Serre's Conjecture on 2-dimensional Galois representations

Denis Xavier Charles

Acknowledgments

I would like to thank Prof. Nigel Boston for offering the course on Fermat's Last Theorem. What was a wide foggy sea is now a clear and beautiful landscape after his lectures. My grateful thanks to Prof. Eric Bach for listening to my unpolished "lectures" on several parts of this article and for his insightful comments. I thank Rohit for all those coffee house brainstorming sessions, and Tal for conducting his enthusiastic weekly seminar. Thanks to Madhulika for her support in things great and small. I would like to add that this article contains no original material or content, except possibly in the errors it contains (for which I apologize in advance.)

Contents

CHAPTER 1

Introduction

Je vais essayer de dresser une liste des conjectures (ou "questions") que l'on peut faire dans la direction "formes modulaires - représentations galoisiennes".

Si f *est une forme modulaire* $\bmod p$ *sur* $\Gamma_0(N)$*, de poids* k*, fonction propre des opérateurs de Hecke* $T_{p'}$*, pour* p' *ne divisant pas* N*, et á coefficients dans* $\mathbb{F}_p$*, je noterai* ρ_f *la représentation de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *á valeurs dans* $\mathrm{GL}_2(\mathbb{F}_p)$ *correspondant á* f*. Et je dirai qu'une telle représentation est "modulaire"; et je dirai aussi, si j'en ai besoin, qu'elle est "de niveau* N *et de poids* k*". La question la plus ambitieuse que l'on pourrait se poser serait de donner un critère portant sur une représentation*

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_p)$$

qui permette d'affirmer que cette repreésentation est bien modulaire de niveau N *et de poids* k*. J'y reviendrai á la fin de cette lettre. Pour l'instant, je vais me concentrer sur les problémes que pose le poids 2. C'est ce dont on a besoin, si l'on veut prouver que "Weil +* $\epsilon \Rightarrow$ *Fermat".*

Serre, in a letter to Mestre, dated 13 August, 1985.

The work of Eichler and Shimura showed that for certain cusp forms of weight 2 and level N, we can associate 2-dimensional Galois representations over a finite field. This was generalized by Deligne [**Del69, DeS74**] to show that associated to every newform in $S_k(\Gamma_0(N), \epsilon)$ we can associate a Galois representation. Serre posed in 1975 the converse problem, of showing that certain 2-dimensional Galois representations over a finite field do indeed come from modular forms ([**Ser75**]). In the 1980s, Gerhard Frey had the idea that if Fermat's Last theorem was false, then this gives rise to an elliptic curve with strange properties, in particular he suspected that such a curve cannot be modular, thereby contradicting a conjecture of Shimura and Taniyama. With a view toward making this connection explicit, Serre set out to formulate his conjecture very precisely (called Serre's strong conjecture), which he accomplished in 1987 [**Ser87**]. Serre showed that a counter-example to Fermat's last theorem, gives a contradiction to this precise formulation of his conjecture. A sequence of further developments showed that the Shimura-Taniyama conjecture implies Fermat's last theorem, this result was proved by Ribet [**Rib90**] (this is the ϵ referred to in the above letter to Mestre). The connection to Fermat's Last theorem is explained in greater detail in [**Bos03**]. This conjecture of Serre remains a fundamental open problem in Number theory. Here we will be concerned mainly with the mechanics of the formulation of the conjecture and present some (paltry) evidence for it.

1.1. The statement of the conjecture

The weak form of Serre's conjecture is the following statement:

Weak Conjecture: *Let* $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *be the absolute Galois group. Suppose we are given a continuous representation:*

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

such that ρ *is irreducible and satisfies* $\det \rho(c) = -1$, *where* $c \in G_{\mathbb{Q}}$ *is complex conjugation. Then there is a cuspidal eigenform* f, *for some congruence subgroup, such that for all but finitely many primes* p, $\mathrm{Tr}\ \rho(\mathrm{Frob}_p) = \varphi(a_p(f))$. *Here* $a_p(f)$ *is the* p*-th Fourier coefficient of* f *and* $\varphi : \mathbb{Q}(\cdots, a_p(f), \cdots) \to \mathbb{F}_l$ *is a ring homomorphism.*

The strong version of the conjecture gives a recipe for the space $S_k(\Gamma_0(N), \epsilon)$ where the form f in the above conjecture resides.

Strong Conjecture: *With the same hypothesis as the* Weak Conjecture. *There is a cuspidal eigenform* $f \in S_k(\Gamma_0(N), \epsilon)$ *that satisfies the conclusions of the* Weak Conjecture, *where* k, N, ϵ *are described in the following sub-sections.*

Remark 1.1.1. We will restrict ourselves to the case where $\ell > 2$. For the case $\ell = 2$ the original recipe of Serre, needs to be modified so we simply ignore this case (see [**Edi92**]).

In the following sections we give basic definitions of the level and the character, but we give the value of the weight k only $\mod \ell - 1$. The definition of the actual weight is quite complicated and we relegate it to the chapter that concerns itself with aspects of the weight.

We will adopt the following notations. Let V be a 2-dimensional vector space over $\overline{\mathbb{F}}_\ell$. We are given a continuous homorphism

$$\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}(V).$$

The group $\mathrm{GL}(V)$ is discrete, so $\ker \rho = \rho^{-1}(I)$ is open. Thus $\ker(\rho)$ is of finite index in $G_{\mathbb{Q}}$ (as these are the open sets of the profinite group $G_{\mathbb{Q}}$), and so the representation factors through a finite extension of $\mathbb{Q}$. This also says that the image of ρ is a finite group, so it lies in $\mathrm{GL}(\mathbb{F}_{\ell^n})$ for a suitable n.

1.1.1. Definition of the level N. The integer N is simply the prime to ℓ part of the *Artin conductor* of the representation ρ (cf. [**Art30, Ser79**]). More precisely, let $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ be the absolute Galois group of the p-adic completion of $\mathbb{Q}$. There is an injection $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \hookrightarrow \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. This group comes with a filtration $G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots$ — the inertia subgroups (in the upper numbering scheme cf. [**Bos03**] Chapters 3 & 5 or [**Ser79**]). Let $V_i = V^{G_i}$ be the subspaces fixed by G_i. Set

$$n(p, \rho) = \sum_{0 \le i} \frac{1}{[G_0 : G_i]} \dim V/V_i. \tag{1.1.1}$$

This can also be written as

$$n(p, \rho) = \dim V/V_0 + \mathrm{Swan}(V)$$

where $\mathrm{Swan}(V)$ is the Swan conductor of the G_0-module V. Serre calls $\mathrm{Swan}(V)$ the "wild invariant" ([**Ser78**] §19.3).
We note the following properties:

(1) $n(p,\rho) \geq 0$ is an integer (see Chapter 3).
(2) $n(p,\rho) = 0$ iff $G_0 = \{1\}$, simply because each term is non-negative in (1.1.1). If $G_0 = \{1\}$, we call the representation *unramified* at p.
(3) $n(p,\rho) = \dim V/V_0$ if and only if $G_1 = \{1\}$. If $G_1 = \{1\}$, the representation is said to be *tamely ramified* at p.

Now the level N is defined by

$$N \stackrel{\triangleright}{=} \prod_{\ell \neq p} p^{n(p,\rho)}.$$

The "integer" defined above is an honest to God integer since $n(p,\rho) \neq 0$ only for finitely many primes p. This is essentially because the representation factors through a finite extension which is ramified only at finitely many primes.

1.1.2. Definition of the Character ε and $k \mod \ell - 1$. Taking the determinant of the representation ρ gives us a 1-dimensional representation, which we study to pick out the character. We have

$$\det \rho : G_{\mathbb{Q}} \to GL(\overline{\mathbb{F}}_\ell^*),$$

its image is a finite cyclic subgroup of $\overline{\mathbb{F}}_\ell^*$ of order prime to ℓ. Suppose the representation were modular (and we believe the recipe for N is the correct one) then comparing with the Deligne's theorem (Chapter 2), we find that the conductor of $\det \rho$ should be a divisor of ℓN. Thus $\det \rho$ can be identified with a homomorphism $(\mathbb{Z}/\ell N\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$. By the Chinese remainder theorem, this is equivalent (since $\ell \not| N$) to giving a pair of homomorphisms:

$$\varphi : (\mathbb{Z}/\ell\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$$

and

$$\varepsilon : (\mathbb{Z}/N\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*.$$

Since $(\mathbb{Z}/\ell\mathbb{Z})^*$ is cyclic of order $\ell - 1$, this homomorphism is of the form $x \mapsto x^h$ for some $h \in \mathbb{Z}/(\ell-1)\mathbb{Z}$. So it can be written as $\varphi = \chi^h$ where $\chi : G_{\mathbb{Q}} \to \mathbb{F}_\ell^*$ is the ℓ-th cyclotomic character i.e., the character that gives the action on $G_{\mathbb{Q}}$ on the ℓ-th roots of unity in $\overline{\mathbb{Q}}$. Again comparing with Deligne's prescription shows that $h \equiv k - 1 \mod \ell - 1$. This gives us the class of $k \mod \ell - 1$. Giving the exact value of k is *much* more involved, and again involves the action of ρ at local p-th decomposition groups.

1.2. Representations from Elliptic Curves

In case we know that the representation arises from an elliptic curve over $\mathbb{Q}$, we can show that Serre's conjecture is true. Let $E/\mathbb{Q}$ be an elliptic curve. Suppose ℓ is a prime (not dividing the conductor N_E of E) and $E[\ell]$ denotes the points on $E(\overline{\mathbb{Q}})$ of ℓ-torsion. This is a subgroup of E isomorphic to $(\mathbb{Z}/\ell\mathbb{Z}) \times (\mathbb{Z}/\ell\mathbb{Z})$. If $\sigma \in G_{\mathbb{Q}}$ and $P \in E[\ell]$ then so is P^σ. This gives us a 2-dimensional vector space over a finite field $\mathbb{F}_\ell$ on which $G_{\mathbb{Q}}$ acts continuously. Thus E gives rise to a Galois representation:

$$\rho_{E,\ell} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[\ell]) \cong GL_2(\mathbb{F}_\ell).$$

Suppose $p \not| N_E \ell$ is a prime then $\rho_{E,\ell}$ is unramified at p as the reduction $\mod p$ map on the points of ℓ torsion is injective for these primes. For such primes $\rho(\mathrm{Frob}_p)$ is well defined upto conjugation and its trace $\mathrm{Tr}\ \rho(\mathrm{Frob}_p)$ is well defined. It is known that $\mathrm{Tr}\ \rho(\mathrm{Frob}_p) = a_p \mod \ell$, where $a_p = p+1-\sharp\tilde{E}(\mathbb{F}_p)$. By the theorem of Breuil, Conrad, Diamond and Taylor following Wiles' work we know that there is a weight 2 cusp form of level N_E whose p-th Fourier coefficient is a_p (cf. [**BCDF00, Wil95, TWi95**]). Thus Serre's conjecture is true for such Galois representations.

