting and with octahedral projective image. Let $\overline{\epsilon} : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ be the character defined by $\overline{\epsilon}(a) = f(\langle a \rangle)$ for all $a \in \mathbb{Z}/n\mathbb{Z}^*$.

Input: n, k, $f(T_p)$ for p prime $p \leq B(n,6)$ where B is the Sturm bound for cusp forms for $\Gamma_0(n)$ and weight 6;
Output: 1 if f has a companion form, 0 otherwise.

$v \leftarrow 0$;
if $k \neq 2$ **then**
    return v;
else
    for $g \in S(n, 2, \overline{\epsilon})_{\overline{\mathbb{F}}_3}$ **do**
        if $g(T_p) = pf(T_p)$ for all primes p, different from 3 up to $B(n,6)$ **then**
            Set $v \leftarrow 1$ and **stop**
return v.

Theorem 10.3.3. *Algorithm* 10.3.2 *is correct.*

Proof. The proof of correctness follows from [Gro90, Theorem 13.10]: we are in fact interested only into tamely ramified representations at 3, hence the case $k = 3$ is excluded. Also the case $k = 4$ is excluded because the representation is assumed to be minimal with respect to weight and so it cannot be peu ramifiée. The bound used is the Sturm bound for cusp forms

for $\Gamma_0(n)$ and weight 6 since we are checking the equality between $\theta_\ell g$ and $\theta_\ell^2 f$ for $g \in S(n,2,\overline{\epsilon})_{\overline{\mathbb{F}}_3}$. □

Algorithm 10.3.4 (Octahedral projective image)**.** Let n, k be positive integers with 3 not dividing n and $2 \leq k \leq 4$. Let $\epsilon\colon (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character. Let $f\colon \mathbb{T}_\epsilon(n,k) \to \overline{\mathbb{F}}_3$ be a morphism of rings and let $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_3)$ be the representation attached to f in Corollary 4.0.5. Suppose that ρ_f is irreducible, $\mathrm{N}(\rho_f) = n$, minimal with respect to weight and twisting and with octahedral projective image. Let $\overline{\epsilon} : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ be the character defined by $\overline{\epsilon}(a) = f(\langle a \rangle)$ for all $a \in \mathbb{Z}/n\mathbb{Z}^*$.

Let $\beta : \mathbb{F}^* \cdot \mathrm{GL}_2(\mathbb{F}_3) \to \mathrm{GL}_2(\mathcal{O}_K)$ be a representation given by a character $\tau : \mathbb{F}^* \to \mathbb{Z}[\zeta]^*$, where $\zeta \in \mathbb{C}$ is a root of unity of order equal to the cardinality of $\mathbb{F}^*$, and a faithful representation representation of $\mathrm{GL}_2(\mathbb{F}_3)$, see Table 5.2, which are compatible. The ring $\mathcal{O}_K$ is the ring of integers of the number field over which β is realized.

Input: n, k, β, $f(T_p)$ for p prime $p \leq B(n,k)$ where B is the Sturm bound for cusp forms for $\Gamma_0(n)$ and weight k, $\mathbb{F}$ field of definition of ρ_f;
Output: f_β

$v \leftarrow [\,]$;$N \leftarrow n$;
if $f(T_3) \neq 0$ **then**
  if $f(T_3) \notin \mathbb{F}$ **then**
    $N \leftarrow N$;
  else if Algorithm 10.3.2 return 1 **then**
    $N \leftarrow 3N$;
  else
    $N \leftarrow 3^2 N$;
else
  $N \leftarrow 3^2 N$;
STEP 0:
List all mod 2 modular forms of level N and image contained in $\mathbb{F}'^* \times \mathrm{GL}_2(\mathbb{F}_2)$ where $\mathbb{F}'$ is field containing the image of the reduction of the character τ, i.e. the residue field of $\mathcal{O}_K$ at 2.
List all q-power series expansion in characteristic zero corresponding to the different choices of conjugacy classes corresponding to the different mod 2 forms in the previous list.
List all systems of eigenvalues in the smallest characteristic co-prime with the level of the form and we delete all q-power series expansion which do not give by reduction a system of eigenvalues.
Repeat twice.
if the process give a unique q-power series expansion g **then**
  Add g to v

else
    Run [Sch12, Algorithm 7.2.6] with input $\mathcal{O}_K$ and level N
    Add g to v
for g in v **do**
    if $N = n$ **then**
        if $g(T_3) \neq \tau(f(T_3)) + \tau(\bar{\epsilon}(3)f(T_3)^{-1})$ **then**
            Remove g from v
    else if $N = 3n$ **then**
        if $g(T_3) \neq \tau(f(T_3))$ **then**
            Remove g from v
    else
        if $g(T_3) \neq 0$ **then**
            Remove g from v
    for p prime such that $p \nmid n$ **do**
        if $f(T_p) \neq 0$ **then**
            if $\mathrm{N}_p(\bar{\epsilon}) = \mathrm{N}_p(n)$ **then**
                if $g(T_p) \neq \tau(f(T_p))$ **then**
                    Remove g from v
            else
                if $g(T_p) \neq 0$ **then**
                    Remove g from v
        else
            if $g(T_p) \neq 0$ **then**
                Remove g from v
for g in v **do**
    for λ maximal ideal in $\mathcal{O}_K$ dividing 3 **do**
        Let $\bar{g}$ be the reduction of g mod λ
        for p prime such that $p \nmid 3n$ **do**
            if $f(T_p) \neq \bar{g}(T_p)$ **then**
                Go to the next λ in the cycle and repeat the check,
                if for all λ we are in this case then remove g from v
if $v = [\,]$; **then**
    for p prime dividing n **do**
        if $f(T_p) \neq 0$ and $\mathrm{N}_p(n) = 1$ **then**
            $N \leftarrow Np$
            Repeat from STEP 0
return $f_\beta \leftarrow v$

Theorem 10.3.5. *Algorithm* 10.3.4 *is correct.*

Proof. The Algorithm follows the construction given in the previous section where all the equalities for the coefficients are proved. The form f_β is unique once $\beta \circ \rho_f$ is determined. □

Remark 10.3.6. The construction described depends on the choice of the representation β. In particular, if instead of the representation ρ_2 we choose the representation ρ_3 we get a form which is Galois conjugate to the form we obtain through the construction.

– Projective image isomorphic to $\mathfrak{A}_4$ in characteristic 3

There is a completely analogous construction to the previous for the tetrahedral case, starting with a mod 3 cuspidal eigenform with tetrahedral projective image. Hence, we will not repeat the construction and the algorithm. Let us remark that in this case, the field of definition of the image contains $\mathbb{F}_9$ since the image has to contain a matrix corresponding to the image of a complex conjugation.

Let $\alpha : \mathbb{F}^* \cdot \mathrm{SL}_2(\mathbb{F}_3) \to \mathrm{GL}_2(\mathcal{O}_K)$ be the irreducible 2-dimensional representation given by the choice of τ_2 as representation of $\mathrm{SL}_2(\mathbb{F}_3)$, where τ_1 is given in Table 5.1, and a compatible character $\tau : \mathbb{F}^* \to \mathbb{Z}[\zeta]^*$, defined as in the previous case. The representation α is realized over $\mathcal{O}_K$, which is the ring of integers of a number field which contains the field of definition of τ_2, which is $\mathbb{Q}(\zeta)$ by Table 5.1, and the cyclotomic extension of $\mathbb{Q}$ given by the image of τ. Let us remark that the field K is completely determined from the choice of α.

Proposition 10.3.7. *Let n and k be two positive integers such that n is not divisible by 3 and $2 \leq k \leq 4$. Let $\epsilon\colon (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character and let $f\colon \mathbb{T}_\epsilon(n,k) \to \overline{\mathbb{F}}_3$ be a morphism of rings. Let us suppose that the representation $\rho_f : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_3)$, attached to f in Corollary 4.0.5, does not arise from lower level or weight, it is irreducible, minimal up to twisting and with tetrahedral projective image.*

Then there exists a characteristic zero, weight one cuspidal eigenform of level n' such that the reduction mod 3 of the associated Artin representation is equivalent to ρ_f, where n' divides

$$3^i \cdot n \cdot \prod p$$

where the product is taken over the primes p dividing n, such that $f(T_p) \neq 0$ and $\mathrm{N}_p(n) = 1$, and if $f(T_3) \neq 0$, then $i = 0, 1$ or 2 according to $\rho_f|_{G_3}$ being unramified, tamely ramified or wildly ramified; otherwise, if $f(T_3) = 0$, then $i = 2$.

Using [Sch12, Algorithm 7.2.6], we list all the modular forms with weight one and level given in the previous proposition over $\mathcal{O}_K$, the ring of integers of the number fields where the representation α is defined. Then we check if the reduction is equal to f. It is enough to check equalities between $f(T_p)$ and the reduced coefficients up to the Sturm bound for cusp forms on $\Gamma_0(n')$

where n' is the level of the characteristic zero form: in this case the reduction is a mod 3 modular form by [Edi97, Lemma 1.9].

The characteristic zero form we obtain in this way can be reduced modulo any odd prime and the image of the Galois representation associated is projectively tetrahedral.

Let us study the reduction in characteristic 2. The representation obtained composing ρ_{f_β} with the reduction map is a reducible representation. This follows from the fact that the projective image is isomorphic to a cyclic group of order 3. Hence, the reduction mod 2 of the form obtained has to be reducible. Again we can use the data in characteristic 2 instead of using [Sch12, Algorithm 7.2.6], and use that algorithm only if we cannot conclude.

The construction described depends on the choice of the representation α. If instead of the representation τ_2 we choose the faithful representation τ_3 of $\mathrm{SL}_2(\mathbb{F}_3)$ then we get a form which is Galois conjugate to the form we obtain through the construction since these two representation are Galois conjugate.

– **Projective image isomorphic to $\mathfrak{A}_5$ in characteristic 5**

There is a completely analogous construction and algorithm also for the icosahedral case, starting with a mod 5 cuspidal eigenform with icosahedral projective image. Hence, we will not repeat it.

Let $\gamma : \mathbb{F}^* \cdot \mathrm{SL}_2(\mathbb{F}_5) \to \mathrm{GL}_2(\mathcal{O}_K)$ be the irreducible 2-dimensional representation given by the choice of ι_1 as representation of $\mathrm{SL}_2(\mathbb{F}_5)$, where ι_1 is given in Table 5.3, and a compatible character τ. The representation γ is realized over $\mathcal{O}_K$, which is the ring of integers of a number field which contains the field of definition of ι_1 (which is $\mathbb{Q}(\eta)$ by Table 5.1) and the cyclotomic extension of $\mathbb{Q}$ given by the image of τ.

Proposition 10.3.8. *Let n and k be two positive integers such that n is not divisible by 5 and $2 \leq k \leq 6$. Let $\epsilon\colon (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character and let $f\colon \mathbb{T}_\epsilon(n,k) \to \overline{\mathbb{F}}_5$ be a morphism of rings. Let us suppose that the representation $\rho_f : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_5)$, attached to f in Corollary 4.0.5, does not arise from lower level or weight, it is irreducible, minimal up to twisting and with icosahedral projective image.*

Then there exists a characteristic zero, weight one cuspidal eigenform of level n' such that the reduction mod 5 of the associated Artin representation is equivalent to ρ_f, where n' where n' divides

$$5^i \cdot n \cdot \prod p$$

where the product is taken over the primes p dividing n, such that $f(T_p) \neq 0$ and $\mathrm{N}_p(n) = 1$, and and if $f(T_5) \neq 0$, then $i = 0, 1$ or 2 according to $\rho_f|_{G_5}$ being unramified, tamely ramified or wildly ramified; otherwise, $f(T_p) = 0$ then $i = 2$.

In this case, since $\mathfrak{A}_5 \cong \mathrm{SL}_2(\mathbb{F}_4)$, we have that:

Corollary 10.3.9. *In the same hypotheses of Proposition* 10.3.8*, the reduction mod* 2 *of the Artin representation associated to the the characteristic zero, weight one cuspidal eigenform is equivalent to the Galois representation of a mod* 2 *modular form with projective image isomorphic to* $\mathrm{SL}_2(\mathbb{F}_4)$.

Moreover, if h is the mod 2 modular form in the Corollary, the $\mathrm{Gal}(\mathbb{F}_4/\mathbb{F}_2)$-conjugate form has icosahedral projective image.

Let us remark that, also in this case, the construction depends on the choice of the representation γ. More precisely, choosing the representation ι_2 we get a Galois conjugate of the form we obtain through the construction which uses ι_1.

Chapter 11

Algorithm

In this chapter we describe an algorithm to compute the image of the Galois representation ρ_f, given by Corollary 4.0.5, up to conjugation, as a subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$. We also describe the associate database and the procedure to fill it in, starting from data coming from a given level.

Our goal is to outline an algorithm, which receives as input: n and k positive integers, a prime ℓ such that $(n, \ell) = 1$ and $2 \leq k \leq \ell + 1$, a character $\epsilon\colon (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ and a morphism of rings $f\colon \mathbb{T}_\epsilon(n, k) \to \overline{\mathbb{F}}_\ell$, and which gives as output the image of the Galois representation ρ_f, up to conjugation. Moreover, we want that this algorithm computes the output using the lowest possible number of Hecke operators and their image through the ring morphism f.

Dickson's classification of finite subgroups of $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$ leads us to distinguish cases. Through the previous chapters, we have drawn a parallel between projective images of a given type and equalities between modular forms, and we have seen, case-by-case, that the bound on the number of Hecke operators needed is the Sturm bound of a certain level and weight.

In order to reach our aim in characteristic 3, we need data from characteristic 5 and vice-versa. More in general, in order to compute data in characteristic greater than 5, we need data coming from characteristic 2, 3 and 5. This is due to the projectively exceptional images.

11.1 Database

The aforementioned algorithm is associated to a database which stores the data obtained. Let us briefly explain which information are stored in the database.

Let $\epsilon\colon (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character. As explained in the introduction, the Hecke algebra $\mathbb{T}_\epsilon(n, k)$ is free of finite rank as $\mathbb{Z}$-module, hence, a morphism of rings $f : \mathbb{T}_\epsilon(n, k) \to \overline{\mathbb{F}}_\ell$ can be expressed, using the module structure and the relative multiplication table, giving the image of a basis.

For all triple (n, k, ℓ), where n and k are positive integers, and ℓ is a prime such that $(n, \ell) = 1$ and $2 \leq k \leq \ell + 1$, for which we run the algorithm, in the database are stored data for every morphism of rings $f\colon \mathbb{T}_\epsilon(n, k) \to \overline{\mathbb{F}}_\ell$.

In particular for each f is stored the image of the semi-simple, 2-dimensional Galois representation ρ_f, given by Corollary 4.0.5, up to conjugation. If the representation comes from lower level or weight then we associate to it the form g of minimal level and weight such that $\rho_f \cong \rho_g$.