1.3. Outline of the rest of the Article

In Chapter 2 we discuss the Eichler-Shimura construction which concerns itself with producing Galois representations given a cusp form. Chapter 3 takes up the task of motivating and clarifying the definition of the level recipe given by Serre. In particular we shall see a result of Carayol and Livné that says that if at all the representation is modular then the level of such a form is a multiple of the one given by Serre's recipe. Chapter 4 gives the full definition of the weight in Serre's conjecture. Throughout these two chapters we also discuss the level and weight optimization ideas and results which led to the proof that the Weak conjecture implies the Strong conjecture if $\ell > 2$. The last chapter gives some idea about the proof that Serre's conjecture is true if the image of the representation is in $\mathrm{GL}_2(\mathbb{F}_3)$, an important result which plays a crucial role in the work of Wiles.

CHAPTER 2

The Eichler-Shimura construction

Serre's conjecture states that certain 2-dimensional Galois representations over finite fields arise from modular forms. In this chapter we shall consider the other direction, where we start with a modular form and try to construct a Galois representation that is associated to it (in the sense of the previous chapter). The first avatar of this idea was in the construction of Eichler and Shimura who showed how to construct such a representation given a newform in $S_2(\Gamma_0(N))$. A general construction of such representations from newforms in $S_k(\Gamma_0(N), \epsilon)$ remained a thorny open problem resisting several attacks [**Iha67, KSh65, Ser67**], until in a brilliant paper by Deligne [**Del69**] the construction for $S_k(\Gamma_0(N))$ for $k \geq 2$ was solved. In subsequent papers [**DeS74, Car86**] all the remaining cases were worked out. The complete account of the whole proof with all the details is available in the Conrad's book [**Con99**].

We will restrict our study to the weight 2 case, i.e., the Eichler-Shimura construction. Recall the basic steps involved ([**Bos03**] Chapter 4): We are given a newform $f \in S_2(\Gamma_0(N))$ which in particular is an eigenform for the Hecke algebra $\mathbb{T}$. This gives us a packet of data a_p for each p prime, where $f = \sum_{1 \leq n} a_n q^n$ and a_p is the p-th coefficient. Since f is a newform, its fourier coefficients are algebraic integers and $K = \mathbb{Q}(\cdots, a_n, \cdots)$ is a finite extension. Let $\mathcal{O}_f$ be the ring of integers of K. Given a prime ℓ, let λ be a prime lying over ℓ in K and let K_λ be the completion of K at the place λ. Our task is to engineer a continuous representation $\rho_\lambda : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(K_\lambda)$ such that $\mathrm{Tr}\ \rho(\mathrm{Frob}_p) = a_p$ for all but finitely many primes p. We will first construct a $G_{\mathbb{Q}}$-module. Our beginning observation is that if $\omega \in S_2(N) \stackrel{\triangleleft}{=} S_2(\Gamma_0(N))$ then ω is a holomorphic differential form on $X_0(N) = (\mathfrak{h}/\Gamma_0(N))^*$. Let $C_1, \cdots, C_{2g}$ be generators for $H_1(X_0(N), \mathbb{Z})$ as a free abelian group (g is the genus of $X_0(N)$). Let $V = \mathrm{Hom}(S_2(\Gamma_0(N)), \mathbb{C})$. The map that sends $C \in H_1(X, \mathbb{Z})$ to V giving the map $\omega \mapsto \int_C \omega$ has discrete image, a subgroup of $\mathbb{C}^g$ i.e., a lattice Λ of rank $2g$. The quotient V/Λ is called the Jacobian of $X_0(N)$ which we denote $J_0(N)$. The description of $J_0(N)$ as this quotient makes it easy to see that it is an abelian variety. Hence, it comes with the multiplication by ℓ^n maps (which we denote $[\ell^n]$) and we can look at the corresponding torsion subgroups $J_0(N)[\ell^n] = \{P \ : \ [\ell^n]P = 0\}$. Patching these together we get the ℓ-adic Tate module of $J_0(N)$, $T_\ell(J_0(N)) = \varprojlim J_0(N)[\ell^n] \cong \mathbb{Z}_\ell^{2g}$. $J_0(N)$ being defined over $\mathbb{Q}$ with the multiplication maps also defined over $\mathbb{Q}$ gives us a module on which $G_{\mathbb{Q}}$ acts. We cannot use this module for defining our Galois representation as it has rank $2g$ and not 2. Here comes a miraculous fact: if we set $W \stackrel{\triangleright}{=} T_\ell(J_0(N)) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ then as a $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$-module this is rank 2. Where the Hecke operators act on $\mathrm{Div}^0(X_0(N))$ and preserve principal divisors (and hence act on the degree 0 portion of the Picard group which is $J_0(N)$) by extending $T_m[z] = \sum [\alpha_i z]$ linearly, where α_i runs through matrices $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, $ad = N, d > 0, \gcd(a, N) = 1$ and $0 \leq b < d$. This yields a representation

$G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q}_\ell)$. Since f is a newform, the map $\mathbb{T} \to \mathcal{O}_f$ given by $T_p \to a_p$ is a ring homomorphism called the eigencharacter of f. Composing the representation with the eigencharacter we get a representation $G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O}_f \otimes \mathbb{Q}_\ell) \cong \mathrm{GL}_2(\prod_{\lambda'} K_{\lambda'})$ where λ' runs over primes above ℓ. Mapping onto the λ-th factor gives us the representation $\rho_\lambda : G_{\mathbb{Q}} \to \mathrm{GL}_2(K_\lambda)$. There still remains the task of showing that this is the required representation, namely has trace of Frobenius at p equal to the a_p. This is actually hard and we will only outline the proof in the following sections.

Our description of the Eichler-Shimura construction follows the elegant exposition in [**RiS01**] by Conrad and Chapter 3 in [**Con99**]. In what follows we shall use the moduli space $X_1(N)$ instead of $X_0(N)$ which parametrizes elliptic curves with a chosen point of *exact* order N. Since we are only giving a detailed overview, we shall skip the many compatibility checks that must be performed between the analytic theory, algebraic geometry and the theory of modular forms.

2.1. The Analytic Side

Let $N \geq 5$ be an integer and let $X_1(N)^{an}$ denote the compactification of the curve $Y_1(N)^{an} = \Gamma_1(N)\backslash\mathfrak{H}$, where

$$\Gamma_1(N) \stackrel{\triangleright}{=} \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod N \right\} \subseteq \mathrm{SL}_2(\mathbb{Z}).$$

For $N < 5$, $X_1(N)^{an}$ has genus 0 and $\dim S_2(\Gamma_1(N)) = 0$ so there is no loss of generality in our assumption that $N \geq 5$. Now $S_2(\Gamma_1(N))$ is the space of holomorphic differential 1-forms on $X_1(N)$ and in terms of cohomology this says

$$H^0(X_1(N), \Omega^{1,hol}_{X_1(N)^{an}}) \cong S_2(\Gamma_1(N)).$$

The Hodge decomposition for the compact Kähler manifold $X_1(N)^{an}$ says that:

$$\begin{aligned} H^1(X_1^{an}, \underline{\mathbb{Z}}) \otimes_{\mathbb{Z}} \mathbb{C} &\cong H^1(X_1^{an}, \underline{\mathbb{C}}) \\ &\cong \bigoplus_{p+q=1} H^{p,q}(X_1(N)^{an}) \\ &= H^{1,0}(X_1(N)^{an}) \oplus H^{0,1}(X_1(N)^{an}) \\ &= H^0(X_1(N)^{an}, \Omega^{1,hol}_{X_1(N)^{an}}) \oplus H^0(X_1(N)^{an}, \overline{\Omega}^{1,hol}_{X_1(N)^{an}}) \\ &= S_2(\Gamma_1(N)) \oplus \overline{S_2(\Gamma_1(N))} \end{aligned}$$

(the notation $\underline{A}$ for an abelian group A refers to the constant sheaf associated to A). This is called the weight-2 *Shimura Isomorphism*. We know that the Hecke operators act on the space $S_2(\Gamma_1(N))$, we would like to construct geometric operations on $X_1(N)^{an}$ which induce actions on $H^1(X_1^{an}(N), \underline{\mathbb{Z}})$ that under the isomorphism correspond to the Hecke operators. We would like to show that the geometric operations that we construct are "natural", this entails understanding $X_1(N)^{an}$ as a certain moduli space, which then comes naturally with some maps.

Let $z \in \mathfrak{H}$, associate to this point the elliptic curve given by the complex analytic description $E_z = \mathbb{C}/[1, z]$ and $1/N$ is a point of exact order N on E_z. Under the action of $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N)$ a lattice $\mathcal{L} = [\omega_1, \omega_2]$ is sent to $\mathcal{L}' = [\omega_1', \omega_2']$ where $\omega_1' = a\omega_1 + b\omega_2, \omega_2' = c\omega_1 + d\omega_2$. Since

$c \equiv 0 \mod N$ and $d \equiv 1 \mod N$, we get $\omega_2' \equiv \omega_2 \mod N\mathcal{L}$ or in other words $\frac{1}{N}\omega_2' \equiv \frac{1}{N}\omega_2 \mod \mathcal{L}$, since $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ the two lattices are the same, and this shows that points of exact order N get sent to points of exact order N. Thus the association of the elliptic curve E_z to $z \in \mathfrak{H}$ shows that we can identify $Y_1(N)^{an}$ as the *set* of isomorphism classes (E, P) consisting of an elliptic curve $E/\mathbb{C}$ and a point $P \in E$ of exact order N. Now consider the intrinsic map $Y_1(N)^{an} \to Y_1(N)^{an}$ given by $(E, P) \mapsto (E, nP)$ where $n \in (\mathbb{Z}/N\mathbb{Z})^*$, this is given by the action of any matrix $\gamma_n \in SL_2(\mathbb{Z}), \gamma_n \equiv \begin{pmatrix} n^{-1} & * \\ 0 & n \end{pmatrix} \mod N$ on $Y_1(N)^{an}$. The action of γ_n extends to an action on $X_1(N)^{an}$ which we denote I_n.