If the representation does not come from lower level or weight then we store additional data. If it is reducible we store the pair of characters in which it decomposes and also the information of the conductor of the representation. On the other hand, if the representation is irreducible then we store its level as conductor of the representation. Moreover, we run Algorithm 8.2.9 and we store the local data of the representation at the ramified primes. Then we associate to f also all forms of lower level such that a twist of the associated representation is equivalent to ρ_f, using Algorithm 8.2.13.

Any time we run the algorithm for a new level m, we first use the information stored in the database to have data at the level m. In order to do so, we extend the computations done in smaller level i.e. we compute the Hecke operators up to the Sturm bound at the new level expressing them in terms of a $\mathbb{Z}$-basis of the Hecke algebra at the new level.

The following algorithm fills in the database at level m from data coming from level n, with n dividing m.

Algorithm 11.1.1 (Fill in the database: old space and twisting)**.** Let n, m and k be positive integers with n a divisor of m. Let ℓ be a prime not dividing n such that $2 \leq k \leq \ell + 1$. Let $\epsilon\colon (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character. Let $f\colon \mathbb{T}_\epsilon(n,k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings and let $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the representation attached to f in Corollary 4.0.5. Let $\overline{\epsilon} : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ be the character defined by $\overline{\epsilon}(a) = f(\langle a \rangle)$ for all $a \in \mathbb{Z}/n\mathbb{Z}^*$.

Input: n, k, ℓ, ϵ, $f(T_p)$ for p prime $p \leq B(m,k)$ where $B(m,k)$ is the is the Sturm bound for cusp forms for $\Gamma_0(m)$ and weight k;
Output: L list of systems of eigenvalues coming from f from level n to level m also by twisting.

$L_1 \leftarrow [\,]$; $L_2 \leftarrow [\,]$;
STEP 1: fill in the "old-space" coming from f
Run Algorithm 6.4.4
Store the output in L_1
STEP 2: twists of f
for p prime dividing m **do**
    if p divides n **then**
        Using the output of Algorithm 8.2.9, which is stored in the database, find the set of non-trivial Dirichlet characters χ such that $\mathrm{N}(\rho_f \otimes \chi)$ is equal to m: the formulas to compute the conductor of $\rho_f \otimes \chi$ are given in Chapter 8

Compute the systems of eigenvalues corresponding to $\rho_f \otimes \chi$ at level m using Proposition 8.2.5 and 8.2.6
Check for companion forms using the explanation in Chapter 8, Section 8.3
Store each systems of eigenvalues in L_2

return $L \leftarrow [L_1, L_2]$

Theorem 11.1.2. *Algorithm* 11.1.1 *is correct.*

Proof. The proof of correctness follows from the fact that Algorithm 6.4.4 and Algorithm 8.2.9 are correct. □

Using the previous algorithm we set the following preliminary checks in order to verify that a 2-dimensional Galois representation ρ_g, attached to a modular form $g \in S(m,k)_{\overline{\mathbb{F}}_\ell}$ with m and k positive integers and ℓ prime, not dividing n, and such that $2 \leq k \leq \ell + 1$, does not arise from lower level or weight:

Preliminary check 1
if $g(T_p)$ for p prime $p \leq B(m,k)$, where $B(m,k)$ is the is the Sturm bound for cusp forms for $\Gamma_0(m)$ and weight k, is in the database i.e. it is an element of the list $L[0]$ from the list L given as output from Algorithm 11.1.1 **then**
Check in the database the image of the form g and return it as output; store the data and **end** the Algorithm.

Preliminary check 2
if $g(T_p)$ for p prime $p \leq B(m,k)$, where $B(m,k)$ is the is the Sturm bound for cusp forms for $\Gamma_0(m)$ and weight k, is in the database i.e. in $L[1]$ from the list L given as output from Algorithm 11.1.1 **then**
Check in the database the projective image of the representation and set it as H

Similarly we want to fill in the database using the construction given for projectively exceptional images:

Algorithm 11.1.3 (Fill in the database: projectively exceptional images)**.** Let n, k be positive integers. Let ℓ be a prime not dividing n such that $2 \leq k \leq \ell + 1$.

Input: n, k, ℓ, ϵ, $B(n,k)$, the Sturm bound for cusp forms for $\Gamma_0(n)$, weight

k;
Output: L_3 list of systems of eigenvalues with projectively exceptional images.

$L_3 \leftarrow [\,]$;
if $\ell \neq 3, 5$ **then**
Check in the database if there exist mod 3 modular forms with projective image isomorphic to $\mathfrak{S}_4$, level n', where n' is the level n away from 3, weight k and character equal to the restriction of ϵ to n'. Let L be the list of such forms.
for $g \in L$ **do**
for β admissible representation as in Chapter 10 **do**
Run Algorithm 10.3.4
Reduce f_β, the characteristic zero weight one cuspidal eigenform obtained as output modulo ℓ
Store the data in the database: store the system of eigenvalues up to $B(n,k)$ in L_3 and for each of these set $H \leftarrow \mathfrak{S}_4$
Proceed in analogous way for tetrahedral and icosahedral projective image and if it is the case set $H \leftarrow \mathfrak{A}_4$ or $H \leftarrow \mathfrak{A}_5$

else if $\ell = 3$ **then**
Check in the database if there exist mod 5 modular forms with projective image isomorphic to $\mathfrak{A}_5$, level n', where n' is the level n away from 5, weight k and character equal to the restriction of ϵ to n'.
Proceed in analogous way as for octahedral projective image and if it is the case set $H \leftarrow \mathfrak{A}_5$
else if $\ell = 5$ **then**
Check in the database if there exist mod 3 modular forms with projective image isomorphic to $\mathfrak{A}_4$ or $\mathfrak{S}_4$, level n', where n' is the level n away from 3, weight k and character equal to the restriction of ϵ to n'.
Proceed in analogous way as the octahedral projective image case for $\ell \neq 3, 5$ and if it is the case set $H \leftarrow \mathfrak{S}_4$ or $H \leftarrow \mathfrak{A}_4$

Theorem 11.1.4. *Algorithm* 11.1.3 *is correct.*

Proof. Algorithm 11.1.3 is divided into three cases according to the characteristic.

In characteristic 3, as we have already remarked, octahedral and tetrahedral projective images are not exceptional images. In Remark 5.1.4, we underlined that in characteristic 3 if the projective image is isomorphic to $\mathfrak{A}_4$ or $\mathfrak{S}_4$

then the field of definition of the projective representation if $\mathbb{F}_3$, while if it is icosahedral then the field of definition of the projective representation is $\mathbb{F}_9$. Hence, in characteristic 3 we can distinguish between octahedral or tetrahedral projective image on the one hand and icosahedral type on the other hand. Therefore, we use this data in characteristic 5 to distinguish between octahedral or tetrahedral projective image and not exceptional.

In characteristic 5 the field of definition of the projective image for projectively exceptional representations is $\mathbb{F}_5$, see Remark 5.1.4. Using the construction given in Chapter 10, we can check if a representation with $\mathbb{F}_5$ as field of definition for the projective image has projectively exceptional image or not. Hence, we decide if a representation has projective image $\mathrm{SL}_2(\mathbb{F}_5)/\{\pm 1\} \cong \mathfrak{A}_5$ or not, and using this datum we can apply the construction given in Chapter 10 to the icosahedral projective representations and distinguish icosahedral representations in characteristic 3. For characteristic larger than 5 we proceed using the data in characteristic 3 and 5, with additional information from characteristic 2, as shown in the construction of Chapter 10, Section 10.3. □

11.2 Algorithm

In this section we give the outline of the algorithm which is the aim of this part of the thesis:

Algorithm 11.2.1 (Image of the Galois representation ρ_f up to conjugation as a subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$)**.** Let n, k be positive integers. Let ℓ be a prime not dividing n such that $2 \leq k \leq \ell+1$. Let $\epsilon\colon (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character. Let $f\colon \mathbb{T}_\epsilon(n,k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings and let $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the representation attached to f in Corollary 4.0.5. Let $\overline{\epsilon} : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ be the character defined by $\overline{\epsilon}(a) = f(\langle a \rangle)$ for all $a \in \mathbb{Z}/n\mathbb{Z}^*$.

Input: n, k, ℓ, ϵ, $f(T_p)$ for p prime $p \leq B(n,k)$ where $B(n,k)$ is the is the Sturm bound for cusp forms for $\Gamma_0(n)$ and weight k;
Output: image of the Galois representation ρ_f up to conjugation as a subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ and store data in the database

---

STEP 1: reduction of the weight
if $k = \ell + 1$ **then**
    Run Algorithm 6.4.1
    if the output of Algorithm 6.4.1 is 0 **then**
        Proceed to **STEP 2**
    else

Check in the database the image of the form in weight 2 given by Algorithm 6.4.1, **return** it as output and **store** the data **end** the algorithm

else

Proceed to **STEP 2**

STEP 2: reduction of the level
Run **Preliminary check 1**
if the algorithm does not terminate go to **STEP 3**

STEP 3: check if the representation is reducible
Run Algorithm 7.2.4
if the output of Algorithm 7.2.4 is 0 **then**

Proceed to **STEP 4**

else

return the output of Algorithm 7.2.4, **store** the data
end the algorithm

STEP 4: determine the minimal field of definition $\mathbb{F}$ of the representation using Proposition 9.1.1;

STEP 5: minimality up to twisting:
Run Algorithm 8.2.15
if the output of Algorithm 8.2.15 is 1 **then**

Proceed to **STEP 6**

else

Run **Preliminary check 2**
Proceed to **STEP 11**

STEP 6: determine the minimal field of definition $\mathbb{F}'$ of the projective representation
Run Algortihm 9.2.3

STEP 7: preliminary check big image
for p prime dividing n **do**

if $f(T_p) \neq 0$ and $\mathrm{N}_p(n) = 1 + \mathrm{N}_p(\bar{\epsilon})$ **then**

Set $H \leftarrow$ large
Go to **STEP 11**

STEP 8: check if the projective representation is dihedral
Run Algorithm 10.1.3
if the output of Algorithm 10.1.3 is 0 **then**

Proceed to **STEP 9**

else

Let α be the output of Algorithm 10.1.3
Set $H \leftarrow [\mathrm{dih}, \alpha]$
Go to **STEP 11**

STEP 9: preliminary check projectively exceptional image
if $\ell > k$ **then**
if $f(T_\ell) \neq 0$ and $\ell > 4k - 3$ **then**
Set $H \leftarrow$ large
Go to **STEP 11**
if $f(T_\ell) = 0$ and $\ell > 4k - 5$ **then**
Set $H \leftarrow$ large
Go to **STEP 11**
if $\ell \geq 5$ **then**
for p prime, $p \leq B(n,k)$ **do**
Set $u \leftarrow f(T_p)^2 / f(\epsilon(p)) p^{k-1}$
if $u \notin \{0,1,2,4\}$ and $u^2 - 3u + 1 \neq 0$ **then**
Set $H \leftarrow$ large
Go to **STEP 11**
else
Change p and continue the cycle

STEP 10: check if the representation is projectively exceptional
Check if the system of eigenvalues occurs in the list L_3 given as output by Algorithm 11.1.1 up to $B(n,k)$
if the system of eigenvalues occurs in the list L_3 **then**
Set $H \leftarrow \mathfrak{S}_4$ or $\mathfrak{A}_4$, or $\mathfrak{A}_5$, according to the data
Go to **STEP 11**
else
Set $H \leftarrow$ large
Go to **STEP 11**

STEP 11: determination of the image up to conjugation as a subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$
Compute D the set of determinants of the representation
if $H =$ large **then**
if D is a subset of $(\mathbb{F}^*)^2$ **then**
The image is computed using Proposition 5.2.1 and the fields $\mathbb{F}$, $\mathbb{F}'$
else
The image is computed using Proposition 5.2.2 and the fields $\mathbb{F}$, $\mathbb{F}'$
else if $H = \mathfrak{A}_4$ **then**
The image is computed using Proposition 5.2.4 and the fields $\mathbb{F}$, $\mathbb{F}'$
else if $H = \mathfrak{S}_4$ **then**

The image is computed using Proposition 5.2.6 and the fields $\mathbb{F}$, $\mathbb{F}'$
else if $H = \mathfrak{A}_5$ **then**
The image is computed using Proposition 5.2.8 and the fields $\mathbb{F}$, $\mathbb{F}'$
else
Compute the order of the cyclic subgroup using [Ser77b, (7.2.1)] and compute the image according to Chapter 5
store data in the database

Theorem 11.2.2. *Algorithm* 11.2.1 *is correct.*

Proof. Almost all the steps are described in the previous chapters of this part of the thesis. STEP 7 is stated in Remark 8.1.6.

The first part of STEP 9 follows from [BD12, Lemma 1.1]: if the image is projectively exceptional then there cannot exist elements of the projective image with order larger than 5 (icosahedral case), so, in particular, the image of the inertia subgroup at ℓ, given in Theorem 6.3.1 and Theorem 6.3.2, cannot have order larger than 5.

If $f(T_\ell) \neq 0$ the image of the representation restricted to the inertia at ℓ is cyclic and isomorphic to the image of χ_ℓ^{k-1} which has order larger than 5 for $\ell > 4k-3$. On the other hand, if $f(T_\ell) = 0$ the image of the representation restricted to the inertia at ℓ has order $(\ell+1)/\gcd(\ell+1, k-1)$, so larger than 5 for $\ell > 4k-5$. The second part follows from [Ser72, Proposition 19] and Remark 5.1.5: it states again that elements cannot have order larger than 5 for projectively exceptional representations. □

Remark 11.2.3. In all aforedescribed algorithms the Sturm bound plays a deep and central role: it is used to guarantee equalities of mod ℓ modular forms after checking a finite amount of equalities. Let n and k be positive integers such that ℓ does not divide n and $2 \leq k \leq \ell + 1$ then the Sturm bound for $\Gamma_0(n)$ is such that:

$$B(n,k) = \frac{k[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(n)]}{12} = \frac{k}{12} \cdot n \cdot \prod_{p|n \text{ prime}} \left(1 + \frac{1}{p}\right) \ll \frac{k}{12} \cdot n \log\log n.$$

Remark 11.2.4. Only in STEP 3 it could be needed to compute more operators than the Sturm bound for $\Gamma_0(n)$ and weight k. In this step, in fact, it could be needed to compute operators up to the Sturm bound for $\Gamma_0(nq^2)$ and weight k, where q is the smallest odd prime not dividing n, or $\Gamma_0(n)$ and weight $k + \ell + 1$. Let us remark that in both cases we still need to compute less operators than in the approach presented in Chapter 6 using degeneracy maps.