There is another map induced by the involution $z \mapsto \frac{-1}{Nz}$ on $\mathfrak{H}$ this extends to a map $w_N : X_1(N)^{an} \to X_1(N)^{an}$. There is a generalization of this map which we give conceptually as follows: Let $\langle\ ,\ \rangle_N$ be the Weil pairing on N-torsion points on an elliptic curve E (with sign convention as in [**Mum70**] Chapter IV, §20). Then given $\zeta \in \mu_N(\mathbb{C})$ a primitive N-th root of unity, define the map ω_ζ that sends the pair (E, P) to $(E/\langle P\rangle, P' \mod P)$ where $P' \in E$ has exact order N and $\langle P', P\rangle_N = \zeta$. Thus we have induced maps on the cohomology:

$$w_\zeta^*, I_n^* : H^1(X_1(N)^{an}, \underline{\mathbb{Z}}) \to H^1(X_1(N)^{an}, \underline{\mathbb{Z}}),$$

we will write $\langle n\rangle^*$ instead of I_n^*.

Let p be a prime and define $\Gamma_1(N, p) = \Gamma_1(N) \cap \Gamma_0(p)$ when $p \nmid N$ and $\Gamma_1(N, p) = \Gamma_1(N) \cap \Gamma_0(p)^t$ when $p \mid N$ where $\Gamma_0(p)^t$ is the transpose of $\Gamma_0(p)$. Define $Y_1(N, p)^{an}$ to be $\Gamma_1(N, p)\backslash\mathfrak{H}$ and set $X_1^{an}(N, p)$ to be the compactification of $Y_1(N, p)^{an}$. By the maps

$$z \mapsto \left(\mathbb{C}/[1, z], \frac{1}{N}, \langle\frac{1}{p}\rangle\right)$$

when $p \nmid N$ and

$$z \mapsto \left(\mathbb{C}/[1, z], \frac{1}{N}, \langle\frac{z}{p}\rangle\right)$$

when $p \mid N$, we can identify $Y_1(N, p)^{an}$ as the set of isomorphism classes of (E, P, C) where E is an elliptic curve, P a point of exact order N and $C \subseteq E$ is a cyclic subgroup of order p, meeting $\langle P\rangle$ trivially.

There are unique analytic maps corresponding to the following conceptual maps: $\pi_1^{(p)}, \pi_2^{(p)} : X_1(N, p)^{an} \to X_1(N, p)^{an}$, given by $\pi_1^{(p)}(E, P, C) = (E, P)$ the "forgetful" map, and $\pi_2^{(p)}(E, P, C) = (E/C, P \mod C)$. We get a pullback map on cohomology by

$$(\pi_2^{(p)})^* : H^1(X_1(N)^{an}, \underline{\mathbb{Z}}) \to H^1(X_1(N, p), \underline{\mathbb{Z}}).$$

The map $\pi_1^{(p)}$ is a finite holomorphic map and we can take the trace ([**GrH78**] Chapter 5) to define the map $(\pi_1^{(p)})_* : H^1(X_1(N, p), \underline{\mathbb{Z}}) \to H^1(X_1(N)^{an}, \underline{\mathbb{Z}})$. Define

$$T_p^* = (\pi_1^{(p)})_* \circ (\pi_2^{(p)})^* : H^1(X_1(N)^{an}, \underline{\mathbb{Z}}) \to H^1(X_1(N)^{an}, \underline{\mathbb{Z}}).$$

The following compatibility theorem whose general form is given as Proposition 3.18, 3.19 in [**Del69**] states:

THEOREM 2.1.1. *The weight-2 Shimura isomorphism*

$$Sh_{\Gamma_1(N)} : S_2(\Gamma_1(N)) \oplus \overline{S_2(\Gamma_1(N))} \cong H^1(X_1(N)^{an}, \underline{\mathbb{Z}}) \otimes_{\mathbb{Z}} \mathbb{C}$$

identifies $\langle n\rangle \oplus \overline{\langle n\rangle}$ *with* $\langle n\rangle^* \otimes 1$, $T_p \oplus \overline{T_p}$ *with* $T_p^* \otimes 1$ *and* $w_N \oplus \overline{w}_N$ *with* $w^*_{e^{2\pi\imath/N}} \otimes 1$.

Let $\mathbb{T}_1(N) \subseteq \mathrm{End}_{\mathbb{Z}}(H^1(X_1(N)^{an}, \underline{\mathbb{Z}}))$ be the subring generated by the T_p^* and $\langle n\rangle^*$, Theorem 2.1.1 shows that via the Shimura isomorphism this is identified with the classical weight-2 Hecke operators of level N.

There is another compatibility between the cup product on $H^1(X_1(N), \underline{\mathbb{Z}})$ and the Petersson scalar product on $S_2(\Gamma_1(N))$. For $f, g \in S_2(\Gamma_1(N))$ define

$$\langle f, g\rangle_{\Gamma_1(N)} = \int_{\Gamma_1(N)\backslash\mathfrak{H}} f(z)\overline{g}(z)dxdy.$$

Since $X_1(N)^{an}$ is a curve we have that $H^2(X_1(N)^{an}, \underline{\mathbb{Z}}) \cong \mathbb{Z}$. The cup product on cohomology gives us another pairing

$$(\ ,\ )_{\Gamma_1(N)} : H^1(X_1(N)^{an}, \underline{\mathbb{Z}}) \otimes_{\mathbb{Z}} H^1(X_1(N)^{an}, \underline{\mathbb{Z}}) \to H^2(X_1(N)^{an}, \underline{\mathbb{Z}}) \cong \mathbb{Z}.$$

After base change to $\mathbb{C}$, this pairing enjoys the following compatibility:

THEOREM 2.1.2. *Under the weight-2 Shimura isomorphism* $Sh_{\Gamma_1(N)}$ *we have*

$$(Sh_{\Gamma_1(N)}(f_1 + \overline{g}_1), Sh_{\Gamma_1(N)}(f_2 + \overline{g}_2))_{\Gamma_1(N)} = 4\pi(\langle f_1, g_1\rangle_{\Gamma_1(N)} - \langle f_2, g_2\rangle_{\Gamma_1(N)}).$$

Set $[x, y]_{\Gamma_1(N)} = (x, w_\zeta^* y)_{\Gamma_1(N)}$ with $\zeta = e^{2\pi/N}$. Then we get the following corollary of Theorem 2.1.2

COROLLARY 2.1.3. *The action of* $\mathbb{T}_1(N)$ *on* $H^1(X_1(N)^{an}, \underline{\mathbb{Z}})$ *is equivariant with respect to the pairing* $[\cdot,\cdot]_{\Gamma_1(N)}$, *i.e.,*

$$[x, Ty]_{\Gamma_1(N)} = [Tx, y]_{\Gamma_1(N)}$$

for all $T \in \mathbb{T}_1(N)$. *With respect to* $(\ ,\ )_{\Gamma_1(N)}$, *the adjoint of* T_p^* *for* $p \nmid N$ *is* $\langle p^{-1}\rangle^* T_p^*$ *and the adjoint of* $\langle n\rangle^*$ *is* $\langle n^{-1}\rangle^*$ *for* $n \in (\mathbb{Z}/N\mathbb{Z})^*$.

Now we focus our attention on the Jacobian with a view towards reformulating our maps with respect to it. For any compact Riemann surface X, we have an isomorphism of complex Lie groups $\mathrm{Pic}^0_X \cong H^1(X, \mathcal{O}_X)/H^1(X, \underline{\mathbb{Z}})$. If $f : X \to Y$ is a finite map between compact Riemann surfaces, then we get a natural trace map

$$f_* : H^1(X, \mathcal{O}_X) \cong H^1(Y, f_*\mathcal{O}_X) \to H^1(Y, \mathcal{O}_Y).$$

It turns out that this trace map is compatible with the other trace map encountered earlier. Given any finite map $f : X \to Y$ gives rise to the following commutative diagrams:

$$\begin{array}{ccc} H^1(Y,\mathcal{O}_Y) & \xrightarrow{f^*} & H^1(X,\mathcal{O}_X) \\ \uparrow & & \uparrow \\ H^1(Y,\underline{\mathbb{Z}}) & \xrightarrow{f^*} & H^1(X,\underline{\mathbb{Z}}) \end{array} \qquad \begin{array}{ccc} H^1(X,\mathcal{O}_X) & \xrightarrow{f_*} & H^1(Y,\mathcal{O}_Y) \\ \uparrow & & \uparrow \\ H^1(X,\underline{\mathbb{Z}}) & \xrightarrow{f_*} & H^1(Y,\underline{\mathbb{Z}}) \end{array}$$

with the column maps induced by the canonical maps $\underline{\mathbb{Z}} \to \mathcal{O}_Y$ and $\underline{\mathbb{Z}} \to \mathcal{O}_X$.
Passing to quotients on the columns gives rise to the maps

$$f^* : \mathrm{Pic}^0_Y \to \mathrm{Pic}^0_X,\ f_* : \mathrm{Pic}^0_X \to \mathrm{Pic}^0_Y$$

of analytic Lie groups. It turns out that these maps are precisely those induced by Pic^0 and Albanese functoriality ([**GrH78**], Chapter 2 §6), so that $f^* = \mathrm{Pic}^0(f)$ and $f_* = \mathrm{Alb}(f)$. Now we define endomorphisms of the Jacobian $\mathrm{Pic}^0_{X_1(N)^{an}}$ via

$$T_p^* = \mathrm{Alb}(\pi_1^{(p)}) \circ \mathrm{Pic}^0(\pi_2^{(p)}),\ \langle n\rangle^* = \mathrm{Pic}^0(I_n),\ w_\zeta^* = \mathrm{Pic}^0(w_\zeta)$$
$$(T_p)_* = \mathrm{Alb}(\pi_2^{(p)}) \circ \mathrm{Pic}^0(\pi_1^{(p)}),\ \langle n\rangle_* = \mathrm{Alb}(I_n), (w_\zeta)_* = \mathrm{Alb}(w_\zeta).$$

Taking the ℓ-adic Tate module of the Jacobian, we find:

$$T_\ell(\mathrm{Pic}^0_{X_1(N)^{an}}) \cong H^1(X_1(N)^{an}, \underline{\mathbb{Z}}_\ell) \tag{2.1.2}$$
$$\cong H^1(X_1(N)^{an}, \underline{\mathbb{Z}}) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell. \tag{2.1.3}$$

Thus our struggle has given us the Tate module of an abelian variety on which our Hecke operators act by the Shimura isomorphism. We do not yet have a Galois action, this is the subject of the next section. We thus have that $\mathbb{T}_1(N)$ acts on $\mathrm{Pic}^0_{X_1(N)}$ in a unique manner compatible with the above definition, and (2.1.2) is an isomorphism of $\mathbb{T}_1(N) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$-modules.

Let $V_\ell(N) = \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_\ell(\mathrm{Pic}^0_{X_1(N)^{an}})$ this comes with a perfect alternating Weil pairing $(\ ,\ )_\ell : V_\ell(N) \otimes V_\ell(N) \to \mathbb{Q}_\ell$ and has two $\mathbb{Q}_\ell \otimes \mathbb{T}_1(N)$-actions coming from the $()^*$ and $()_*$ actions. As $w_\zeta^{-1} = w_\zeta$ we find that $(w_\zeta)_* = w_\zeta^*$, and we write w_ζ for this operator.

THEOREM 2.1.4. *Let $\mathbb{T}_1(N)$ act on $V_\ell(N)$ with respect to the $()^*$-action or with respect to the $()_*$-action. With respect to $(\ ,\ )_\ell$, the adjoint of T_p for $p \nmid N$ is $\langle p\rangle^{-1}T_p$ and the adjoint of $\langle n\rangle$ is $\langle n\rangle^{-1}$ for $n \in (\mathbb{Z}/N\mathbb{Z})^*$. With respect to $[x,y]_\ell = (x, w_\zeta(y))_\ell$ for $\zeta \in \mu_N(\mathbb{C})$ a primitive Nth root of unity, the action of $\mathbb{T}_1(N)$ on $V_\ell(N)$ is self-adjoint. In general, adjointness with respect to $(\ ,\ )_\ell$ interchanges the $()_*$ and $()^*$ actions.*

We finally come to the following important corollary:

COROLLARY 2.1.5. *The $\mathbb{Q}_\ell \otimes_{\mathbb{Z}} \mathbb{T}_1(N)$-module $V_\ell(N)$ is free of rank 2 for either action and $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{T}_1(N), \mathbb{Q})$ is free of rank 1 over $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{T}_1(N)$.*

Proof :(Sketch) We sketch the proof of the first assertion, which by (2.1.2) reduces to showing $H^1(X_1(N)^{an}, \mathbb{Q})$ is free of rank 2 over $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{T}_1(N)$. Using $[\ ,\ ]_{\Gamma_1(N)}$, we see that

$$H^1(X_1(N)^{an}, \mathbb{Q}) \cong \mathrm{Hom}_{\mathbb{Q}}(H^1(X_1(N)^{an}, \underline{\mathbb{Q}}), \mathbb{Q})$$

as $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{T}_1(N)$-modules. A series of reductions shows that it suffices to show that

$$\mathrm{Hom}_{\mathbb{C}}(H^1(X_1(N)^{an}, \underline{\mathbb{C}}), \mathbb{C})$$

is free of rank 2 over $\mathbb{T}_1(N) \otimes_{\mathbb{Z}} \mathbb{C}$. Now by the Shimura isomorphism which is compatible with Hecke actions, this is reduced to showing that $\mathrm{Hom}(S_2(\Gamma_1(N)), \mathbb{C})$ is free of rank 1 over $\mathbb{C} \otimes_{\mathbb{Z}} \mathbb{T}_1(N)$. For this, we study the $\mathbb{C} \otimes \mathbb{T}_1(N)$-equivariant $\mathbb{C}$-bilinear pairing

$$S_2(\Gamma_1(N), \mathbb{C}) \otimes_{\mathbb{C}} (\mathbb{C} \otimes \mathbb{T}_1(N)) \to \mathbb{C}$$

by $(f, T) \mapsto a_1(Tf)$, where $a_n(\cdot)$ is the n-th Fourier coefficient. This is $\mathbb{C} \otimes \mathbb{T}_1(N)$-equivariant, as $\mathbb{T}_1(N)$ is commutative. We verify that the kernel on either side is trivial. The map $\mathbb{C} \otimes \mathbb{T}_1(N) \to \mathrm{End}_{\mathbb{C}}(S_2(\Gamma_1(N)))$ is injective. Now suppose $(f, T) = 0$ for all T then since $(f, T_n) = a_1(T_n(f)) = a_n(f) = 0$ we see that $f = 0$ so there is no kernel on the left. Now if $(f, T) = 0$ for all f, then applying this to $T_n f$, we see that $a_1(T(T_n f)) = a_n(Tf) = 0$ showing that $Tf = 0$ or that T is 0 by the injection of the Hecke algebra into $\mathrm{End}_{\mathbb{C}}(S_1(\Gamma_1(N)))$. $\square$

2.2. The Algebraic Side

This section will be more sketchy as a proper discussion of it needs a good understanding of scheme theoretic methods. The aim now given the work we did in the previous section, is to endow $V_\ell(N)$ with a Galois action, and finally tie up the relation between the Frobenius action and geometric Hecke action under the representation that we get. It is known that for $N \geq 5$, we can produce a proper smooth $\mathbb{Z}[\frac{1}{N}]$-scheme $X_1(N)$ equipped with a "nice" map to $\mathbb{P}^1_{\mathbb{Z}[\frac{1}{N}]}$, such that an open subscheme $Y_1(N)$ lying above the affine piece $\mathbb{P}^1_{\mathbb{Z}[\frac{1}{N}]} - \{\infty\}$ is the base of a universal object for elliptic curves with a point of exact order N over variable $\mathbb{Z}[\frac{1}{N}]$-schemes [**KaM85**]. The point is that base change of this scheme $X_1(N)$ upto $\mathbb{C}$ recovers $X_1(N)^{an}$ with the isomorphism carrying the moduli data compatibly. Similarly one defines $X_1(N, p)$ now a proper smooth $\mathbb{Z}[\frac{1}{Np}]$ scheme, whose base change to $\mathbb{C}$ recovers $X_1(N, p)^{an}$.

Analogous to the previous section, we can define the maps $\langle n \rangle^*$, $\langle n \rangle_*, w_\zeta^*, T_p^*, (T_p)_*$, it turns out as before that $w_\zeta^* = (w_\zeta)_*$. Analytization then recovers the same operators that we defined earlier. Let $\mathbb{T}_1^{alg}(N)$ be the subring of $\mathrm{End}(\mathrm{Pic}^0_{X_1(N)})$ generated by T_p^* and $\langle n \rangle^*$. It turns out that $\mathbb{T}_1^{alg}(N)$ is identified with $\mathbb{T}_1(N)$ defined earlier by

$$\varprojlim \mathrm{Pic}^0_{X_1(N)/\mathbb{Z}[\frac{1}{N}]}[\ell^n](\overline{\mathbb{Q}}) \cong T_\ell(\mathrm{Pic}^0_{X_1(N)^{an}}). \tag{2.2.4}$$

Now this gives our $V_\ell(N)$ with a canonical continuous Galois action! By Néron-Ogg-Shafarevich ([**SeT68**] Theorem 1) we have that this action is unramified at all $p \nmid N\ell$. We summarize our progress in this lemma:

LEMMA 2.2.1. *Let $\mathbb{T}_1(N)$ act on $V_\ell(N)$ through either the $()^*$-action on $()_*$-action. Then $\rho_{N,\ell} : G_{\mathbb{Q}} \to \mathrm{Aut}(V_\ell(N)) \cong \mathrm{GL}_2(\mathbb{Q}_\ell \otimes \mathbb{T}_1(N))$ is a continuous representation, unramified at $p \nmid N\ell$.*

Of course, the mystery is why should the p-th Frobenius action and the p-th Hecke operator have the same trace. Unfortunately we will not be able to show this fact here, referring the interested reader to [**RiS01**] §5.3 instead. We state what we need as the following theorem:

THEOREM 2.2.2. *Let* $\mathbb{T}_1(N)$ *act on* $\mathrm{Pic}^0_{X_1(N)/\mathbb{Z}[\frac{1}{N}]}$ *via the* $()_*$*-action. For any* $p \nmid N\ell$*, the characteristic polynomial of* $\rho_{N,\ell}(\mathrm{Frob}_p)$ *is*

$$X^2 - (T_p)_* X + p\langle p\rangle_*$$

relative to the $\mathbb{Q}_\ell \otimes \mathbb{T}_1(N)$*-module structure on* $V_\ell(N)$*, where* Frob_p *denotes an arithmetic Frobenius element at* p*.*

Note that upto now, our discussion has been pretty generic and we have not yet used the newform $f \in S_2(\Gamma_1(N))$. This is where we specialize the situation to the form f. Let $K_f = \mathbb{Q}(\cdots, a_p, \cdots)$ where a_p is the p-th fourier coefficient of f. Assume that χ_f the Nebentypus character of f also takes values in K_f. Now consider the eigencharacter map $T_f : \mathbb{T}_1(N) \to K_f$, by $T_p \mapsto a_p$. Let $\mathfrak{p}_f = \ker(T_f)$, this is a prime ideal as the image is an integral domain.

Let A_f be the quotient of $\mathrm{Pic}^0_{X_1(N)/\mathbb{Z}[\frac{1}{N}]}$ by $\mathfrak{p}_f$. The action of $\mathbb{T}_1(N)$ on $\mathrm{Pic}^0_{X_1(N)}$ induces an action of $\mathbb{T}_1(N)/\mathfrak{p}_f$ on A_f and hence an action of $K_f \cong (\mathbb{T}_1(N)/\mathfrak{p}_f \otimes \mathbb{Q})$ on it.
Then we have:

THEOREM 2.2.3. *(Shimura) We have* $\dim A_f = [K_f : \mathbb{Q}]$ *and* $V_\ell(A_f)$ *is free of rank* 2 *over* $\mathbb{Q}_f \otimes_{\mathbb{Q}} K_f$*, with* Frob_p *having characteristic polynomial,*

$$X^2 - (1 \otimes a_p(f))X + 1 \otimes p\chi_f(p)$$

for all $p \nmid N\ell$*.*

Choosing a place λ of K_f over ℓ we deduce:

COROLLARY 2.2.4. *Let* $f \in S_2(\Gamma_1(N))$ *be a newform and* λ *a place of* K_f *over* ℓ*. There exists a continuous representation* $\rho_{f,\lambda} : G_{\mathbb{Q}} \to \mathrm{GL}_2(K_{f,\lambda})$ *unramified at all* $p \nmid N\ell$*, with* Frob_p *having characteristic polynomial*

$$X^2 - a_p(f)X + p\chi_f(p) \in K_{f,\lambda}[X].$$

Suppose now we are given a newform f in $S_k(\Gamma_1(N))$ for $k \geq 2$, we can reduce the problem of finding a Galois representation associated to f, to the case of $k = 2$ in the case that we are only looking for mod λ congruences between the traces. This is discussed for example in Gross's paper [**Gro90**].