Appendix A

Minimal level of realization

The aim of this appendix is to analyse degeneracy maps between modular curves. In the next sections are presented results similar to the ones obtained in [Edi06], where the action of Frobenius and multiplication by the Hasse invariant on Katz modular forms are studied. In particular, from this we deduce statements on residual modular Galois representations and their level of realization. This appendix is based on the theory of Katz modular forms, see [Kat73], [Kat77] and [Edi92], and modular curves, see [KM85] and [Gro90].

Let us recall that also in [DS05, Section 5.7] there is a detailed explanation about degeneracy maps between modular curves over $\overline{\mathbb{Q}}$ and are obtained similar results to the ones that we prove in this appendix, see [DS05, Theorem 5.7.1 (Main Lemma)]. The statement of [DS05, Theorem 5.7.1 (Main Lemma)] is proved through a reduction to linear algebra and representation theory: in particular, the first step is to change the congruence subgroups in order to pass from degeneracy maps to inclusions, see [DS05, p.191]. In this appendix, instead, we focus on the study of modular curves over finite fields and on a geometric interpretation of degeneracy maps.

A.1 Notations and preliminaries

For n, k positive integers, ℓ prime not dividing n and $\overline{\mathbb{F}}_\ell$ an algebraic closure of $\mathbb{F}_\ell$, let $M(\Gamma_1(n),k)_{\overline{\mathbb{F}}_\ell}$ be the space of Katz modular forms of weight k for $\Gamma_1(n)$ on $\overline{\mathbb{F}}_\ell$. Let $S(\Gamma_1(n),k)_{\overline{\mathbb{F}}_\ell}$ be the subspace of $M(\Gamma_1(n),k,\epsilon)_{\overline{\mathbb{F}}_\ell}$ whose elements have q-expansions that are power series with constant term zero at all cusps.

For any character $\epsilon\colon (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$, let $S(\Gamma_1(n),k,\epsilon)_{\overline{\mathbb{F}}_\ell}$ be the space of Katz cusp forms of weight k for $\Gamma_1(n)$ and character ϵ:

$$S(\Gamma_1(n),k,\epsilon)_{\overline{\mathbb{F}}_\ell} := \{f \in S(\Gamma_1(n),k)_{\overline{\mathbb{F}}_\ell} \,|\, \forall d \in (\mathbb{Z}/n\mathbb{Z})^*,\ \langle d\rangle f = \epsilon(d) f\}.$$

If $n = mp^r$ with $r \geq 1$ and p not dividing m, we will "split" the level structure accordingly, and denote the space as $S(\Gamma_1(m),\Gamma_1(p^r),k,\epsilon_m,\epsilon_p)_{\overline{\mathbb{F}}_\ell}$, but, in order to shorten the notation, we will write $S(m,p^r,k,\epsilon)_{\overline{\mathbb{F}}_\ell}$ instead. We will use analogous notation for modular curves.

If $n>4$, then $S(\Gamma_1(n),k)_{\overline{\mathbb{F}}_\ell}$ is isomorphic to $\mathrm{H}^0(X_1(n)_{\overline{\mathbb{F}}_\ell},\omega^{\otimes k}(-\mathrm{Cusps}))$, the space of global sections of the line bundle $\omega^{\otimes k}(-\mathrm{Cusps})$, while the space of Katz modular forms $M(\Gamma_1(n),k)_{\overline{\mathbb{F}}_\ell}$ is isomorphic to $\mathrm{H}^0(X_1(n)_{\overline{\mathbb{F}}_\ell},\omega^{\otimes k})$, see [Gro90, Proposition 2.2].

Let us recall some useful concepts and notations. Given a modular curve $X_1(n)_{\overline{\mathbb{F}}_\ell}$ with $(n,\ell)=1$, if $n=mp^r$ with $r\geq 1$ and p not dividing m, we have two degeneracy maps B_p and α:

$$\begin{array}{ccc} & X_1(m,p^r)_{\overline{\mathbb{F}}_\ell} & \\ {\scriptstyle B_p}\swarrow & & \searrow{\scriptstyle \alpha} \\ X_1(m,p^{r-1})_{\overline{\mathbb{F}}_\ell} & & X_1(m,p^{r-1})_{\overline{\mathbb{F}}_\ell}. \end{array} \tag{A.1}$$

Using the moduli interpretation for $X_1(n)_{\overline{\mathbb{F}}_\ell}$, i.e. considering E/S, an elliptic curve over an $\overline{\mathbb{F}}_\ell$-scheme S, with P and Q respectively points of order m and p^r, we give the following description of the degeneracy maps: α is the forgetful map $\alpha\colon (E,P,Q)\longmapsto(E,P,pQ)$ and B_p is the p-th degeneracy map defined by $B_p\colon (E,P,Q)\mapsto(E/\langle p^{r-1}Q\rangle,\beta(P),\beta(Q))$, where

$$\langle p^{r-1}Q\rangle \rightarrowtail E \xrightarrow{\beta} E/\langle p^{r-1}Q\rangle$$

is the degree p isogeny whose kernel is generated by $p^{r-1}Q$.

Let us fix ζ_{p^r} a root of unity of order p^r in $\overline{\mathbb{F}}_\ell$. The Atkin-Lehner map $w_{\zeta_{p^r}}$ on $X_1(n)_{\overline{\mathbb{F}}_\ell}$ is defined as follows:

$$\begin{array}{ccc} X_1(n)_{\overline{\mathbb{F}}_\ell} & \xrightarrow{w_{\zeta_{p^r}}} & X_1(n)_{\overline{\mathbb{F}}_\ell} \\ (E,P,Q) & \longmapsto & (E/\langle Q\rangle,\beta_r(P),Q') \end{array} \tag{A.2}$$

where β_r is the degree p^r isogeny whose kernel is generated by Q, and where Q' belongs to $\ker(\beta_r^t)(S)$:

$$\langle Q\rangle \rightarrowtail E \underset{\beta_r^t}{\overset{\beta_r}{\rightleftarrows}} E/\langle Q\rangle \twoheadleftarrow \langle Q'\rangle$$

and it is the unique element such that $e_\beta(Q,Q')=\zeta_{p^r}$, where e_β is the Weil pairing related to β i.e. the perfect μ_{p^r} valued pairing between $\ker(\beta)$ and $\ker(\beta^t)$, see [KM85, Section 2.8].

Let us recall basic facts about Tate curves. Precise results can be found in [DR73, Chapter VII], see also [Sil94, Chapter V] for a more elementary and explicit approach.

For every positive integer d, the d-th Tate curve is a certain generalized elliptic curve $\mathrm{Tate}(q^d)\to\operatorname{Spec}\mathbb{Z}[[q]]$ that becomes a Néron d-gon after

base change to the zero locus of q and that is a smooth elliptic curve over $\operatorname{Spec}\mathbb{Z}[[q]][q^{-1}]$, the complement of this zero locus.

Let d, e and n be positive integers such that n is the least common multiple of d and e. Then the curve $\mathrm{Tate}(q^d)$ over $\operatorname{Spec}\mathbb{Z}[[q,\zeta_e]]$, where ζ_e is a e-th root of unity, admits a $\Gamma_1(n)$-structure. Each choice of d, e and of the a $\Gamma_1(n)$-structure gives rise to an injective map from $M(\Gamma_1(n),k)_{\overline{\mathbb{F}}_\ell}$ to $\overline{\mathbb{F}}_\ell \otimes_{\mathbb{Z}} \mathbb{Z}[[q,\zeta_e]]$, which is called the q-expansion map relative to $\mathrm{Tate}(q^d)$ with the given $\Gamma_1(n)$-structure. The $\Gamma_1(n)$-structure on $\mathrm{Tate}(q^n)$ over $\operatorname{Spec}\mathbb{Z}[[q]]$ given by $\psi(i) = q^i$ for $i \in \mathbb{Z}/n\mathbb{Z}$, gives rise to a particular q-expansion called the q-expansion at ∞, see [KM85, Sections 8.8 and 8.11] for explanation. For any $f \in M(\Gamma_1(n),k)_{\overline{\mathbb{F}}_\ell}$ we define $a_m(f)$ to be the m-th coefficient in this q-expansion.

A.2 Level lowering for Katz cusp forms

Main Lemma 1. *Let n and k be positive integers. Let ℓ and p be primes such that p strictly divides n and $n/p > 4$, while ℓ does not divide n and $1 \leq k \leq \ell+1$. Let f be a* mod ℓ *cusp form in $S(n/p,p,k)_{\overline{\mathbb{F}}_\ell}$ such that*

$$f(\mathrm{Tate}(q),\zeta_{n/p},\zeta_p) = \sum_{j\geq 1} a_j(f) q^j \left(\frac{dt}{t}\right)^{\otimes k} \in \overline{\mathbb{F}}_\ell[[q^p]] \left(\frac{dt}{t}\right)^{\otimes k}, \qquad \text{(A.3)}$$

where $\zeta_{n/p}$ and ζ_p are respectively n/p-th and p-th roots of unity. Then there exists a unique modular form $g \in S(n/p,k)_{\overline{\mathbb{F}}_\ell}$, such that $B_p^* g = f$, where B_p^* is the morphism induced by $B_p\colon X_1(n)_{\overline{\mathbb{F}}_\ell} \to X_1(n/p)_{\overline{\mathbb{F}}_\ell}$, the p-th degeneracy map.

Proof. Since p strictly divides n, let us write $n = mp$. Hypothesis (A.3) means that the q-expansion of f at the cusp at ∞ is such that $a_j(f) = 0$ for all positive integers j not divisible by p.

As $m > 4$ by hypothesis, f is an element of $\mathrm{H}^0(X_1(n)_{\overline{\mathbb{F}}_\ell}, \omega^{\otimes k}(-\mathrm{Cusps}))$, hence, using known relations and correspondences between modular curves, we have the following commutative diagram:

$$\begin{array}{ccc} X_1(n)_{\overline{\mathbb{F}}_\ell} & \xrightarrow{w_{\zeta_p}} & X_1(n)_{\overline{\mathbb{F}}_\ell} \\ {\scriptstyle B_p}\downarrow & & \downarrow{\scriptstyle \alpha} \\ X_1(m)_{\overline{\mathbb{F}}_\ell} & = & X_1(m)_{\overline{\mathbb{F}}_\ell} \end{array}$$

where B_p and α are the degeneracy maps defined in (A.1) and w_{ζ_p} is the Atkin-Lehner map associated to the isogeny β, defined in (A.2). The isogeny

β induces a morphism β^* from the line bundle $\omega^{\otimes k}(-\text{Cusps})$ on $X_1(m)_{\overline{\mathbb{F}}_\ell}$ to the line bundle $\omega^{\otimes k}(-\text{Cusps})$ on $X_1(n)_{\overline{\mathbb{F}}_\ell}$, because for each $(E/S, P, Q)$ we have an isomorphism of invertible O_S-modules β^* between $\omega_{E/\langle Q\rangle}$ and ω_E. Similarly, we define $w^*_{\zeta_p} : S(n,k)_{\overline{\mathbb{F}}_\ell} \to S(n,k)_{\overline{\mathbb{F}}_\ell}$ by

$$(w^*_{\zeta_p} h)(E,P,Q) = \beta^*(h(w_{\zeta_p}(E,P,Q))) = \beta^*(h(E/\langle Q\rangle, \beta(P), Q')),$$

where h belongs to $S(n,k)_{\overline{\mathbb{F}}_\ell}$, see [Gro90, Section 6]. In particular, it follows from the construction that there exists a unique $f' \in S(n,k)_{\overline{\mathbb{F}}_\ell}$ such that $w^*_{\zeta_p} f' = f$. In fact, let us consider the q-expansion at the cusp at ∞:

$$\begin{aligned}
(w^*_{\zeta_p} f')(\infty) &= (w^*_{\zeta_p} f')(\mathrm{Tate}(q), \zeta_m, \zeta_p) = \beta^*(f'(\infty')) = \\
&= \beta^*(f'(\mathrm{Tate}(q^p), \zeta_m^p, q)) = \beta^* \left(\sum_{j\geq 1} a_j(f') q^j \left(\frac{dt}{t}\right)^{\otimes k} \right) = \\
&= \left(\sum_{j\geq 1} a_j(f') q^j \right) p^k \left(\frac{dt}{t}\right)^{\otimes k}
\end{aligned}$$

where $\infty' := w_{\zeta_p}(\infty)$ and the last equality follows from:

$$\mu_p \rightarrowtail \mathrm{Tate}(q) \xrightarrow{\beta} \mathrm{Tate}(q^p)$$

hence $\beta^*((dt)/t) = p((dt)/t)$. Since $f(\mathrm{Tate}(q), \zeta_m, \zeta_p) \in \overline{\mathbb{F}}_\ell\,[[q^p]]\,((dt)/t)^{\otimes k}$ we deduce that for all positive integer j we have $a_j(f')p^k = a_j(f)$ and

$$f'(\mathrm{Tate}(q^p), \zeta_m^p, q) \in \overline{\mathbb{F}}_\ell\,[[q^p]] \left(\frac{dt}{t}\right)^{\otimes k}.$$

In order to prove that f comes from $X_1(m)_{\overline{\mathbb{F}}_\ell}$ via B_p^*, it is enough to show that f' does via α. To prove this claim, we study to the following diagram of modular curves:

$$\begin{array}{ccc}
X(\Gamma_1(m), \Gamma(p)^{\zeta_p - \mathrm{can}})_{\overline{\mathbb{F}}_\ell} & (E,P,Q_1,Q_2) & (\mathrm{Tate}(q^p), \zeta_m^p, q, \zeta_p) \\
\downarrow{\scriptstyle \gamma} & \downarrow & \downarrow \\
X(\Gamma_1(m), \Gamma_1(p))_{\overline{\mathbb{F}}_\ell} & (E,P,Q_1) & (\mathrm{Tate}(q^p), \zeta_m^p, q) \\
\downarrow{\scriptstyle \alpha} & \downarrow & \downarrow \\
X(\Gamma_1(m))_{\overline{\mathbb{F}}_\ell} & (E,P) & (\mathrm{Tate}(q^p), \zeta_m^p)
\end{array}$$

where Q_1, Q_2 are such that $e_p(Q_1,Q_2) = \zeta_p$, and α, γ are both forgetful maps.

On $X(\Gamma_1(m),\Gamma(p)^{\zeta_p-\mathrm{can}})_{\overline{\mathbb{F}}_\ell} \to X(\Gamma_1(m))_{\overline{\mathbb{F}}_\ell}$ there is the natural $\mathrm{SL}_2(\mathbb{F}_p)$ action, given by the action of $\mathrm{SL}_2(\mathbb{F}_p)$ on $\Gamma(p)^{\zeta_p-\mathrm{can}}$. This action is trivial on $X(\Gamma_1(m))_{\overline{\mathbb{F}}_\ell}$.