CHAPTER 3

The Level

Let $\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_\ell)$ be an irreducible representation that arises from a modular form. Since there are many congruences between modular forms, it turns out that such a representation could arise from an infinite number of modular forms. The strong form of Serre's conjecture predicts the optimal weight and level of a modular form from which this representation could arise. In §1.1.1 we gave a definition of Serre's prescription for the optimal level for such a form. The optimal level which we shall denote by $N(\rho)$ is the prime to ℓ part of the Artin conductor. The Artin conductor is obtained by looking at the local representations the ρ yields of $\mathbb{G}_{\mathbb{Q}_p}$ for every prime p and defining certain exponents $n(\rho, p)$. From the definition of $n(\rho, p)$ given in (1.1.1), it is not even clear that this is an *integer*! In the next section we will outline the proof that $n(\rho, p)$ is an integer. In §3.2 we look at a result of Carayol and Livné that shows that any modular form that gives rise to ρ must come from a level that is a multiple of N. Since $\ell \not| N(\rho)$, we must be able to remove the prime ℓ from the level of the modular form giving rise to ρ, this will be the subject of §3.3. Finally, in §3.4 we give a brief idea of how general level lowering is achieved by a reduction to the weight 2 case.

3.1. The Artin Conductor of ρ

To give a proof of the integrality of the $n(\rho, p)$, we need to digress a bit and discuss Ramification groups. We will simply collect some of the relevant facts and state the important Hasse-Arf theorem. Then we will define the Artin representation of the Galois group of a local field, and then state Artin's fundamental theorem regarding this representation. The integrality of $n(\rho, p)$ follows as an easy corollary of this theorem. Our principal reference is Serre's book *Local fields* [**Ser79**], the presentation here is simply a weak shadow of the one given there.

Notation: For the following subsections, we adopt the following notations and conventions. K will denote a local field, complete under a discrete valuation v_K. Let $A_K = \{x \in K \mid v_K(x) \geq 0\}$ be the valuation ring corresponding to v_K, i.e., its ring of integers. Let $\mathfrak{p}_K = \{x \in K \ : \ v_K(x) > 0\}$ be its unique maximal ideal, and let $\overline{K} = A_K/\mathfrak{p}_K$ be its residue field, and $U_K = A_K - \mathfrak{p}_K$. We will only consider separable extensions L of K. In this case, we know that A_L the integral closure of A_K in L is again a complete discrete valuation ring (cf. [**Ser79**] Chapter II §2). Define $v_L, \mathfrak{p}_L, U_L$ and $\overline{L}$ as above. We will also assume that $\overline{L}/\overline{K}$ is separable. In the case that we are interested in the residue fields will be finite and since these fields are perfect, this assumption will not be a restriction. The ramification index of $\mathfrak{p}_L$ in L/K is denoted $e_{L/K}$ and the residue class degree $f_{L/K}$ so that $e_{L/K}f_{L/K} = [L : K]$.

3.1.1. Definition of the Ramification Groups. Let L/K be a *Galois* extension in addition to the above assumptions and let $G = \mathrm{Gal}(L/K)$ be its Galois group. G acts on the ring A_L. We

know that there is an element $x \in A_L$ which generates A_L as an A_K-algebra (cf. [**Ser79**] Chapter III).

LEMMA 3.1.1. *Let $\sigma \in G$ and $i \geq -1$ an integer. Then the following are equivalent:*

(1) σ operates trivially on $A_L/\mathfrak{p}_L^{i+1}$;
(2) For all $a \in A_L$, $v_L(\sigma(a) - a) \geq i + 1$;
(3) $v_L(\sigma(x) - x) \geq i + 1$.

Proof : (1) $\Leftrightarrow$ (2) is trivial. The image of x in $A_L/\mathfrak{p}_L^{i+1}$ generates A_i as an A_K-algebra, and thus (3) is equivalent to the first two conditions. $\square$

PROPOSITION 3.1.2. *Let $i \geq -1$ be an intger, let $G_i \stackrel{\triangleright}{=} \{\sigma \in G : \sigma fixes A_L/\mathfrak{p}_L^{i+1}\}$. Then $G_i \trianglerighteq G_{i+1}$ forming a decreasing sequence of normal subgroups of G. Furthermore, if i is sufficiently large G_i is $\{1\}$.*

Proof : The G_i are normal by assertion (1) of Lemma 3.1.1. The last assertion follows from the fact that if $i \geq \sup_{\sigma \neq 1}\{v_L(\sigma(x) - x)\}$ then G_i is trivial. $\square$

G_i is called the ith *ramification group* of G. Note that $G_{-1} = G$. G_0 is called the *inertia subgroup* of G. The quotient $G/G_0 \cong \mathrm{Gal}(\overline{L}/\overline{K})$ which is cyclic of order equal to the residue class degree $f_{L/K}$ if $\overline{K}$ is a finite field (cf. [**Ser79**] Chapter I). We define a certain *index* function of the group G as follows:

$$i_G(\sigma) = v_L(\sigma(x) - x). \tag{3.1.5}$$

If $\sigma \neq 1$, then $i_G(\sigma)$ is a non-negative integer and $i_G(1) = +\infty$. The index function gives the index (off by 1 actually) of the "deepest" ramification group in which σ sits. It enjoys the following properties:

$$\begin{aligned} i_G(\sigma) \geq i + 1 &\Leftrightarrow \sigma \in G_i \\ i_G(\psi\sigma\psi^{-1}) &= i_G(\sigma) \\ i_G(\sigma\tau) &\geq \inf(i_G(\sigma), i_G(\tau)). \end{aligned}$$

Let $H \trianglelefteq G$ be a normal subgroup and let K' be the fixed field of H. Thus G/H can be indentified with the Galois group of K'/K. The index function satisfies the following nice property:

PROPOSITION 3.1.3. *For $\sigma \in G/H$,*

$$i_{G/H}(\sigma) = \frac{1}{e_{L/K'}} \sum_{s \to \sigma} i_G(s).$$

Next we collect properties of the quotient G_i/G_{i+1} for $i \geq 0$. For this purpose, we define a filtration of the group of units U_L by:

$$\begin{aligned} U_L^{(0)} &= U_L \\ U_L^{(i)} &= 1 + \mathfrak{p}_L^i \text{ for } i \geq 1. \end{aligned}$$

Its easy to see that $U_L = \varprojlim U_L/U_L^{(i)}$.

The structure of $U_L^{(i)}/U_L^{(i+1)}$ is described by the following proposition:

PROPOSITION 3.1.4. *The quotient* $U_L^{(0)}/U_L^{(1)} = \overline{L}^*$. *For* $i \geq 1$, *the group* $U_L^{(i)}/U_L^{(i+1)}$ *is canoncially isomorphic to the grop* $\mathfrak{p}_L^i/\mathfrak{p}_L^{i+1}$ *which is isomorphic to the additive group of the reside field* $\overline{L}$.

Let π be a uniformizer of L.

PROPOSITION 3.1.5. *The map which assigns to* $\sigma \in G_i$ *to* $\sigma(\pi)/\pi$ *induces an isomorphism* θ_i *by passage to quotient from* G_i/G_{i+1} *onto a subgroup of* $U_L^{(i)}/U_L^{(i+1)}$.

Now we reap the harvest of properties of G_i/G_{i+1} in the following corollary:

COROLLARY 3.1.6. *(1) The group* G_0/G_1 *is cyclic, and is mapped isomorphically by* θ_0 *onto a subgroup of the group of roots of unity contained in* $\overline{L}^*$. *Its order is prime to the characteristic of the residue field* $\overline{L}$.

(2) If the characteristic of $\overline{L}$ *is zero, then* $G_1 = \{1\}$ *and the group* G_0 *is cyclic.*

(3) If the characteristic of $\overline{L}$ *is* $p \neq 0$, *the quotient* $G_i/G_{i+1}, i \geq 1$ *are abelian groups, and are direct products of cyclic groups of order* p. *The group* G_1 *is a* p*-group.*

(4) The group G_0 *is solvable. If* $\overline{K}$ *is a finite field, then* G *is also solvable.*

3.1.2. Upper numbering scheme and the Hasse-Arf theorem. It turns out that for several applications the most natural numbering of the ramification groups is not the one defined above. For our purposes we need to define what is called the *upper numbering* scheme of ramification groups. Firstly, if $u \geq -1$ is a *real* number then define $G_u = G_{\lceil u \rceil}$. Thus $\sigma \in G_u \Leftrightarrow i_G(\sigma) \geq u + 1$. Define

$$\varphi(u) = \int_0^u \frac{dt}{[G_0 : G_t]}$$

where if $-1 \leq t \leq 0$, our convention is $[G_0 : G_t] = 1$ if $-1 < t \leq 0$ and for $t = -1$, it is $[G_{-1} : G_0]^{-1}$. Explicitly, if $m \leq u \leq m + 1$, with m a positive integer, then

$$\varphi(u) = \frac{1}{|G_0|}\big(|G_1| + \cdots + |G_m| + (u - m)|G_{m+1}|\big).$$

Let ψ denote the inverse of the map φ. We now define the *upper numbering* of the ramification groups by:

$$G^v = G_{\psi(v)}$$

or equivalently

$$G^{\varphi(u)} = G_u.$$

A direct check shows that $G^{-1} = G, G^0 = G_0$, and $G^v = \{1\}$ if v is sufficiently large.

Let L/K be an infinite Galois extension, with G as its Galois group. We can define $G^v = \varprojlim \mathrm{Gal}(L'/K)^v$, L' running through the set of finite Galois subextensions of L. The G^v form a filtration of G as in the finite case. This filtration is *left continous*, i.e., $G^v = \cap_{w<v} G^w$. We say that v is a *jump* for the filtration if $G^v \neq G^{v+\epsilon}$ for all $\epsilon > 0$. A jump need not be an integer (even if L/K is finite, cf. [**Ser79**] Chapter IV.)

Now we come to the Hasse-Arf theorem, a proof of which is given in [**Ser79**] Chapter V §7.

THEOREM 3.1.7 (Hasse-Arf). *If G is an abelian group, and if v is a jump in the filtration G^v, then v is an integer.*

3.1.3. Artin Representation. We assume a nodding familiarity with character theory, a good reference is [**Isa76**]. Let L/K be a finite Galois extension, with Galois group G. Let $f = [\overline{L} : \overline{K}]$. If $\sigma \neq$ is an element of G, then we define a certain function $a_G : G \to \mathbb{Z}$ as follows:

$$a_G(\sigma) = -f i_G(\sigma), \text{ if } \sigma \neq 1$$
$$a_G(1) = f\sigma_{s\neq 1} i_G(s).$$

By definition $\sum_{\sigma\in G} a_G(\sigma) = 0$, in other words, the inner product with the trivial character $[a_G, 1_G] = 0$. Since $i_G(\psi\sigma\psi^{-1}) = i_G(\sigma)$, the function a_G is a class function (meaning that its value is insensitive to elements in the same conjugacy class.) The irreducible characters of G form an orthogonal basis for every class function thus we have

$$a_G = \sum_{\chi\in \mathrm{Irr}(G)} c_\chi \chi,$$

where $c_\chi = [\chi, a_G]$. The theorem of Artin shows that this class function is in fact a character!

THEOREM 3.1.8 ([**Art30**]). *The function a_G is a character. In particular, $[a_G, \chi]$ is a non-negative integer for every character χ of G.*

The second part of the claim of the theorem follows from the first, since every character is a linear combination of the irreducible characters with non-negative integer coefficients.

We collect some properties of the function a_G.

PROPOSITION 3.1.9. *Let G_i be the ith ramification group of G, let u_i be the character afforded by the agumentation representation of G_i, and let u_i^* be the character of G induced by u_i. Then*

$$a_G = \sum_{0\leq i} \frac{1}{[G_0 : G_t]} u_i^*.$$

Proof : Let $g_i = |G_i|$. We have $u_i^*(\sigma) = 0$ if $\sigma \notin G_i$, while $u_i^*(\sigma) = -g/g_i = -fg_0/g_i$ if $\sigma \in G_i$, $\sigma \neq 1$. For $\sigma \in G_k$ but not in G_{k+1}, the sum on the right side is $-f(k+1)$ and $a_G(\sigma)$ has the same value. For $s = 1$ by orthogonality of both sides with 1_G we get the result. □

If ϕ is a class function on G, define

$$\phi(G_i) = \frac{1}{g_i} \sum_{\sigma\in G_i} \phi(\sigma)$$

where $g_i = |G_i|$.

COROLLARY 3.1.10. *If ϕ is a class function on G, then*

$$[\phi, a_G] = \sum_{0\leq i} \frac{g_i}{g_0} (\phi(1) - \phi(G_i)).$$

Proof : This follows from the Proposition 3.1.9, by observing that $[\phi, u_i^*] = [\phi|_{G_i}, u_i^*] = \phi(1) - \phi(G_i)$. □

Finally we get:

COROLLARY 3.1.11. *If χ is the character of a representation of G in a vector space V, then*

$$[\chi, a_G] = \sum_i \frac{g_i}{g_0} \dim V/V^{G_i},$$

where V^{G_i} is the subspace of V fixed by G_i.

Proof : This follows from the previous corollary because $\chi(1) = \dim V$ and $chi(G_i) = \dim V^{G_i}$. □

REMARK 3.1.12. Now returning to our local representation $\rho_p : G_{\mathbb{Q}_l} \to GL_2(\mathbb{F}_\ell)$ we can substitute the character afforded by ρ_p as χ in the above Corollary and using Artin's theorem, we find that $n(\rho, p)$ is an integer. Thus all that is left to do is prove Artin's theorem.

The idea of the proof is to reduce the computation of $[\chi, a_G]$ for a character of G to characters of subgroups of G. This is achieved by Brauer's "Characterization of Characters" theorem. Brauer's theorem actually gives more (and this is critical) in that every character is induced from degree 1 characters, namely homomorphisms from G to a subgroup of the roots of unity of $\mathbb{C}$. This enables us to reduce to considering abelian sub-extensions and we will be able to prove the theorem in this case by using the Hasse-Arf theorem. We begin with the following lemma for whose proof we refer to [**Ser79**] (corollary to proposition 4 in VI §2.)

LEMMA 3.1.13. *Let H be a subgroup of G with K' being the corresponding subextension K'/K of L, and let $\mathfrak{d}_{K'/K}$. Suppose ψ is a character of H, and ψ^* the character induced on G, then*

$$[\psi^*, a_G] = v_K(\mathfrak{d}_{K'/K})\psi(1) + f_{K'/K}[\psi, a_G]$$

Since $\psi(1)$ is simply the dimension of the representation that yields ψ so it is an integer. So all the terms are non-negative integers except possibly $[\psi, a_G]$.

PROPOSITION 3.1.14. *Let χ be a degree 1 character on G. Let c_χ be the largest integer for which the restriction of χ to the ramification group G_{c_χ} is not the unit character (if $\chi = 1_G$ then set $c_\chi = -1$). Then*

$$[\chi, a_G] = \varphi_{L/K}(c_\chi) + 1.$$

Where $\varphi_{L/K}$ is the function defined in the previous section.
Proof : If $i \leq c_\chi$, then $\chi(G_i) = 0$ (use the fact that degree of $\chi = 1$), so that $\chi(1) - \chi(G_i) = 1$. Now if $i > c_\chi$, then $\chi(G_i) = 1$, and so $\chi(1) - \chi(G_i) = 0$. By Corollary 3.1.10 we see that

$$[\chi, a_G] = \sum_{0 \leq i \leq c_\chi} \frac{|G_i|}{|G_0|} = \varphi_{L/K}(c_\chi) + 1.$$

□

COROLLARY 3.1.15. *Let* H *be the kernel of* χ *(a degree* 1 *character), let* K' *be the subextension of* L/K *corresponding to* H. *Let* c'_χ *be the largest integer for which* $(G/H)_{c'_\chi} \neq 1$. *Then* $[\chi, a_G] = \varphi_{K'/K}(c'_\chi) + 1$, *and this is a non-negative integer.*

Proof : Herbrand's theorem ([**Ser79**] VI §3 lemma 5) shows that $c'_\chi = \varphi_{L/K'}(c_\chi)$. Now by proposition 3.1.14 we have $[\chi, a_G] = \varphi_{L/K}(c_\chi) + 1$. But the function φ is transitive, in the sense that $\varphi_{L/K} = \varphi_{K'/K} \circ \varphi_{L/K'}$. Using this we have $\varphi_{L/K}(c_\chi) = \varphi_{K'/K}(\varphi_{L/K'}(c_\chi)) = \varphi_{K'/K}(c'_\chi)$. Thus $[\chi, a_G] = \varphi_{L/K}(c_\chi) + 1$. Since χ is a degree 1 character, we have that G/H is abelian. Thus the Hasse-Arf theorem (3.1.7) shows that $\varphi_{K'/K}(c'_\chi)$ is an integer. The non-negativity is clear as $\varphi(u) \geq -1$. □

Proof :[of Theorem 3.1.8] We need to show $[\chi, a_G]$ is a non-negative integer for every character χ of G. By corollary 3.1.11 it is at least a non-negative rational number. By Brauer's theorem $\chi = \sum n_i \chi_i^*$ where χ_i^* is the induced character of some degree 1 character χ_i on a subgroup H_i of G. This reduces us to showing that $[\chi^*, a_G]$ is an integer, if χ is a degree 1 character. In this case corollary 3.1.15 says that $[\chi, a_G]$ is an integer, and lemma 3.1.13 says that $[\chi^*, a_G]$ is an integer. □

3.2. The result of Carayol and Livné

Our aim here is to show that if at all an irreducible odd representation $\rho : G_{\mathbb{Q}} \to GL_2(\overline{\mathbb{F}}_\ell)$ is modular, i.e., $f \in S_k(M, \chi)$ such that $\rho \sim \rho_f$ then $N \mid M$, where N is the level given by Serre's recipe. It turns out that this fact is an easy consequence of facts about ℓ-adic and automorphic representations (Carayol in [**Car89**] devotes a single paragraph at the end of page 787 to its proof). We will simply outline the key idea, without any proofs.

Now given the modular form f, we can construct by Deligne's mechanism a λ-adic representation of $G_{\mathbb{Q}}$ call this $\hat{\rho_f}$. Now the reduction of this λ-adic representation gives rise to our residual representation to $\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_{\ell^n})$. The following two facts are true:

(1) Under the reduction operation, the local exponents of the Artin conductor do not go up, i.e. $n(\rho, p) \leq n(\hat{\rho_f}, p)$. This is the content of Proposition 1.1 and 2.1 in [**Liv89**].
(2) The "conductor" obtained by the taking the products of primes with the local exponents of the λ-adic representation *is* the level M in which the form f resides. This is Lemma 4.1 of [**Liv89**].

Now the above two facts say that the Artin conductor of ρ is a divisor of the level M of f, which is what we wanted. The proof of fact (1) does not use anything more that the material in [**Ser79**], the proof of fact (2) requires some work by Jacquet-Langlands and Tunnell [**JLa70, Tun79, Del73, Car86**].

3.3. Removing the prime ℓ from the level

In this section, we will show that if the odd irreducible Galois representation given to us is modular, then the representation also arises from a modular form of level prime to ℓ. This result is from [**Rib94**].

THEOREM 3.3.1. *Assume $\ell \geq 3$. Suppose that $\rho : G_{\mathbb{Q}} \to GL_2(\overline{\mathbb{F}}_\ell)$ is an odd irreducible representation, that arises from a modular form on $\Gamma_1(M)$, where $M = N\ell^\alpha$, with $(\ell, N) = 1$. Then ρ arises from a modular form on $\Gamma_1(N)$.*

Proof : Let f be the eigenform that gives rise to ρ, we will assume that it is normalized (without loss of generality). In the proof ν will denote a prime dividing ℓ in $\overline{\mathbb{Q}}$. Clearly, we can assume that $\alpha \geq 1$ for otherwise there is nothing to prove.

(1) The representation ρ arises from $\Gamma_0(\ell^r) \cap \Gamma_1(\ell N)$ for some $r \geq 0$.

Let $f = \sum_{1 \leq n} a_n q^n \in S_k(\Gamma_1(M))$ and let κ be its associated Dirichlet character $\mod M$. We assume $k \geq 2$. This means that if $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(M)$, then

$$f\left(\frac{az+b}{cz+d}\right) = \kappa(d)(cz+d)^k f(z).$$

Since $M = \ell^\alpha N$, we can decompose the character κ as a product $\epsilon\eta\omega^i$, where ϵ has conductor dividing N, η has ℓ-power order and ℓ-power conductor, and ω is a character of conductor ℓ and order $\ell - 1$ which is the identity $\mod \nu$ (such a character is called a "Teichmüller" character). The character η has odd order so it can be written as ξ^{-2} where ξ is a character of ℓ-power order. The cusp form $f \otimes \xi$ which is $\sum_{1 \leq n} \xi(n) a_n q^n$ is a form in $S_k(\Gamma_0(\ell^{2h}M), \xi^2(\epsilon\eta\omega^i))$ where ℓ^h is the conductor of ξ (see [**Bum97**] Ex. 1.5.1). Since $\eta = \xi^{-2}$, $f \otimes \xi \in S_k(\Gamma_0(\ell^{2h}M), \epsilon\omega^i)$. Now assume that $r \geq 2h$, so that $f \otimes \xi \in S_k(\Gamma_0(\ell^r N), \epsilon\omega^i)$. Suppose $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(\ell^r N)$, then

$$(f \otimes \xi)\left(\frac{az+b}{cz+d}\right) = \epsilon(d)\omega^i(d)(f \otimes \xi)(z)$$

but if $\gamma \in \Gamma_0(\ell^r) \cap \Gamma_1(\ell N)$ then $\epsilon(d) = \omega^i(d) = 1$, so that

$$(f \otimes \xi)\left(\frac{az+b}{cz+d}\right) = (f \otimes \xi)(z).$$

The twisted form $f \otimes \xi$ also gives rise to the same representation. Thus we can assume that ρ arises from some form on $\Gamma_0(\ell^r) \cap \Gamma_1(\ell N)$ for some $r > 0$.