In the following diagram we describe the action of $\mathrm{SL}_2(\mathbb{F}_p)$:

$$\begin{array}{ccc} & & X(\Gamma_1(m),\Gamma(p)^{\zeta_p-\mathrm{can}})_{\overline{\mathbb{F}}_\ell} \\ & & \Big\downarrow \left(\begin{smallmatrix}1 & *\\ 0 & 1\end{smallmatrix}\right) \\ \mathrm{SL}_2(\mathbb{F}_p) & \circlearrowright & X(\Gamma_1(m),\Gamma_1(p))_{\overline{\mathbb{F}}_\ell} \\ & & \Big\downarrow \\ & & X(\Gamma_1(m))_{\overline{\mathbb{F}}_\ell} \end{array}$$

Taking into account this action, there exists $g \in S(m,k)_{\overline{\mathbb{F}}_\ell}$ such that $B_p^* g = f$ if and only if $\gamma^* f'$ is $\mathrm{SL}_2(\mathbb{F}_p)$-invariant.

The map $\gamma : X(\Gamma_1(m),\Gamma(p)^{\zeta_p-\mathrm{can}})_{\overline{\mathbb{F}}_\ell} \to X(\Gamma_1(m),\Gamma(p))_{\overline{\mathbb{F}}_\ell}$ corresponds to the action of elements of the form $\left(\begin{smallmatrix}1 & *\\ 0 & 1\end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{F}_p)$ and $\gamma^* f'$ is invariant under the action of $\left(\begin{smallmatrix}1 & *\\ 0 & 1\end{smallmatrix}\right)$ by construction. Since $\{\left(\begin{smallmatrix}1 & 0\\ * & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & *\\ 0 & 1\end{smallmatrix}\right)\}$ generate $\mathrm{SL}_2(\mathbb{F}_p)$, and $\left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)$ generates the subgroup $\left(\begin{smallmatrix}1 & 0\\ * & 1\end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbb{F}_p)$, in order to conclude it is enough to prove that $\gamma^* f'$ is invariant under the action of $\left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)$.

Let us remark that $\left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)$ fixes $\infty' \in X(\Gamma_1(m),\Gamma(p)^{\zeta_p-\mathrm{can}})_{\overline{\mathbb{F}}_\ell}$ and it acts on the complete local ring at ∞', $\overline{\mathbb{F}}_\ell[[q]]$, as:

$$\begin{cases} \text{identity on } \overline{\mathbb{F}}_\ell \\ q \mapsto \zeta_p q \end{cases}.$$

It follows that $\left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)$ acts on $\overline{\mathbb{F}}_\ell[[q]](dt/t)^{\otimes k}$ by $t \mapsto t$, by definition, and, hence, $(dt/t)^{\otimes k} \mapsto (dt/t)^{\otimes k}$. As $a_j(f') = 0$ for all positive integers j not divisible by p, then $\left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)^* f'$ has the same q-expansion as f'.

Since $X(\Gamma_1(m),\Gamma(p)^{\zeta_p-\mathrm{can}})_{\overline{\mathbb{F}}_\ell}$ is an irreducible and reduced curve, this means that $\left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)^* \gamma^* f' = \gamma^* f'$.

The modular form $g \in S(m,k)_{\overline{\mathbb{F}}_\ell}$ such that $B_p^* g = f$ is unique: this follows because, from the one hand, pullback does not change q-expansions and, on the other hand, the q-expansion principle holds, see [Kat73, Section 1.12]. □

Lemma A.2.1. *Given $r \in \mathbb{Z}_{>0}$ and a prime p, the set*

$$\left\{ \begin{pmatrix} 1 & 0 \\ p^r & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\} \subset \mathrm{SL}_2(\mathbb{Z}/p^{r+1}\mathbb{Z})$$

generates the subgroup

$$\overline{\Gamma_1(p^r)} := \left\{ \begin{pmatrix} 1+p^r a & b \\ p^r c & 1+p^r d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/p^{r+1}\mathbb{Z}) \right\}.$$

Proof. We will show that every matrix in $\overline{\Gamma_1(p^r)}$ can be written as a finite product of $\left(\begin{smallmatrix} 1 & 0 \\ p^r & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Let $\left(\begin{smallmatrix} 1+p^r a & b \\ p^r c & 1+p^r d \end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbb{Z}/p^{r+1}\mathbb{Z})$, with $a, b, c, d \in \mathbb{F}_p$, by direct computation in $\mathrm{SL}_2(\mathbb{Z}/p^{r+1}\mathbb{Z})$ we get:

$$\begin{pmatrix} 1+p^r a & b \\ p^r c & 1+p^r d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ p^r & 1 \end{pmatrix}^{c-1} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{a} \begin{pmatrix} 1 & 0 \\ p^r & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{(p^r a-1)(a-b)}.$$

Let us remark that the computation is done by multiplying the matrix $\left(\begin{smallmatrix} 1+p^r a & b \\ p^r c & 1+p^r d \end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbb{Z}/p^{r+1}\mathbb{Z})$ on the left and on the right by powers of $\left(\begin{smallmatrix} 1 & 0 \\ p^r & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ in order to obtain the identity matrix. In particular, for $m \in \mathbb{Z}$, multiplying by $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)^m$

– on the left means add m-times the first column to the second;
– on the right means add m-times the second row to the first;

and multiplying by $\left(\begin{smallmatrix} 1 & 0 \\ p^r & 1 \end{smallmatrix}\right)^m$

– on the left is equal to change the elements of the second row respectively multiplying by p^r the sum of the first element of the second row and m, adding mp^r times the second element of the first row to the second element of the second row;
– on the right is equal to change the elements of the first column respectively adding mp^r times the first element of the second column to the first element of the column; and multiplying by p^r the sum of the second element of the column and m.

□

Lemma A.2.2. *Let E/S be an elliptic curve over an $\overline{\mathbb{F}}_\ell$-scheme S, $r \geq 1$ an integer, p be a prime different from ℓ and*

$$E \xrightarrow[\beta_1]{} E/\langle p^r Q\rangle \xrightarrow[\beta_r]{} E/\langle Q\rangle, \qquad E \xrightarrow{\beta_{r+1}} E/\langle Q\rangle$$

the standard factorization of a cyclic p^{r+1}-isogeny into a cyclic p-isogeny followed by a cyclic p^r-isogeny, where Q is a point of order p^{r+1}. Let Q_{r+1} and Q_r be the unique points that normalize the Weil pairings: $e_{\beta_{r+1}}(Q, Q_{r+1}) = \zeta_{p^{r+1}}$ and $e_{\beta_r}(\beta_1(Q), Q_r) = \zeta_{p^r}$. Then

$$Q_r = pQ_{r+1}.$$

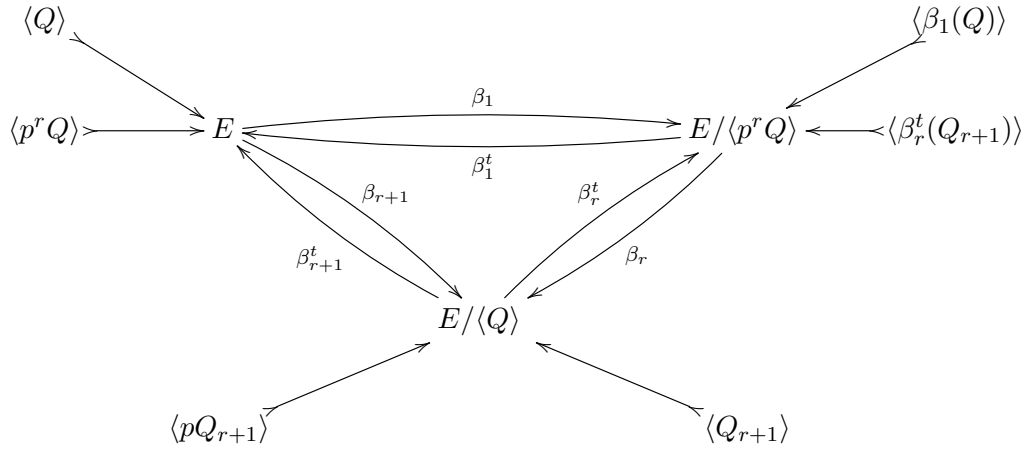
Proof. First of all, we apply the "Backing-up Theorem", see [KM85, 6.7.11], to the isogeny β_{r+1} and to its dual isogeny, we have that:

$$\langle \beta_1(Q)\rangle = \ker(\beta_r), \quad \langle p^r Q\rangle = \ker(\beta_1),$$

and, respectively,

$$\langle \beta_r^t(Q_{r+1})\rangle = \ker(\beta_1^t), \quad \langle p(Q_{r+1})\rangle = \ker(\beta_r^t).$$

In the following diagram, for clarity, we resume all the isogenies we have taken into account:



By definition of the Weil pairing, we have that $\langle Q_r\rangle = \ker(\beta_r^t) = \langle pQ_{r+1}\rangle$, so there exists $k \in (\mathbb{Z}/p^r\mathbb{Z})^*$ such that $kQ_r = pQ_{r+1}$, since they generate the same cyclic group of order p^r. Hence, by bilinearity of the pairing we have

$$e_{\beta_r}(\beta_1(Q), kQ_r) = \zeta_{p^r}^k = e_{\beta_r}(\beta_1(Q), pQ_{r+1}).$$

The compatibility of the pairing, see [KM85, 2.8] and [Sil09, III 8.1], implies that

$$e_{\beta_r}(\beta_1(Q), pQ_{r+1}) = e_{\beta_{r+1}}(Q, pQ_{r+1}) = \zeta_{p^{r+1}}^p = \zeta_{p^r}.$$

As $e_{\beta_r}(\beta_1(Q), Q_r) = \zeta_{p^r}$, then $k = 1$, hence $Q_r = pQ_{r+1}$. □

Main Lemma 2. *Let n and k be positive integers. Let ℓ and p be primes such that $n = mp^{r+1}$ with p and m co-prime, $r \in \mathbb{Z}_{\geq 1}$ and $mp^r > 4$, while ℓ does not divide n and $1 \leq k \leq \ell+1$. Let f be a* mod ℓ *cusp form in $S(m, p^{r+1}, k)_{\overline{\mathbb{F}}_\ell}$ such that*

$$f(\mathrm{Tate}(q), \zeta_m, \zeta_{p^{r+1}}) = \sum_{j\geq 1} a_j(f) q^j \left(\frac{dt}{t}\right)^{\otimes k} \in \overline{\mathbb{F}}_\ell\,[[q^p]] \left(\frac{dt}{t}\right)^{\otimes k}$$

where ζ_m and $\zeta_{p^{r+1}}$ are respectively fixed m-th and p^{r+1}-th roots of unity. Then there exists a unique modular form $g \in S(m, p^r, k)_{\overline{\mathbb{F}}_\ell}$, such that $B_p^* g = f$, where B_p^* is induced by $B_p : X_1(m, p^{r+1})_{\overline{\mathbb{F}}_\ell} \to X_1(m, p^r)_{\overline{\mathbb{F}}_\ell}$ the p-th degeneracy map.

Proof. Since $mp^r > 4$ we have the following diagram:

$$\begin{array}{ccc} X_1(m,p^{r+1})_{\overline{\mathbb{F}}_\ell} & \xrightarrow{w_{\zeta_{p^{r+1}}}} & X_1(m,p^{r+1})_{\overline{\mathbb{F}}_\ell} \\ \Big\downarrow{\scriptstyle B_p} & & \Big\downarrow{\scriptstyle \tilde{\alpha}} \\ X_1(m,p^r)_{\overline{\mathbb{F}}_\ell} & \xrightarrow{w_{\zeta_{p^r}}} & X_1(m,p^r)_{\overline{\mathbb{F}}_\ell} \end{array}$$

where B_p is the degeneracy map defined in (A.1), $w_{\zeta_{p^r}}$ and $w_{\zeta_{p^{r+1}}}$ are the Atkin-Lehner maps defined as in (A.2) and where $\tilde{\alpha} := w_{\zeta_{p^r}} \circ B_p \circ w^{-1}_{\zeta_{p^{r+1}}}$.

Our first goal is to prove that the map $\tilde{\alpha}$ is the forgetful map α defined in (A.1). On a elliptic curve E over S, $\overline{\mathbb{F}}_\ell$-scheme, with P and Q respectively points of order m and p^{r+1}, we have:

$$\begin{array}{ccc} (E,P,Q) & \xmapsto{w_{\zeta_{p^{r+1}}}} & (E/\langle Q\rangle, \beta_{r+1}(P), Q_{r+1}) \\ \Big\downarrow{\scriptstyle B_p} & & \Big\downarrow{\scriptstyle \tilde{\alpha}} \\ (E/\langle p^rQ\rangle, \beta_1(P), \beta_1(Q)) & \xmapsto{w_{\zeta_{p^r}}} & (E/\langle Q\rangle, \beta_r(\beta_1(P)), Q_r) \end{array}$$

and

$$(E/\langle Q\rangle, \beta_{r+1}(P), Q_{r+1}) \xmapsto{\alpha} (E/\langle Q\rangle, \beta_{r+1}(P), pQ_{r+1}) \ ,$$

where the maps $\beta_1, \beta_r, \beta_{r+1}$ are isogenies defined by:

$$\begin{array}{ccccc} & & \overset{\beta_{r+1}}{\frown} & & \\ E & \xrightarrow[\beta_1]{} & E/\langle p^rQ\rangle & \xrightarrow[\beta_r]{} & E/\langle Q\rangle \end{array}$$

so $\beta_r(\beta_1(P)) = \beta_{r+1}(P)$. In order to show that $\tilde{\alpha} = \alpha$, it is sufficient to apply Lemma A.2.2: $Q_r = pQ_{r+1}$.