(2) ρ arises from $\Gamma_0(\ell^r) \cap \Gamma_1(N)$.

Now from **(1)** we are provided with a modular form f on $\Gamma_0(\ell^r) \cap \Gamma_1(\ell N)$ with nebentypus character $\epsilon\omega^i$, where we can assume that i is a positive integer. Consider the Eisenstein series

$$G \stackrel{\triangleright}{=} L(1-i, \omega^{-i}) + \sum_{1 \leq n} \left(\sum_{d \mid n} \omega^{-i}(d) d^{i-1} \right) q^n.$$

It is a known fact that G is of weight i nebentypus ω^{-i} on $\Gamma_0(\ell)$ (see [**Ser73**] Lemma 10). Normalizing G by setting $E = c^{-1}G$, where c is the constant coefficient, we get a form E that is in fact $\equiv 1 \mod \nu$. Thus fE viewed $\mod \nu$, is a non-zero eigenform. By a similar

analysis as in **(1)** $f|E$ is on the group $\Gamma_0(\ell^r) \cap \Gamma_1(N)$ (essentially because all the characters with conductor a power ℓ have been killed). Now a beautiful result of Deligne and Serre ([**DeS74**] Lemma 6.11) ensures that we can find an eigenform on $\Gamma_0(\ell^r) \cap \Gamma_1(N)$ whose eigenvalues are congruent to those of f.

(3) ρ arises from $\Gamma_0(\ell) \cap \Gamma_1(N)$.

Now we have an $f = \sum_{1 \leq n} a_n q^n$ an eigenform on $\Gamma_0(\ell^r) \cap \Gamma_1(N)$, with $r > 1$. Let K be a finite Galois extension of $\mathbb{Q}$ containing the a_n, and let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ be an element such that $\sigma a \equiv a^\ell \mod \nu$ for all $a \in \mathcal{O}_K$. Now $\sigma^{-1} f = \sum_{1 \leq n} \sigma^{-1} a_n q^n$ is a normalized eigenform of the same weight as f. We wish to show that f is congruent $\mod \nu$ to a cusp form of some weight on $\Gamma_0(\ell^{r-1}) \cap \Gamma_1(N)$. Let $g = (\sigma^{-1} f)^\ell | U$, where $U = T_\ell$ the ℓth Hecke operator. It turns out that g is a form on $\Gamma_0(\ell^{r-1}) \cap \Gamma_1(N)$ ([**Li75**] Lemma 1), and by our choice the Fourier expansion of g is congruent $\mod \nu$ to $\sum (\sigma^{-1} a_n)^\ell q^n$ which is congruent to the Fourier expansion of f.

(4) ρ arises from $\Gamma_1(N)$.

Let W be the operator given by the matrix $\begin{pmatrix} \ell x & y \\ N\ell z & \ell \end{pmatrix}$ where x, y, z are integers such that $\ell x - N\ell z = 1$. Now if F is a form on $\Gamma_0(\ell) \cap \Gamma_1(N)$ of weight w and character ϵ, then [**Li75**] Lemma 3, implies that the form

$$\mathrm{Tr}\ (F) \stackrel{\triangleright}{=} F + \epsilon^{-1}(\ell) \ell^{1 - \frac{w}{2}} F|W|U$$

is a form of weight w on $\Gamma_1(N)$. Also, if G is a form of weight w and character ϵ on $\Gamma_1(N)$ then $G|W = \ell^{w/2} \epsilon(\ell) G|V$ ([**AtL78**] Proposition 1.5). If $\ell = 3$, let E be the normalized Eisenstein series E_4 of weight four, and if $\ell \neq 3$, let E be the normalized Eisenstein series of weight $\ell - 1$, so that $E \equiv 1 \mod \ell$. Let a denote the weight of E, consider the form

$$g \stackrel{\triangleright}{=} E - \ell^{a/2} E|W = E - \ell^a E|V.$$

The $g \equiv 1 \mod \ell$ and furthermore $g|W$ is divisible by ℓ. Let f be an eigenform giving rise to ρ on $\Gamma_0(\ell) \cap \Gamma_1(N)$. Then for large enough i one can show that $\mathrm{Tr}\ (f g^i) \equiv f \mod \ell$.

□

3.4. General level lowering principles

Many methods of level lowering proceed by first reducing the problem to the weight 2 case. The first step replaces the representation ρ by a suitable twise by a $\mod \ell$ cyclotomic character χ so that it arises from a newform of weight k, where $2 \leq k \leq \ell + 1$ (see [**Edi92**]). Next we use a theorem of Ribet ([**Rib94**] Theorem 2.2) that says that $\mod \ell$, the eigenforms of level N whose weight lies in the range $2 < k \leq \ell + 1$ correspond to eigenforms of weight 2 and level ℓN. So at the cost of putting back one power of ℓ into the level we can reduce the weight to 2.

Once we are in weight 2, we use a theorem of Carayol ([**Car89**] Théorème 2) to reduce to the following problem (called the Key case by Ribet):

Key case: Let $\rho : G_{\mathbb{Q}} \to GL_2(\overline{\mathbb{F}}_\ell)$ be a Galois representation that arises from a weight 2 newform f of level pM, with $p \not| \ell M$, and character $\epsilon : (\mathbb{Z}/pM\mathbb{Z}^*) \to \mathbb{C}^*$. Assume that ρ is unramified at p, and that ϵ factors through the natural map $(\mathbb{Z}/pM\mathbb{Z}) \to (\mathbb{Z}/M\mathbb{Z})^*$. Then show that ρ arises from a form of level M.

Another advantage of weight 2 is that we have the clean geometric interpretation of the modular representation as explained in Chapter 2. In this case there are basically four different approaches to level lowering as explained in §3.5 of [**RiS01**], we refer the reader to that article for the discussion of these principles.

CHAPTER 4

The Weight

Let $\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_\ell)$ be an odd irreducible Galois representation. Our main task in this chapter is to give Serre's recipe for $k(\rho)$ the weight of the modular form that conjecturally gives rise to ρ ([**Ser87**] §2). After that, we will discuss a result of Edixhoven that says that if ρ arises from a modular form of weight k level N and nebentypus ϵ, then it also arises from a weight $k(\rho)$ modular form of same level and nebentypus.

4.1. The prescription for the weight

Assume the notation of Chapter 1. The definition of the weight $k(\rho)$ depends only on the induced local representation at ℓ:

$$\rho_\ell : G_\ell \to GL(V) \cong GL_2(\overline{\mathbb{F}}_\ell),$$

where $G_\ell = \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$. Let I denote the inertia subgroup of G_ℓ, and I_w denote the largest pro-ℓ subgroup of I (this is called the *wild inertia* subgroup). The quotient $I_t = I/I_w$ is called the *tame inertia* subgroup. This quotient is isomorphic to $\varprojlim \mathbb{F}_{\ell^n}^*$ where the limit is taking with respect to the norm maps ([**Ser72**] Propositions 1 & 2). A character of I_t is said to be of *level* n, if it factors through $\mathbb{F}_{\ell^n}^*$ but not through $\mathbb{F}_{\ell^m}^*$ for any proper divisor of n. Let ρ^{ss} denote the semi-simplification of ρ_ℓ, it is either ρ if the action is irreducible or a direct sum of two characters. Serre shows in [**Ser72**] (Proposition 4) that in either case $\rho^{ss}(I_w)$ acts trivially (ρ_ℓ is a tame representation at ℓ). Thus we can think of I_t acting on V^{ss} (the semi-simplification of V). This action of I_t is diagonalizable; it is given by two characters:

$$\varphi, \varphi' : I_t \to \overline{\mathbb{F}}_\ell^*.$$

Proposition 4.1.1 ([**Ser72**] Prop. 1). *The characters φ and φ' giving the action of I_t on V^{ss} are either level 1 or 2. If they are level 2, then they are conjugate in the sense that $\varphi' = \varphi^\ell$ and $\varphi = \varphi'^\ell$.*

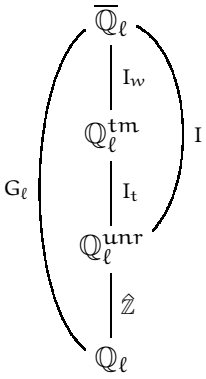
Proof : Let $\sigma \in G_\ell$, whose image in the group $G_\ell/I \cong \mathrm{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}_\ell)$ gives the Frobenius automorphism $x \mapsto x^\ell$. One can check that this condition implies that $\sigma u \sigma^{-1} \equiv u^\ell \mod I_w$ for $u \in I$. So that conjugation by σ operates on I_t by $u \mapsto u^\ell$. This results in the set $\{\varphi, \varphi'\}$ being stable under the operation of raising to the ℓ-th power. Thus we have two cases:

(1) $\varphi^\ell = \varphi, \varphi'^\ell = \varphi'$, so that both the characters are level 1;
(2) $\varphi^\ell = \varphi', \varphi'^\ell = \varphi$ and $\varphi \neq \varphi'$, so that they are characters of level 2.

This proves the proposition. □

We will deal with each case above separately. Before that we need to discuss fundamental characters (see also [**Bos03**] §3.2).