We have that:

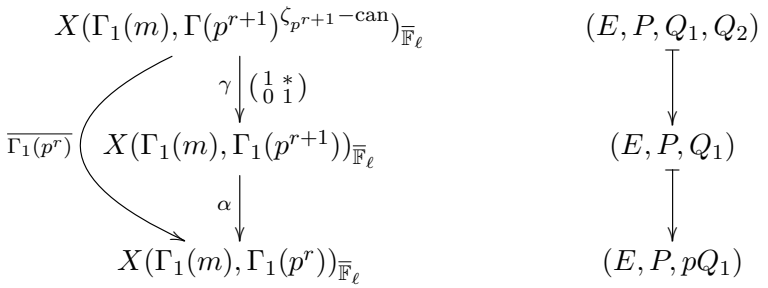
$$w_{\zeta_{p^{r+1}}}(\infty) = w_{\zeta_{p^{r+1}}}(\mathrm{Tate}(q), \zeta_m, \zeta_{p^{r+1}}) = (\mathrm{Tate}(q^{p^{r+1}}), \zeta_m^{p^{r+1}}, q) = \infty'.$$

Proceeding as in the Main Lemma 1, we deduce that there exists a unique Katz cusp form $f' \in S(m,p^{r+1},k)_{\overline{\mathbb{F}}_\ell}$ such that $w_{\zeta_{p^{r+1}}}(f') = f$: by direct computation at the standard cusp, we have that for all positive integers j

$$a_j(f')p^{(r+1)k} = a_j(f),$$

hence $f'(\mathrm{Tate}(q), \zeta_m, \zeta_{p^{r+1}}) \in \overline{\mathbb{F}}_\ell\,[[q^p]]\,((dt)/t)^{\otimes k}$. As in the Main Lemma 1,

on the modular curves there is a natural action on the level structure:



where

$$\overline{\Gamma_1(p^r)}\colon = \left\{ \begin{pmatrix} 1+p^r\cdot a & b \\ p^r\cdot c & 1+p^r\cdot d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/p^{r+1}\mathbb{Z}) \right\}.$$

In analogy with Main Lemma 1, there exists $g \in S(m,p^r,k)_{\overline{\mathbb{F}}_\ell}$ such that $B_p^* g = f$ if and only if $\gamma^* f'$ is $\overline{\Gamma_1(p^r)}$-invariant. Since the set $\left\{ \left(\begin{smallmatrix}1 & 0\\ p^r & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right) \right\}$ generates $\overline{\Gamma_1(p^r)}$ by Lemma A.2.1, it is enough to show the invariance for the generators.

The map $\gamma : X(\Gamma_1(m),\Gamma(p^{r+1})^{\zeta_{p^{r+1}}-\mathrm{can}})_{\overline{\mathbb{F}}_\ell} \to X(\Gamma_1(m),\Gamma(p^{r+1}))_{\overline{\mathbb{F}}_\ell}$ corresponds to the action of elements of the form $\left(\begin{smallmatrix}1 & *\\ 0 & 1\end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}/p^{r+1}\mathbb{Z})$ and $\gamma^* f'$ is invariant under the action of such elements by construction. The action of $\left(\begin{smallmatrix}1 & 0\\ p^r & 1\end{smallmatrix}\right)$ fixes $\infty' \in X(\Gamma_1(m),\Gamma(p^{r+1})^{\zeta_{p^{r+1}}-\mathrm{can}})_{\overline{\mathbb{F}}_\ell}$ and it acts on the complete local ring at ∞', $\overline{\mathbb{F}}_\ell[[q]]$, as:

$$\begin{cases} \text{identity on } \overline{\mathbb{F}}_\ell \\ q \mapsto \zeta_{p^{r+1}}^{p^r} q = \zeta_p q \end{cases},$$

then, by definition, $\left(\begin{smallmatrix}1 & 0\\ p^r & 1\end{smallmatrix}\right)$ acts on $\overline{\mathbb{F}}_\ell[[q]](dt/t)^{\otimes k}$ by $t \mapsto t$.

Since $a_j(f') = 0$ for all positive integers j not divisible by p, then $\left(\begin{smallmatrix}1 & 0\\ p^r & 1\end{smallmatrix}\right)^* f'$ has the same q-expansion as f'. Now, since $X(\Gamma_1(m),\Gamma(p^{r+1})^{\zeta_{p^{r+1}}-\mathrm{can}})_{\overline{\mathbb{F}}_\ell}$ is an irreducible reduced curve, this means that $\left(\begin{smallmatrix}1 & 0\\ p^r & 1\end{smallmatrix}\right)^* \gamma^* f' = \gamma^* f'$. The uniqueness of the modular form $g \in S(m,p^r,k)_{\overline{\mathbb{F}}_\ell}$ such that $B_p^* g = f$ follows, as in the previous lemma, by the q-expansion principle. □

In the previous main lemmas, we have not used the action of diamond operators. First of all, let us recall briefly how this operators are defined. For $n > 4$, and for all $d \in (\mathbb{Z}/n\mathbb{Z})^*$, we define an automorphism

$$\begin{array}{rcl} r_d : X(n)_{\overline{\mathbb{F}}_\ell} & \to & X(n)_{\overline{\mathbb{F}}_\ell} \\ (E,P) & \mapsto & r_d(E,P) = (E,dP) \end{array}$$

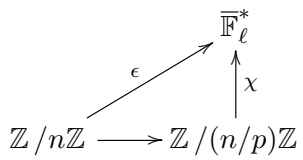
for all generalized elliptic curves E together with a $\Gamma_1(n)$-structure P. The diamond operator $\langle d\rangle$ on $M(\Gamma_1(n),k)_{\overline{\mathbb{F}}_\ell}$ for every $d \in (\mathbb{Z}/n\mathbb{Z})^*$ is defined as the automorphism of $M(\Gamma_1(n),k)_{\overline{\mathbb{F}}_\ell}$ induced by pullback via the automorphism r_d. If we are dealing with Katz cusp forms with a character $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$, we are imposing that for all $d \in (\mathbb{Z}/n\mathbb{Z})^*$, the diamond operator $\langle d\rangle$ acts as $\epsilon(d)$.

If we take this into account, we have an analogous to Main Lemma 1 and Main Lemma 2 for forms in $S(n,k,\epsilon)_{\overline{\mathbb{F}}_\ell}$.

Lemma A.2.3. *Let n and k be positive integers. Let ℓ and p be primes such that p divides n and $n/p > 4$, while ℓ does not divide n and $1 \leq k \leq \ell+1$. Let $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ and $\chi : (\mathbb{Z}/(n/p)\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ be characters.*

Let f and g be mod ℓ *cusp forms in $S(n,k,\epsilon)_{\overline{\mathbb{F}}_\ell}$ and in $S(n/p,k,\chi)_{\overline{\mathbb{F}}_\ell}$ respectively, such that $B_p^*(g) = f$, where B_p^* is the morphism induced by the degeneracy map $B_p : X_1(n)_{\overline{\mathbb{F}}_\ell} \to X_1(n/p)_{\overline{\mathbb{F}}_\ell}$. Then*

$$\chi = \mathrm{Res}^{\mathbb{Z}/(n/p)\mathbb{Z}}_{\mathbb{Z}/n\mathbb{Z}}(\epsilon)$$



i.e. for all $d \in \mathbb{Z}/(n/p)\mathbb{Z}$ we have $\chi(d) = \epsilon(d)$.

Proof. Let E/S be an elliptic curve over an $\overline{\mathbb{F}}_\ell$-scheme S, let P be a point of order n, and let B_p be the degeneracy map $B_p : X_1(n)_{\overline{\mathbb{F}}_\ell} \to X_1(n/p)_{\overline{\mathbb{F}}_\ell}$ defined in (A.1) through the isogeny β then

$$(B_p^* g)(E,P) = \beta^*(g(E/\langle (n/p)P\rangle, \beta(P))).$$

The action of the diamond operator $\langle d\rangle$ for $d \in \mathbb{Z}/(n/p)\mathbb{Z}$ is given by

$$\begin{aligned}\langle d\rangle (B_p^* g)(E,P) = (B_p^* g)(E,dP) &= \beta^*(g(E/\langle (n/p)P\rangle, \beta(dP))) = \\ &= \beta^*(g(E/\langle (n/p)P\rangle, d\beta(P))) = \\ &= \beta^*(\chi(d) g(E/\langle (n/p)P\rangle, \beta(P))) = \chi(d)(B_p^* g)(E,P);\end{aligned}$$

hence, for all $d \in \mathbb{Z}/(n/p)\mathbb{Z}$ we have $\langle d\rangle (B_p^* g) = \chi(d)(B_p^* g)$. Since $B_p^*(g) = f$, then for all $d \in \mathbb{Z}/(n/p)\mathbb{Z}$ it follows that $\langle d\rangle f = \chi(d) f = \epsilon(d) f$. Hence, for all $d \in \mathbb{Z}/(n/p)\mathbb{Z}$ the equality $\chi(d) = \epsilon(d)$ holds. □

Applying this lemma, we have the following:

Corollary of Main Lemma 1. *Let n and k be positive integers. Let ℓ and p be primes such that p strictly divides n and $n/p > 4$, while ℓ does not divide*

n and $1 \leq k \leq \ell+1$. Let $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ be a character. Let f be a mod *ℓ cusp form in $S(n/p, p, k, \epsilon)_{\overline{\mathbb{F}}_\ell}$ such that*

$$f(\mathrm{Tate}(q), \zeta_{n/p}, \zeta_p) = \sum_{j \geq 1} a_j(f) q^j \left(\frac{dt}{t}\right)^{\otimes k} \in \overline{\mathbb{F}}_\ell\left[[q^p]\right] \left(\frac{dt}{t}\right)^{\otimes k}$$

where $\mathrm{Tate}(q)$ is the Tate curve over $\overline{\mathbb{F}}_\ell((q))$, $\zeta_{n/p}$ and ζ_p are respectively fixed n/p-th and p-th roots of unity. Then there exists a unique form $g \in S(n/p, k, \epsilon')_{\overline{\mathbb{F}}_\ell}$, such that $B_p^* g = f$, where B_p^* is the morphism induced by the degeneracy map $B_p : X_1(n)_{\overline{\mathbb{F}}_\ell} \to X_1(n/p)_{\overline{\mathbb{F}}_\ell}$ and $\epsilon' = \mathrm{Res}^{\mathbb{Z}/(n/p)\mathbb{Z}}_{\mathbb{Z}/n\mathbb{Z}}(\epsilon)$.

Corollary of Main Lemma 2. *Let n and k be positive integers. Let ℓ and p be primes such that $n = mp^{r+1}$ with p and m coprime, $r \in \mathbb{Z}_{\geq 1}$ and $mp^r > 4$, while ℓ does not divide n and $1 \leq k \leq \ell+1$. Let $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ be a character. Let f be a* mod *ℓ cusp form in $S(m, p^{r+1}, k, \epsilon)_{\overline{\mathbb{F}}_\ell}$ such that*

$$f(\mathrm{Tate}(q), \zeta_m, \zeta_{p^{r+1}}) = \sum_{j \geq 1} a_j(f) q^j \left(\frac{dt}{t}\right)^{\otimes k} \in \overline{\mathbb{F}}_\ell\left[[q^p]\right] \left(\frac{dt}{t}\right)^{\otimes k}$$

where $\mathrm{Tate}(q)$ is the Tate curve over $\overline{\mathbb{F}}_\ell((q))$, ζ_m and $\zeta_{p^{r+1}}$ are respectively fixed m-th and p^{r+1}-th roots of unity. Then there exists a unique form $g \in S(m, p^r, k, \epsilon')_{\overline{\mathbb{F}}_\ell}$, such that $B_p^* g = f$, where B_p^* is the morphism induced by the degeneracy map $B_p : X_1(m, p^{r+1})_{\overline{\mathbb{F}}_\ell} \to X_1(m, p^r)_{\overline{\mathbb{F}}_\ell}$ and and $\epsilon' = \mathrm{Res}^{\mathbb{Z}/(mp^r)\mathbb{Z}}_{\mathbb{Z}/n\mathbb{Z}}(\epsilon)$.

Remark A.2.4. In Main Lemma 1 and 2, and also in the corollaries above, we assume that the prime p, dividing the level n, is such that the quotient $n/p > 4$. This hypothesis implies that all the objects used in the proofs are modular curves. Without such hypothesis, we should use the theory of algebraic stacks: for level n smaller than 4, the algebraic object $X(\Gamma_1(n))_{\overline{\mathbb{F}}_\ell}$ is an algebraic stack, see [Con07, Theorem 1.2.1], and dealing with such objects is beyond our purposes. It is highly likely that this condition can be removed.

A.3 Optimization

Theorem A.3.1. *Let n and k be positive integers. Let ℓ be a prime not dividing n, such that $2 \leq k \leq \ell+1$. Let $f : \mathbb{T}_\epsilon \to \overline{\mathbb{F}}_\ell$ be a ring homomorphism from the Hecke algebra of level n, weight k and nebentypus $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$, to $\overline{\mathbb{F}}_\ell$. Let $T_p \in \mathbb{T}_\epsilon$ be the p-th Hecke operator and $\overline{\epsilon} : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ be the character defined by $a \mapsto f(\langle a \rangle)$ for all $a \in (\mathbb{Z}/n\mathbb{Z})^*$. Let us suppose that there exists a prime m dividing $n\ell$ such that the $\overline{\mathbb{F}}_\ell$-vector space*

$$V :\, = \bigcap_{p \neq m} \ker\left(T_p - f(T_p), S(n, k, \overline{\epsilon})_{\overline{\mathbb{F}}_\ell}\right),$$

has dimension bigger than 1.

If m is different from ℓ then there exists a mod ℓ cusp form g in $S(n/m, k, \mathrm{Res}(\epsilon))_{\overline{\mathbb{F}}_\ell}$ such that $B_m^* g = f$. If $m = \ell$ then $k \in \{\ell, \ell+1\}$; in the first case there exists a mod ℓ cusp form g in $S(n, 1, \epsilon)_{\overline{\mathbb{F}}_\ell}$ such that $F(g) = f$, where F is the Frobenius, while in the second case there exists a mod ℓ cusp form g in $S(n, 2, \epsilon)_{\overline{\mathbb{F}}_\ell}$ such that $A_\ell g = f$, where A_ℓ is the Hasse invariant.

Proof. Let v be the dimension of V, by hypothesis $v > 1$. As T_m commutes with all T_p, T_m acts on V, and since $v > 1$ hence V contains a non-zero eigenvector f for all T_p, $p \geq 1$, in particular $a_1(f) \neq 0$.

The subspace $V_1 \subset V$ consisting of the g in V with $a_1(g) = 0$ is of dimension $v - 1 > 0$. Every element $g \in V_1$ is such that $0 = a_1(g) = a_1(T_j(g))$ for all integer j not divisible by m.

This means that g is an eigenform with q-expansion in $\mathbb{F}\left[\left[q^m\right]\right]\left((dt)/t\right)^{\otimes k}$ at the standard cusp.

Let us first suppose $m \neq \ell$. By assumptions $n/m > 4$, then we are in the hypotheses of the Main Lemmas, so there exists a non zero modℓ modular form $g' \in S(n/m, k, \epsilon')_{\overline{\mathbb{F}}_\ell}$ such that $B_p^* g' = g$, where $\epsilon' = \mathrm{Res}(\epsilon)$ and B_p^* is the morphism induced by the degeneracy map B_p defined in (A.1). This means that $V_1 = B_p^* V_2$ where V_2 is the eigenspace of $S(n, k, \overline{\epsilon})_{\overline{\mathbb{F}}_\ell}$ associated to the system of eigenvalues

$$\begin{aligned} f_{n,k}^{\{m\}} \colon = f_{n,k}|_{\mathcal{P}\setminus\{m\}} \colon \{\mathcal{P} \setminus \{m\}\} &\to \overline{\mathbb{F}}_\ell \times \overline{\mathbb{F}}_\ell \\ p &\mapsto (f(T_p), f(\langle p \rangle)) \end{aligned}$$

Hence the system of eigenvalues $f_{n,k}^{\{m\}}$ occurs in level n/m.

Let us suppose $m = \ell$. As proved in [Edi06, Proposition 6.2], the only two following cases occur. First case: $k = \ell$. The form g, constructed as before, is in the image of the Frobenius F, i.e. there exists $g' \in S(n, 1, \epsilon)_{\mathbb{F}}$ such that $g = (g')^\ell = F(g')$. This means that the system of eigenvalues occurs already in weight 1. Second case: $k = \ell + 1$. We have that $g = A_\ell g'$ where A_ℓ is the Hasse invariant of weight $\ell - 1$ and $g' \in S(n, 2, \epsilon)_{\mathbb{F}}$, hence the system of eigenvalues occurs in weight 2. □

From the previous theorem we deduce the following result:

Corollary A.3.2. *In the same hypotheses of Theorem A.3.1, the Galois representation attached to f in Corollary 4.0.5, $\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ arises from a lower level or weight.*

Moreover, we have that:

Corollary A.3.3. *In the same hypotheses of Theorem A.3.1, if $m \neq \ell$ then the dimension of V is at most $a+1$ where a is such that $m^a \operatorname{cond}(\rho_f) = n$.*

Proof. The subspace $V_1 \subset V$ consisting of the g in V with $a_1(g) = 0$ is of co-dimension 1 in V. Every element $g \in V_1$ is such that $0 = a_1(g) = a_1(T_j(g))$ for all integer j not divisible by m. This means that g is an eigenform with q-expansion in $\mathbb{F}\left[[q^m]\right]((dt)/t)^{\otimes k}$ at the standard cusp. The hypotheses of the Main Lemmas are satisfied, so there exists a non zero modℓ modular form $g' \in S(n/m, k, \operatorname{Res}(\epsilon))_{\overline{\mathbb{F}}_\ell}$ such that $B_p^* g' = g$. This means that $V_1 = B_p^* V_2$ where V_2 is the eigenspace of $S(n, k, \overline{\epsilon})_{\overline{\mathbb{F}}_\ell}$ associated to the system of eigenvalues $f_{n,k}^{\{m\}}$. We recursively apply the previous argument to the subspace V_1. This can be iterated at most a-times where a is the biggest power of m dividing $\operatorname{cond}(\rho_f)$. □

Bibliography

[Ann13] Samuele Anni. A local-global principle for isogenies of prime degree over number fields. `http://arxiv.org/pdf/1303.3809.pdf`, 2013.

[BD12] Nicolas Billerey and Luis V. Dieulefait. Explicit Large Image Theorems for Modular Forms. `http://arxiv.org/pdf/1210.5428v1.pdf`, 2012.

[Bea10] Arnaud Beauville. Finite subgroups of $\mathrm{PGL}_2(K)$. In *Vector bundles and complex geometry*, volume 522 of *Contemp. Math.*, pages 23–29. Amer. Math. Soc., Providence, RI, 2010.

[Ber06] Jacob Bernoulli. *The art of conjecturing.* Johns Hopkins University Press, Baltimore, MD, 2006. Together with "Letter to a friend on sets in court tennis", Translated from the Latin and with an introduction and notes by Edith Dudley Sylla.

[BK75] Bryan J. Birch and Willem Kuyk. *Modular functions of one variable. IV.* Lecture Notes in Mathematics, Vol. 476. Springer-Verlag, Berlin, 1975.

[Bos11] Johan Bosman. Modular forms applied to the computational inverse galois problem. `http://arxiv.org/pdf/1109.6879v1.pdf`, 2011.

[BS02] Kevin Buzzard and William A. Stein. A mod five approach to modularity of icosahedral Galois representations. *Pacific J. Math.*, 203(2):265–282, 2002.

[Buz00] Kevin Buzzard. On level-lowering for mod 2 representations. *Math. Res. Lett.*, 7(1):95–110, 2000.

[Car59a] Leonard Carlitz. Arithmetic properties of generalized Bernoulli numbers. *J. Reine Angew. Math.*, 202:174–182, 1959.

[Car59b] Leonard Carlitz. Some arithmetic properties of generalized Bernoulli numbers. *Bull. Amer. Math. Soc.*, 65:68–69, 1959.

[Car86] Henri Carayol. Sur les représentations l-adiques associées aux formes modulaires de Hilbert. *Ann. Sci. École Norm. Sup. (4)*, 19(3):409–468, 1986.

[Car89] Henri Carayol. Sur les représentations galoisiennes modulo l attachées aux formes modulaires. *Duke Math. J.*, 59(3):785–801, 1989.

[CH05] Alina C. Cojocaru and Chris Hall. Uniform results for Serre's theorem for elliptic curves. *International Mathematics Research Notices*, (50):3065–3080, 2005.

[CKR10] Imin Chen, Ian Kiming, and Jonas B. Rasmussen. On congruences mod $\mathfrak{p}^m$ between eigenforms and their attached Galois representations. *J. Number Theory*, 130(3):608–619, 2010.

[Con07] Brian Conrad. Arithmetic moduli of generalized elliptic curves. *J. Inst. Math. Jussieu*, 6(2):209–278, 2007.

[Cox89] David A. Cox. *Primes of the form $x^2 + ny^2$*. A Wiley-Interscience Publication. John Wiley & Sons Inc., New York, 1989. Fermat, class field theory and complex multiplication.

[CR06] Charles W. Curtis and Irving Reiner. *Representation theory of finite groups and associative algebras*. AMS Chelsea Publishing, Providence, RI, 2006. Reprint of the 1962 original.

[Del73] Pierre Deligne. Les constantes des équations fonctionnelles des fonctions L. In *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 501–597. Lecture Notes in Math., Vol. 349. Springer, Berlin, 1973.

[DI95] Fred Diamond and John Im. Modular forms and modular curves. In *Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994)*, volume 17 of *CMS Conf. Proc.*, pages 39–133. Amer. Math. Soc., Providence, RI, 1995.

[Dia97] Fred Diamond. An extension of Wiles' results. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 475–489. Springer, New York, 1997.

[Dic58] Leonard E. Dickson. *Linear groups: With an exposition of the Galois field theory*. with an introduction by W. Magnus. Dover Publications Inc., New York, 1958.

[Die71] Jean A. Dieudonné. *La géométrie des groupes classiques*. Springer-Verlag, Berlin, 1971. Troisième édition, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 5.

[DR73] Pierre Deligne and Michael Rapoport. Les schémas de modules de courbes elliptiques. In *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 143–316. Lecture Notes in Math., Vol. 349. Springer, Berlin, 1973.

[DS74] Pierre Deligne and Jean-Pierre Serre. Formes modulaires de poids 1. *Ann. Sci. École Norm. Sup. (4)*, 7:507–530, 1974.

[DS05] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[EC11] Bas Edixhoven and Jean-Marc Couveignes, editors. *Computational aspects of modular forms and Galois representations*, volume 176 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2011. How one can compute in polynomial time the value of Ramanujan's tau at a prime.

[Edi92] Bas Edixhoven. The weight in Serre's conjectures on modular forms. *Invent. Math.*, 109(3):563–594, 1992.

[Edi97] Bas Edixhoven. Serre's conjecture. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 209–242. Springer, New York, 1997.

[Edi06] Bas Edixhoven. Comparison of integral structures on spaces of modular forms of weight two, and computation of spaces of forms mod 2 of weight one. *J. Inst. Math. Jussieu*, 5(1):1–34, 2006. With appendix A (in French) by Jean-François Mestre and appendix B by Gabor Wiese.

[Fab11] Xander Faber. Finite p-irregular subgroups of $\mathrm{PGL}(2, k)$. `http://arxiv.org/pdf/1112.1999v2.pdf`, 2011.

[FH91] William Fulton and Joe Harris. *Representation theory*, volume 129 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991. A first course, Readings in Mathematics.

[Gor02] Eyal Z. Goren. *Lectures on Hilbert modular varieties and modular forms*, volume 14 of *CRM Monograph Series*. American Mathematical Society, Providence, RI, 2002. With the assistance of Marc-Hubert Nicole.

[Gro90] Benedict H. Gross. A tameness criterion for Galois representations associated to modular forms (mod p). *Duke Math. J.*, 61(2):445–517, 1990.

[Hid93] Haruzo Hida. *Elementary theory of L-functions and Eisenstein series*, volume 26 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1993.

[Kat73] Nicholas M. Katz. p-adic properties of modular schemes and modular forms. In *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 69–190. Lecture Notes in Mathematics, Vol. 350. Springer, Berlin, 1973.

[Kat77] Nicholas M. Katz. A result on modular forms in characteristic p. In *Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, pages 53–61. Lecture Notes in Math., Vol. 601. Springer, Berlin, 1977.

[Kat81] Nicholas M. Katz. Galois properties of torsion points on abelian varieties. *Inventiones mathematicae*, 62:481–502, 1981.

[KM85] Nicholas M. Katz and Barry Mazur. *Arithmetic moduli of elliptic curves*, volume 108 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1985.

[Koh04] Winfried Kohnen. On Fourier coefficients of modular forms of different weights. *Acta Arith.*, 113(1):57–67, 2004.

[Kra90] Alain Kraus. Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive. *Manuscripta Math.*, 69(4):353–385, 1990.

[KW09a] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture. I. *Invent. Math.*, 178(3):485–504, 2009.

[KW09b] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture. II. *Invent. Math.*, 178(3):505–586, 2009.

[Lan76] Serge Lang. *Introduction to modular forms.* Springer-Verlag, Berlin, 1976.

[Liv89] Ron Livné. On the conductors of mod l Galois representations coming from modular forms. *J. Number Theory*, 31(2):133–141, 1989.

[Maz77a] Barry Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.

[Maz77b] Barry Mazur. Rational points on modular curves. In Jean-Pierre Serre and DonBernard Zagier, editors, *Modular Functions of one Variable V*, volume 601 of *Lecture Notes in Mathematics*, pages 107–148. Springer Berlin Heidelberg, 1977.

[Maz11] Barry Mazur. How can we construct abelian Galois extensions of basic number fields? *Bull. Amer. Math. Soc. (N.S.)*, 48(2):155–209, 2011.

[Miy06] Toshitsune Miyake. *Modular forms.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, english edition, 2006. Translated from the 1976 Japanese original by Yoshitaka Maeda.

[Par99] Pierre J. R. Parent. Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres. *J. Reine Angew. Math.*, 506:85–116, 1999.

[Par05] Pierre J. R. Parent. Towards the triviality of $X_0^+(p^r)(\mathbb{Q})$ for $r > 1$. *Compos. Math.*, 141(3):561–572, 2005.

[PT07] Ariel Pacetti and Gonzalo Tornaría. Examples of the Shimura correspondence for level p^2 and real quadratic twists. In *Ranks of elliptic curves and random matrix theory*, volume 341 of *London Math. Soc. Lecture Note Ser.*, pages 289–314. Cambridge Univ. Press, Cambridge, 2007.

[Que95] Jordi Quer. Liftings of projective 2-dimensional galois representations and embedding problems. *J. of Algebra*, 171(2):541 – 566, 1995.

[Ras09] Jonas B. Rasmussen. *Higher congruences between modular forms.* PhD thesis, 2009. `http://www.math.ku.dk/~jonas/Thesis.pdf`.

[Rib76a] Kenneth A. Ribet. Galois action on division points of Abelian varieties with real multiplications. *Amer. J. Math.*, 98(3):751–804, 1976.

[Rib76b] Kenneth A. Ribet. A modular construction of unramified p-extensions of $Q(\mu_p)$. *Invent. Math.*, 34(3):151–162, 1976.

[Rib85] Kenneth A. Ribet. On l-adic representations attached to modular forms. II. *Glasgow Math. J.*, 27:185–194, 1985.

[Rib94] Kenneth A. Ribet. Report on mod l representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. In *Motives (Seattle, WA, 1991)*, volume 55 of *Proc. Sympos. Pure Math.*, pages 639–676. Amer. Math. Soc., Providence, RI, 1994.

[Rob96] Derek J. S. Robinson. *A course in the theory of groups*, volume 80 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1996.

[Sch12] George J. Schaeffer. *The Hecke Stability Method and Ethereal Forms*. PhD thesis, 2012. `http://www.math.ucla.edu/~gschaeff/schaeffer-thesis.pdf`.

[Ser66] Jean-Pierre Serre. Groupes de Lie l-adiques attachés aux courbes elliptiques. In *Les Tendances Géom. en Algébre et Théorie des Nombres*, pages 239–256. Éditions du Centre National de la Recherche Scientifique, Paris, 1966.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones mathematicae*, 15:259–331, 1972.

[Ser77a] Jean-Pierre Serre. *Cours d'arithmétique*. Presses Universitaires de France, Paris, 1977. Deuxième édition revue et corrigée, Le Mathématicien, No. 2.

[Ser77b] Jean-Pierre Serre. Modular forms of weight one and Galois representations. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 193–268. Academic Press, London, 1977.

[Ser78] Jean-Pierre Serre. *Représentations linéaires des groupes finis*. Hermann, Paris, revised edition, 1978.

[Ser87] Jean-Pierre Serre. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. *Duke Math. J.*, 54(1):179–230, 1987.

[Ser94] Jean-Pierre Serre. Sur la semi-simplicité des produits tensoriels de représentations de groupes. *Invent. Math.*, 116(1-3):513–530, 1994.

[Ser95] Jean-Pierre Serre. Corps locaux et isogénies. In *Séminaire Bourbaki, Vol. 5*, pages Exp. No. 185, 239–247. Soc. Math. France, Paris, 1995.

[Shi71] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*. Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo, 1971. Kanô Memorial Lectures, No. 1.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[Sri79] Bhama Srinivasan. *Representations of finite Chevalley groups*, volume 764 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1979. A survey.

[Ste07] William Stein. *Modular forms, a computational approach*, volume 79 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2007. With an appendix by Paul E. Gunnells.

[Stu87] Jacob Sturm. On the congruence of modular forms. In *Number theory (New York, 1984–1985)*, volume 1240 of *Lecture Notes in Math.*, pages 275–280. Springer, Berlin, 1987.

[Sut12] Andrew V. Sutherland. A local-global principle for rational isogenies of prime degree. *J. Théor. Nombres Bordeaux*, 24(2):475–485, 2012.

[Tak11] Yuuki Takai. An effective isomorphy criterion for mod ℓ Galois representations. *J. Number Theory*, 131(8):1409–1419, 2011.

[Vig89] Marie-France Vignéras. Correspondance modulaire galois-quaternions pour un corps p-adique. In *Number theory (Ulm, 1987)*, volume 1380 of *Lecture Notes in Math.*, pages 254–266. Springer, New York, 1989.

[Wal81] Jean-Loup Waldspurger. Sur les coefficients de Fourier des formes modulaires de poids demi-entier. *J. Math. Pures Appl. (9)*, 60(4):375–484, 1981.

[Wie04] Gabor Wiese. Dihedral Galois representations and Katz modular forms. *Doc. Math.*, 9:123–133 (electronic), 2004.

[Wie05] Gabor Wiese. *Modular Forms of Weight One Over Finite Fields*. PhD thesis, 2005.

List of Notations

χ_ℓ	modℓ cyclotomic character, page 27
$\mathbb{F}_\ell$	finite field with ℓ elements, page 4
$\Gamma_0(n)$	subgroup of $\mathrm{SL}_2(\mathbb{Z})$ whose elements reduce to $\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)$ mod n, page 52
$\Gamma_1(n)$	subgroup of $\mathrm{SL}_2(\mathbb{Z})$ whose elements reduce to $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$ mod n, page iii
$\mathbb{P}^1(\mathbb{F}_\ell)^g$	set of elements fixed by g, page 5
$\mathbb{P}^1(\mathbb{F}_\ell)/g$	set of g-orbits of $\mathbb{P}^1(\mathbb{F}_\ell)$, page 5
$\mathfrak{A}_n$	alternating group on n-elements, page 9
$\mathfrak{S}_n$	symmetric group on n-elements, page 9
$\mathrm{N}(\rho)$	Artin conductor of ρ, page 33
$\mathrm{N}_p(\rho)$	valuation of $\mathrm{N}(\rho)$ at p, page 33
$\mathbb{T}(n,k)$	cuspidal Hecke algebra, page 25
$\mathbb{T}_\epsilon(n,k)$	cuspidal Hecke algebra related to $S(n,k,\epsilon)_{\mathbb{C}}$, page 25
θ_ℓ	$q\,d/dq$ operator, page 32
A_ℓ	Hasse invariant in characteristic ℓ, page 31
$B(n,k)$	Sturm bound, page 51
B_k^χ	k-th generalized Bernoulli number, page 69
B_p	p-th degeneracy map, page 53
e_β	Weil pairing related to the isogeny β, page 131
$f_{n,k}$	system of eigenvalues, page 50
$f_{n,k}^{(*)}$	system of eigenvalues truncated at $(*)$, page 65
$G_{\mathbb{Q}}$	absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, page i
$k(\rho)$	minimal weight of the representation ρ, page 33
$M(n,k)_{\mathbb{C}}$	complex vector space of weight k modular forms on $\Gamma_1(n)$, page 25
$M(n,k)_{\overline{\mathbb{F}}_\ell}$	Katz modular forms of weight k for $\Gamma_1(n)$ on $\overline{\mathbb{F}}_\ell$, page 30
$S(n,k,\epsilon)_{\mathbb{C}}$	complex vector space of weight k, level n cusp forms with character, page 25

$S(n,k)_{\mathbb{C}}$	complex vector space of weight k cusp forms on $\Gamma_1(n)$, page 25
$S(n,k)_{\overline{\mathbb{F}}_\ell}$	Katz cusp forms of weight k for $\Gamma_1(n)$ on $\overline{\mathbb{F}}_\ell$, page 30
V_4	Klein 4-group, page 20
$w_{\zeta_{p^r}}$	Atkin-Lehner map, page 131
$X(\ell)$	modular curve, page 17
$X_0(\ell)$	modular curve related to the Borel subgroup, page 18
$X_{\mathfrak{A}_4}(\ell)$, $X_{\mathfrak{S}_4}(\ell)$, $X_{\mathfrak{A}_5}(\ell)$	modular curves related to the exceptional subgroups, page 18
$X_{\mathrm{sp.Car}}(\ell)$	modular curve related to the split Cartan subgroup, page 4
$X_{\mathrm{split}}(\ell)$	modular curve related to the normalizer of a split Cartan subgroup, page 4
$X_{V_4}(\ell)$	modular curve related to V_4, page 20

Index

List of Algorithms

Abstract

In this thesis we investigate 2-dimensional, continuous, odd, residual Galois representations and their images. This manuscript consists of two parts in which two different topics are studied.

In the first part we solve a problem related to elliptic curves for which the knowledge of the image of a certain Galois representation is the crucial element for the solution. The second part of this thesis has a computational purpose: to outline an algorithm for computing the images of 2-dimensional, continuous, odd, residual Galois representations.

The first part of this thesis is committed to analyse a local-global problem for elliptic curves over number fields.

Let E be an elliptic curve over a number field K, and let ℓ be a prime number. If E admits an ℓ-isogeny locally at a set of primes with density one then does E admit an ℓ-isogeny over K?

The study of the Galois representation associated to the ℓ-torsion subgroup of E is the crucial ingredient used to solve the problem.

Let K be a number field and E an elliptic curve over K. Assume that the j-invariant of E is different from 0 and 1728. A pair $(\ell, j(E))$ is said to be exceptional for K if E/K admits an ℓ-isogeny locally for a set of density one of primes of K but not globally over K.

In this part of the thesis we give a complete description of the set of exceptional pairs for a number field K.

In particular, we obtain an upper bound for the possible values of ℓ occurring in such pairs in terms of d, the degree of K over $\mathbb{Q}$, and Δ, the discriminant of K:

$$\ell \leq \max\{\Delta, 6d{+}1\}.$$

Moreover, we show finiteness results for the set of exceptional pairs studying particular modular curves and their genus.

The main result of the first part of this thesis is the following theorem:

Main Theorem. *Let K be a number field of degree d over $\mathbb{Q}$ and discriminant Δ, and let $\ell_K := \max\{\Delta, 6d{+}1\}$. The following holds:*

(1) *if $(\ell, j(E))$ is an exceptional pair for the number field K then $\ell \leq \ell_K$;*

(2) *there are only finitely many exceptional pairs for K with $7 < \ell \leq \ell_K$;*

(3) *the number of exceptional pairs for K with $\ell = 7$ is finite or infinite, according to the rank of Elkies-Sutherland's elliptic curve:*

$$y^2 = x^3 - 1715x + 33614$$

being zero or positive over K;

(4) *there exists no exceptional pair for K with $\ell = 2$ and with $\ell = 3$;*

(5) *there exist exceptional pairs for K with $\ell = 5$ if and only if $\sqrt{5}$ belongs to K. Moreover, if $\sqrt{5}$ belongs to K then there are infinitely many exceptional pairs for K with $\ell = 5$.*

In the second part of this thesis, we outline an algorithm for computing the image of a residual modular 2-dimensional semi-simple Galois representation. This means determining the image as as a finite subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$, up to conjugation, as well as certain local properties of the representation and tabulating the result in a database.

Let n and k be positive integers. Let $S(n,k)_{\mathbb{C}}$ be the complex vector space of weight k cusp forms on $\Gamma_1(n)$, and let $\mathbb{T}(n,k)$ denote the associated Hecke algebra that is the $\mathbb{Z}$-subalgebra of $\mathrm{End}_{\mathbb{C}}(S(n,k)_{\mathbb{C}})$ generated by the Hecke operators T_p for every prime p and the diamond operators $\langle d \rangle$ for every $d \in (\mathbb{Z}/n\mathbb{Z})^*$.

The aforementioned algorithm is developed for residual modular 2-dimensional semi-simple Galois representations: by a theorem of Shimura and Deligne, given a finite field $\mathbb{F}$ of characteristic ℓ and $f : \mathbb{T}(n,k) \to \mathbb{F}$ a morphism of rings from the cuspidal Hecke algebra of level n and weight k to $\mathbb{F}$, there is a unique, up to isomorphism, continuous semi-simple representation $\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F})$ that is unramified outside $n\ell$ such that for all primes p not dividing $n\ell$ we have $\mathrm{Trace}(\rho_f(\mathrm{Frob}_p)) = f(T_p)$ and $\det(\rho_f(\mathrm{Frob}_p)) = f(\langle p \rangle)p^{k-1}$ in $\mathbb{F}$.

The representation ρ_f can be computed in time polynomial in n, k and the cardinality of $\mathbb{F}$, where $\mathbb{F}$ is a finite field of characteristic ℓ where the representation is defined, ℓ not dividing n. Due to the current state of technology, we cannot compute such representations for large values of n, k over finite fields of arbitrary order (greater than 41). Anyway, the computation of the image of a residual 2-dimensional odd semi-simple Galois representation is a totally different matter than the computation of the representation itself.

One of the main results of this part of the thesis is that the algorithm does use only Hecke operators up to the Sturm bound at the given level n in almost all cases, i.e. the bound on the number of operators needed is of the order:

$$\frac{k}{12} \cdot n \log\log n,$$

and in the cases where this is not sufficient, the bound increases, in the worst case, of a factor q^2, where q is the smallest odd prime not dividing n. In addition, almost all the computations are performed in positive characteristic: only in the construction related to projectively exceptional images some computations in characteristic zero are needed. Moreover, no pre-computed

list of number fields with specific Galois groups is needed in order to compute the projective image.

To obtain such an algorithm we solved different problems. For example, two different mod ℓ modular forms can give rise to the same Galois representation or two Galois representations can have the same projective image. In order to give a solution to the first instance, without increasing the bound needed for the computations, we study the local description of the representation at primes dividing the level and the characteristic. Similarly, we investigate the conductor of the twist of a representation by characters and the coefficients of the form of minimal level and weight associated to the given twist to answer to the second.

The algorithm is designed using Dickson's classification of the finite subgroups of $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$. We characterize each possible case giving a precise description and algorithms to deal with it. In particular, we give a new approach and a construction to deal with irreducible representations with projective image isomorphic to either the symmetric group on 4 elements or the alternating group on 4 or 5 elements.

Samenvatting

In dit proefschrift bestuderen we 2-dimensionale, continue, oneven, residuale Galoisrepresentaties en hun beelden. Dit proefschrift bestaat uit twee onderdelen waarin verschillende onderwerpen worden bestudeerd.

In het eerste deel lossen we een probleem op gerelateerd aan elliptische krommen waarvoor kennis van het beeld van zekere Galoisrepresentaties een cruciale rol speelt. Het tweede deel van dit proefschrift heeft een computationeel doel: het beschrijven van een algoritme om beelden van residuele 2-dimensionale Galoisrepresentaties komend van modulaire vormen uit te rekenen.

Het eerste deel van dit proefschrift houdt zich bezig met een locaal-globaal probleem voor elliptische krommen over getallenlichamen.

Zij E een elliptische kromme over een getallenlichaam K, en zij ℓ een priemgetal. Heeft E een ℓ-isogenie over K als deze een lokale ℓ-isogenie heeft voor een verzameling priemen met dichtheid één?

De studie van de Galoisrepresentatie verbonden aan de ℓ-torsie ondergroep van E speelt een cruciale rol voor het oplossen van dit probleem.

Zij K een getallenlichaam en E een elliptische kromme over K. Neem aan dat de j-invariant van E verschillend is van 0 en 1728. Een paar $(\ell, j(E))$ heet exceptioneel voor K als E/K een ℓ-isogenie heeft voor een verzameling priemen van dichtheid één, maar niet globaal over K.

In dit deel van het proefschrift geven we een volledige beschrijving van de verzameling exceptionele paren voor een getallenlichaam K.

In het bijzonder geven we een bovengrens voor de mogelijke waardes van ℓ die kunnen voorkomen in termen van d, de graad van K over $\mathbb{Q}$, en Δ, de discriminant van K:

$$\ell \leq \max\{\Delta, 6d{+}1\}\,.$$

Bovendien geven we eindigheidsresultaten voor de verzameling van exceptionele paren door te kijken naar bepaalde modulaire krommen en hun geslacht.

Het hoofdresultaat van de eerste helft van dit proefschrift is de volgende stelling:

Hoofdstelling. *Zij K een getallenlichaam van graad d over $\mathbb{Q}$ en discriminant Δ, en zij $\ell_K := \max\{\Delta, 6d{+}1\}$. Dan geldt het volgende:*

(1) *als $(\ell, j(E))$ een exceptioneel paar is voor het getallenlichaam K, dan $\ell \leq \ell_K$;*
(2) *er zijn slechts eindig veel exceptionele paren voor K met $7 < \ell \leq \ell_K$;*

(3) *het aantal exceptionele paren voor K met $\ell = 7$ is eindig als de rang over K van de Elkies-Sutherland's elliptische kromme:*

$$y^2 = x^3 - 1715x + 33614$$

nul is, en anders oneindig;

(4) *er zijn geen exceptionele paren voor K met $\ell = 2$ en $\ell = 3$;*

(5) *er zijn exceptionele paren voor K met $\ell = 5$ dan en slechts dan als $\sqrt{5}$ een element van K is. Bovendien, als $\sqrt{5}$ een element van K is, dan zijn er oneindig veel exceptionele paren voor K met $\ell = 5$.*

In het tweede deel van dit proefschrift beschrijven we een algoritme dat de beelden van residuele 2-dimensionale Galoisrepresentaties komend van modulaire vormen uitrekent.

Zij n en k positieve gehele getallen. Zij $S(n,k)_{\mathbb{C}}$ de complexe vectorruimte van spitsvormen van gewicht k op $\Gamma_1(n)$, en zij $\mathbb{T}(n,k)$ de geassocieerde Hecke-algebra, de $\mathbb{Z}$-deelalgebra van $\mathrm{End}_{\mathbb{C}}(S(n,k)_{\mathbb{C}})$ voortgebracht door de Hecke-operatoren T_p voor alle priemen p en de diamantoperatoren $\langle d \rangle$ voor elke $d \in (\mathbb{Z}/n\mathbb{Z})^*$.

Een stelling van Shimura en Deligne zegt dat, gegeven een eindig lichaam $\mathbb{F}$ van karakteristiek ℓ en $f : \mathbb{T}(n,k) \to \mathbb{F}$ een morfisme van ringen van de spits Hecke-algebra van niveau n en gewicht k naar $\mathbb{F}$, er een uniek, op isomorfisme na, continue semi-simpele representatie $\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F})$ is die overtakt is buiten $n\ell$ zodanig dat voor alle priemen p die $n\ell$ niet delen we de identiteiten $\mathrm{Trace}(\rho_f(\mathrm{Frob}_p)) = f(T_p)$ en $\det(\rho_f(\mathrm{Frob}_p)) = f(\langle p \rangle)p^{k-1}$ in $\mathbb{F}$ hebben.

Dit algoritme bepaalt het beeld als een eindige ondergroep van $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$, op conjugatie na, alsmede bepaalde lokale eigenschappen van de representaties en tabuleert de resultaten in een database.

De representatie ρ_f kan worden uitgerekend in polynomiale tijd in n, k en de kardinaliteit van $\mathbb{F}$, waarbij $\mathbb{F}$ een eindig lichaam is van karakteristiek ℓ waarover de presentatie gedefinieerd is, waarbij ℓ het getal n niet deelt. Met de huidige techniek kunnen we deze representaties niet uitrekenen voor grote waardes van n, k over lichamen van willekeurige kardinaliteiten (groter dan 41). De berekening van het beeld van een residuele 2-dimensionale oneven semi-simpele Galoisrepresentatie is een totaal ander probleem dan het berekenen van de representatie zelf.

Eén van de hoofdresultaten van dit deel van het proefschrift is dat het algoritme in bijna alle gevallen slechts Hecke-operatoren gebruikt tot aan de Sturmgrens bij een gegeven niveau n , dat wil zeggen, de grens op het aantal operatoren dat nodig is, is van de orde:

$$\frac{k}{12} \cdot n \log\log n,$$

en in de gevallen waarin dit niet voldoende is, wordt de grens in het ergste geval met een factor q^2 verhoogd, waarbij q het kleinste oneven priemgetal is dat n niet deelt. Daarnaast worden bijna alle berekeningen in positieve karakteristiek gedaan: alleen bij de constructie gerelateerd aan projectieve exceptionele beelden zijn misschien berekeningen in karakteristiek 0 nodig. Bovendien zijn er geen voorberekende lijsten van getallenlichamen met specifieke Galoisgroep nodig om de orde van het projectieve beeld uit te rekenen.

Om een dergelijk algoritme te verkrijgen, hebben we verschillende problemen opgelost. Bijvoorbeeld, twee verschillende mod ℓ modulaire vormen kunnen dezelfde Galoisrepresentatie geven of twee Galoisrepresentaties kunnen hetzelfde projectieve beeld hebben. Om het eerste probleem op te lossen, zonder de grens die nodig is voor de berekening te verhogen, bestuderen we de lokale beschrijving van de representatie bij priemen die het niveau en de karakteristiek delen. Voor het tweede probleem bestuderen we de conductor van de verdraaiing van de representatie met karakters en de coëfficiënten van de vorm van minimaal niveau en gewicht daarmee geassocieerd.

Het algoritme is gebaseerd op resultaten van Dickson, Khare-Wintenberger en Faber over de classificatie, op conjugatie na, van eindige ondergroepen van $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$. We karakterisen alle mogelijke gevallen door een precieze beschrijving en algoritmes te geven die ze afhandelen. In het bijzonder geven we een nieuwe benadering en een constructie die irreducibele representaties afhandelt waarvan het projectieve beeld isomorf met de symmetrische groep op 4 letters of de alternerende groep op 4 of 5 letters.

Résumé

Dans cette thèse, on étudie les représentations 2-dimensionnelles continues du groupe de Galois absolu d'une clôture algébrique fixée de $\mathbb{Q}$ sur les corps finis qui sont modulaires et leurs images.

Ce manuscrit se compose de deux parties dans lesquelles deux thèmes différents sont étudiés.

La première partie est consacrée à l'analyse d'un problème local-global pour les courbes elliptiques sur les corps de nombres. Soit E une courbe elliptique sur un corps de nombres K, et soit ℓ un nombre premier. Si E admet une ℓ-isogénie localement sur un ensemble de nombres premiers de densité 1, alors est-ce que E admet une ℓ-isogénie sur K ?

L'étude de la représentation galoisienne associée à la ℓ-torsion de E est l'ingrédient essentiel utilisé pour résoudre ce problème.

On donne une description de l'ensemble des paires exceptionnelles pour un corps de nombres K : l'ensemble des couples $(\ell, j(E))$, où ℓ est un nombre premier et $j(E)$ est le j-invariant d'une courbe elliptique E sur K, en supposant que $j(E)$ soit différent de 0 et 1728, qui admet une ℓ-isogénie localement presque partout, mais pas globalement.

En particulier, on obtient une borne supérieure pour ℓ survenant dans ces paires en fonction de d, le degré de K sur $\mathbb{Q}$, et de Δ, le discriminant de K :

$$\ell \leq \max\{\Delta, 6d{+}1\}\,.$$

Par ailleurs, on montre des résultats de finitude pour l'ensemble des couples exceptionnels en étudiant des courbes modulaires particulières et leur genre.

Le résultat principal de la première partie de cette thèse est le théorème suivant :

Théorème principal. *Soit K un corps de nombres de degré d sur $\mathbb{Q}$ et discriminant Δ, et soit $\ell_K := \max\{\Delta, 6d{+}1\}$. Les énoncés suivants sont vérifiés :*

(1) *si $(\ell, j(E))$ est une paire exceptionnelle pour le corps de nombres K, alors $\ell \leq \ell_K$;*

(2) *il y a seulement un nombre fini de paires exceptionnelles pour le corps de nombre K avec $7 < \ell \leq \ell_K$;*

(3) *le nombre de paires exceptionnelles pour K avec $\ell = 7$ est fini ou infini, selon que le rang de la courbe elliptique de Elkies-Sutherland :*

$$y^2 = x^3 - 1715x + 33614$$

est nul ou positif sur K ;

(4) *il n'existe aucune paire exceptionnelle pour K avec $\ell = 2$ et $\ell = 3$;*
(5) *il existe des paires exceptionnelles pour K avec $\ell = 5$ si et seulement si $\sqrt{5}$ appartient à K. De plus, si $\sqrt{5}$ appartient à K, alors il existe une infinité de paires exceptionnelles pour K avec $\ell = 5$.*

Dans la deuxième partie, on présente un algorithme pour calculer l'image d'une représentation 2-dimensionnelle continue du groupe de Galois absolu d'une clôture algébrique fixée de $\mathbb{Q}$ sur un corps fini qui est modulaire. Ceci est équivalent à la détermination de l'image comme sous-groupes fini de $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$, à conjugaison près, ainsi que certaines propriétés locales de la représentation et le stockage du résultat dans une base de données.

Soient n et k des entiers positifs. Soit $S(n,k)_{\mathbb{C}}$ l'espace vectoriel complexe des formes paraboliques sur $\Gamma_1(n)$ de poids k, et soit $\mathbb{T}(n,k)$ l'algèbre de Hecke associée qui est la $\mathbb{Z}$-algèbre de $\mathrm{End}_{\mathbb{C}}(S(n,k)_{\mathbb{C}})$ engendrée par les opérateurs de Hecke T_p pour chaque premier p et les opérateurs diamant $\langle d \rangle$ pour chaque $d \in (\mathbb{Z}/n\mathbb{Z})^*$.

Soit $\mathbb{F}$ un corps fini de caractéristique ℓ et soit $f : \mathbb{T}(n,k) \to \mathbb{F}$ un morphisme d'anneaux de l'algèbre de Hecke cuspidale de niveau n et poids k sur $\mathbb{F}$. Alors, il existe une unique, à isomorphisme près, représentation continue semi-simple

$$\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F})$$

qui est non ramifiée dehors de $n\ell$ telle que pour tout premier p ne divisant pas $n\ell$ on a

$$\mathrm{Trace}(\rho_f(\mathrm{Frob}_p)) = f(T_p) \text{ et } \det(\rho_f(\mathrm{Frob}_p)) = f(\langle p \rangle)p^{k-1} \text{ en } \mathbb{F}.$$

L'algorithme ci-dessus est développé pour ce type de représentations.

La représentation ρ_f peut être calculée en temps polynomial en n, k et la cardinalité de $\mathbb{F}$, où $\mathbb{F}$ est un corps fini de caractéristique ℓ où la représentation est définie, ℓ ne divisant pas n. L'état actuel de la technologie ne permet pas de calculer de telles représentations pour les grandes valeurs de n, k sur un corps fini d'ordre arbitraire (ordre supérieur à 41). Quoi qu'il en soit, le calcul de l'image est une question totalement différente de celle du calcul de la représentation elle-même.

L'un des résultats principaux de cette partie de la thèse est que l'algorithme n'utilise que des opérateurs de Hecke jusqu'à la borne de Sturm au niveau donné n dans presque tous les cas. Cela signifie que la borne sur le nombre d'opérateurs nécessaires est de l'ordre de :

$$\frac{k}{12} \cdot n \log\log n,$$

et dans les cas où cela n'est pas suffisant, l'augmentation de la borne est, au pire, d'un facteur q^2, où q est le plus petit nombre premier impair qui ne divise pas n.

En outre, presque tous les calculs sont effectués en caractéristique positive. Il n'y a que dans la construction liée à des images exceptionnelles projectives que quelques calculs en caractéristique zéro sont nécessaires.

Dans cet algorithme, aucune liste pré-calculée des corps de nombres avec un groupe de Galois spécifique n'est nécessaire pour calculer l'image projective.

Différents problèmes sont résolus afin d'avoir un tel algorithme. Par exemple, deux formes modulaires mod ℓ différentes peuvent donner lieu à la même représentation de Galois ou deux représentations de Galois peuvent avoir la même image projective. Afin de donner une solution dans la première situation, sans augmenter la borne nécessaire aux calculs, on étudie la description locale de la représentation aux nombres premiers divisant le niveau et la caractéristique.

En particulier, on obtient une caractérisation précise des formes propres dans l'espace des formes anciennes en caractéristique positive : ce sont des formes d'un niveau donné provenant de formes de niveau inférieur ou poids inférieur et elles sont vues au niveau donné à travers des morphismes de dégénérescence, ou la multiplication par l'invariant de Hasse ou l'application de Frobenius.

De la même manière, pour répondre à la seconde question on étudie le conducteur de la tordue d'une représentation par un caractère et les coefficients de la forme de niveau et poids minimaux associée. Ceci est fait dans le but de ne pas répéter les calculs pour déterminer la représentation projective et de les effectuer seulement si la représentation projective est de niveau et poids minimaux.

Voici comment l'algorithme est conçu.

Dans l'algorithme ci-dessus pour toutes les données ne provenant pas de niveau ou poids inférieurs, on détermine si la représentation associée est réductible ou non. L'idée principale pour effectuer ce test est de contrôler les égalités entre la forme modulaire donnée et la réduction modulo ℓ de certaines séries d'Eisenstein.

Si la représentation est irréductible, alors on calcule le corps de définition de la représentation.

Afin de déterminer l'image, à conjugaison près, il suffit de connaître l'image projective de la représentation et l'ensemble des déterminants. Par conséquent, on calcule le corps de définition de la représentation projective.

Pour calculer l'image projective de la représentation, on effectue une liste de contrôles en fonction de la classification de Dickson, sauf si la représentation survient de tordues d'une représentation de conducteur inférieur, auquel cas l'image projective est déjà enregistrée dans la base de données. En particulier, on donne une nouvelle approche pour déterminer les représentations

irréductibles avec image projective isomorphe soit au groupe symétrique sur 4 éléments ou au groupe alterné sur 4 ou 5 éléments.

Une fois que l'on a exclu tous les cas exceptionnels i.e. tous les cas où l'ordre de l'image n'est pas divisible par ℓ, l'image est "grande", ce qui signifie qu'elle contient le groupe spécial linéaire de degré 2 de l'extension de $\mathbb{F}_\ell$ correspondant au corps de définition de l'image projective.

Acknowledgements

"think globally, act locally"
Patrick Geddes

This thesis comes after a long journey through Europe: since I started my master in 2010, I have never spent more than two consecutive years in the same country.

First of all I would like to thank my advisors for supporting me during these past three years, for all the conversations we have had. Thanks to Bas, for all the time, for all the great ideas, for all the support he gave me. I have learnt a lot from you. Thanks to Pierre, for all the patience, for your guidance and for all the long skype talks.

Thanks to the promotiecommissie for the time spent reading my thesis. In particular, thanks to Gabor Wiese for all the precious comments and for all the nice discussions we had during these years.

I would like to thank the ALGANT consortium for funding my studies, but also for having given me the possibility to do mathematics with very nice and interesting people. Thanks to all my ALGANT friends: Alberto, Ariyan, Thanos, Andrea, Sophie, Chao, Albert, Mima, Valentina, Stefano, Michele, Chiara, Corina, Catalina, Dino, Liu, Shuang, Martin, Tomo, Rosa ...

Many thanks to the number theory, algebra, and geometry group in Leiden and the number theory group at the IMB in Bordeaux. Especially to Peter Stevenhagen, Lenny Taelman, Marco Streng, Bart de Smit, Robin de Jong, Hendrik Lenstra, Rachel Newton, David Holmes, Boas Erez, Qing Liu, Fabien Pazuki, Dajano Tossici.

Thanks to Michiel and Alberto for being such great friends and for all the mathematical discussions we had. Alberto you are like a brother to me. Michiel, the best officemate ever (sorry Ariyan).

Thanks to Peter Bruin for all the nice discussions we had through the years. Thanks to Diego for being such a good friend and having spent days checking my English.

Thanks to all my dear friends in Bordeaux: Samuel, Nicola, Giovanni, Daniela, Bruno, for all the nice time spent together. Thanks to all the Leideners for this great year. Thanks to all my Leiden friends: Michiel, René, Ana, Renato, Dirk, Julian, Julien.

Un grazie di cuore alla mia famiglia per avermi sempre supportato, per essermi stata sempre vicino, nonostante la distanza. Grazie mamma e papà,

grazie sorellina. Grazie ai miei nonni, che ancora si lamentano perché li chiamo poco, e a tutti i miei zii.

Thanks to all the people with whom, through the years, I have shared a homemade dinner at my house: eating good food with great people is the perfect remedy for every kind of problem!

Curriculum Vitae

Samuele Anni was born on 20th June 1985 in Galliate, Italy. He grew up in Bellinzago Novarese, where he got his diploma at the "Liceo scientifico Alessandro Antonelli" in 2004.

He then started his bachelor in mathematics at the Università degli Studi di Pavia, where he became alumnus of "Almo Collegio Borromeo". In 2007 he finished his bachelor, and he started his master at the Università degli Studi di Pavia.

In 2008 he was part of the Erasmus project spending a semester at the Universitat de Barcelona. In 2010 he spent several months at Universitat de Barcelona and CRM thanks to the Erasmus Placement project. He wrote his master thesis, with title "Certifying exceptional primes for residual modular Galois representations", under the supervision of Professor Luis Dieulefait at the Universitat de Barcelona and Professor Alberto Canonaco at the Università degli Studi di Pavia, and he received his master degree in 2010.

In 2010 he was awarded an ALGANT-Doc joint Ph.D. fellowship to continue his studies in mathematics at Universiteit Leiden and Université Bordeaux 1, under the supervision of Professor Bas Edixhoven and Professor Pierre Parent.

He obtained a three-year Post-Doc fellowship at the University of Warwick for the research project "LMF: L-functions and Modular Forms" and he joined the Number Theory group there in October 2013.