4.1.1. Fundamental characters. For a nice discussion of this see [**Ser72**] §1.3 – §1.7 (and [**RiS01**] §2.1.2). Let $\mathbb{Q}_\ell^{unr}$ be the maximal unramified extension of $\mathbb{Q}_\ell$, and $\mathbb{Q}_\ell^{tm}$ the maximal tamely ramified extension of $\mathbb{Q}_\ell^{unr}$. We have the following diagram of field inclusions and relative Galois groups:



The extension $\mathbb{Q}_\ell^{tm}$ is generated by the extensions $\mathbb{Q}_\ell^{unr}(\ell^{\frac{1}{n}})$ for all n not divisible by ℓ. For n with $\gcd(n,\ell)=1$, the n-th roots of unity μ_n are contained in $\mathbb{Q}_\ell^{unr}$. By Kummer theory, we get for each n, a canonical isomorphism:

$$\mathrm{Gal}(\mathbb{Q}_\ell^{unr}(\ell^{\frac{1}{n}})/\mathbb{Q}_\ell^{unr}) \xrightarrow{\sim} \mu_n,$$

by $\sigma \mapsto \frac{\sigma(\ell^{\frac{1}{n}})}{\ell^{\frac{1}{n}}}$. Each isomorphism gives a map from $I \to \mu_n$ that factor through I_t. Composing any of the maps $I_t \to \mu_n$ with reduction $\mod$ the maximal ideal of $\overline{\mathbb{Z}}_\ell$ gives a $\mod \ell$ chracter $I_t \to \overline{\mathbb{F}}_\ell^*$. The map $I_t \to \mu_\ell$ defines a character $\epsilon : I \to \mathbb{F}_{\ell^k}^*$. There are k embeddings of $\mathbb{F}_{\ell^k} \to \overline{\mathbb{F}}_\ell$, composing gives us k different characters $I_t \to \overline{\mathbb{F}}_\ell$. These are the k fundamental characters of level k. In particular, there are 2 fundamental characters of level 2, and these are conjugate under the ℓ-th power map.

4.1.2. Definition of $k(\rho)$ when φ and φ' are level 2. Suppose that φ and φ' are of level 2. In this case the representation is irreducible. For if there was a 1-dimensional subspace stable under the action, then the action of I_t on this subspace is given by a character that will extend to G_ℓ, which is of level 1. Let ψ and $\psi' = \psi^\ell$ be the two fundamental characters of level 2 of I_t (cf. §4.1.1). Thus we can write φ in the following manner:

$$\varphi = \psi^{a+pb} = \psi^a \psi'^b, \text{ with } 0 \le a, b \le p-1.$$

We have $a \neq b$ since otherwise $\varphi = (\psi\psi')^a = \chi^a$, where $\chi|I$ is a cyclotomic character contradicting the assumption that ψ is of level 2. Since φ' is a conjugate of φ, we have $\varphi' = \psi^b \psi'^a$. Thus by reordering φ and φ', we can assume that $0 \le a < b \le p-1$. In this case we define

$$k(\rho) = 1 + \ell a + b. \tag{4.1.6}$$

4.1.3. Definition of $k(\rho)$ when φ and φ' are level 1, and I_w operates trivially. In this case, we can assume that the action of I on V is semisimple, and is given by two characters φ, φ' that are powers χ^a and χ^b of the cyclotomic character χ, i.e.,

$$\rho_\ell|_I \sim \begin{pmatrix} \chi^a & 0 \\ 0 & \chi^b \end{pmatrix}.$$

The integers a and b are determined $\mod \ell - 1$. Normalizing so that $0 \leq a, b \leq p-2$. We can also assume $0 \leq a \leq b \leq p-2$ by permuting φ and φ'. The weight in this case is defined by:

$$k = \begin{cases} 1 + \ell a + b & \text{if } (a,b) \neq (0,0) \\ \ell & \text{if } (a,b) = (0,0). \end{cases} \tag{4.1.7}$$

4.1.4. Definition of $k(\rho)$ when φ and φ' are level 1, and I_w does not operate trivially. In this case V^{I_w} forms a subspace of V that is stable under the G_ℓ action. The action of G_ℓ on V/D is given by a character θ_1 and on D by another character θ_2 of G_ℓ, so that the action on V is given by:

$$\rho_\ell \sim \begin{pmatrix} \theta_2 & * \\ 0 & \theta_1 \end{pmatrix}.$$

We can write θ_1, θ_2 uniquely in the form: $\theta_1 = \chi^\alpha \epsilon_1$ and $theta_2 = \chi^\beta \epsilon_2$, where ϵ_i is an unramified character on G_p and $\alpha, \beta \in \mathbb{Z}/(\ell-1)\mathbb{Z}$. Restriction to the inertia subgroup is thus of the form:

$$\rho_\ell|_I \sim \begin{pmatrix} \chi^\beta & * \\ 0 & \chi^\alpha \end{pmatrix}.$$

Note that $\alpha \neq \beta$, for otherwise the action on I_w will be trivial contradicting our assumption. Normalizing so that $0 \leq \alpha \leq \ell - 2$ and $1 \leq \beta \leq \ell - 1$ we set $a = \inf(\alpha, \beta)$ and $b = \sup(\alpha, \beta)$. Now for defining $k(\rho)$ we distinguish between two cases:

(1) *The case* $\beta \neq \alpha + 1$*:* In this case as in 4.1.6 we set

$$k(\rho) = 1 + \ell a + b. \tag{4.1.8}$$

(2) *The case* $\beta = \alpha + 1$*:* In this case we have to distinguish between the type of the wild ramification. We shall distinguish between two cases that we call *slightly ramified* and *highly ramified* (Serre calls them *peu ramifié* and *trés ramifieé*).

Let $K_0 = \mathbb{Q}_\ell^{unr}$. The group $\rho_\ell(I)$ is the Galois group of a certain totally ramified extension K of K_0, and the wild inertia group $\rho_\ell(I_w)$ is the Galois group of K/K_t, where K_t is the maximal tamely ramified extension of K_0 containing K. Since $\beta = \alpha + 1$, one can show that $\mathrm{Gal}(K_t/K_0) \cong (\mathbb{Z}/\ell\mathbb{Z})^*$, thus $K_t = K_0(\zeta)$, where ζ is a primitive ℓ-th root of unity. On the other hand $\mathrm{Gal}(K/K_t) = \rho_\ell(I_w)$ is an elementary abelian group of type $(\ell, \cdots, \ell)$, which can be represented by matrices $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$. Furthermore, one can show that the action by congugation of $\mathrm{Gal}(K_t/K_0) = (\mathbb{Z}/p\mathbb{Z})^*$ on $\mathrm{Gal}(K/K_t)$ is the obvious action. By Kummer theory, this implies that K can be written as $K = K_t(x_1^{\frac{1}{\ell}}, \cdots, x_m^{\frac{1}{\ell}})$, where $\ell^m = [K : K_t]$. Let

v_ℓ the normalized valuation of K_0 that gives $v_\ell(\ell) = 1$, we say that K is *slightly ramified* if

$$v_\ell(x_i) \equiv 0 \mod \ell, \text{ for } 1 \leq i \leq m.$$

So that the x_i can be chosen to be units of K_0. If the above is not true, then we say that K and ρ_ℓ are *highly ramified*.

Now we can define $k(\rho)$ in these cases:

(a) *The case* $\beta = \alpha + 1$, *slightly ramified*. The prescription is the same as for $\beta \neq \alpha + 1$

$$k = 1 + \ell a + b. \tag{4.1.9}$$

(b) *The case* $\beta = \alpha + 1$, *highly ramified*. Here we define

$$k = 1 + \ell a + b + (\ell - 1). \tag{4.1.10}$$

Note that we have assumed $\ell \neq 2$.

Finally, we have given a full description of Serre's prescription of the weight of the representation $k(\rho)$.

REMARK 4.1.2. Note that in all the cases we have defined, the value of $k(\rho)$ lies in the interval $[2 \cdots \ell^2 - 1]$.

4.2. Edixhoven's result

In [**Edi92**] Edixhoven proved the following theorem:

THEOREM 4.2.1. *Let* $\rho : G_{\mathbb{Q}} \to GL_2(\overline{\mathbb{F}}_\ell)$ *be a continous, odd irreducible representation. Suppose there is a cusp form* g *of level* N, *weight* k *and nebentypus* ϵ *with* $\ell \nmid N$ *which is an eigenform, such that* ρ *is isomorphic to* ρ_g. *Then there exists a cuspidal eigenform* f *of weight* $k(\rho)$, *level* N *and nebentypus* ϵ *that gives rise to* ρ. *Here* $k(\rho)$ *is the weight of* ρ *as defined in the previous section.*

The proof makes use of the following result of Fontaine (which was proved in two letters to Serre)

THEOREM 4.2.2 (Fontaine). *Let* f *be a cusp form of level* N, *weight* k *and nebentypus* ϵ *that is an eigenform with eigenvalue* a_p *for the* p*-th Hecke operator. Assume that* $2 \leq k \leq \ell + 1$, *and* $a_\ell = 0$. *Then the local representation at* ℓ *afforded by* f *(in the sense of Chapter 2)* $\rho_{f,\ell}$ *is irreducible. Furthermore,*

$$\rho_f|_I \sim \begin{pmatrix} \psi^{k-1} & 0 \\ 0 & \psi'^{k-1} \end{pmatrix}$$

where ψ, ψ' *are the two fundamental characters of level* 2.

We will also need the θ-operator, that operates on q-expansions by $\theta(\sum a_n q^n) = \sum n a_n q^n$. This operator has the property that if f is an eigenform of weight k, then there is a $\mod \ell$ eigenform θf of weight $k + \ell + 1$ of the same level N, whose q-expansion is $\theta(\sum a_n q^n)$.

We outline the construction of f with the properties claimed in Theorem 4.2.1 in a special case. Suppose $\rho|_I \sim \begin{pmatrix} \varphi & 0 \\ 0 & \varphi' \end{pmatrix}$, where φ and φ' are level 2 characters as in §4.1.2. Let ψ, ψ' be the two

fundamental characters of level 2, and assume a, b are such that $\varphi = \psi^a \psi'^b$ with $0 \leq a < b \leq \ell - 1$. Now as mentioned in §3.4, we can find a twist of the representation ρ by a cyclotomic character $\rho \otimes \chi^{-\alpha}$ (say) that is associated to a modular form of weight $2 \leq k_1 \leq \ell + 1$. Call the modular form giving rise to $\rho \otimes \chi$, f_1. The eigenform f_1 has p-th eigenvalue $p^{-\alpha} a_p$ for $p \neq \ell$. Furthermore, one can show that $a_\ell(f_1) = 0$ and that the weight of f_1, is $k_1 = 1 + b - a$. Define the modular form f by $f \stackrel{\triangleright}{=} \theta^a f$, where θ is the operator defined above. Then by the property alluded to above, we have $\text{weight}(f) = 1 + b - a + (\ell + 1)a = 1 + \ell a + b$. A detailed check then shows that f gives rise to ρ, so that it is the desired form. We refer to [**Edi92**] for all the details and also a proof of Theorem 4.2.2.

CHAPTER 5

The Evidence for the conjecture

In this chapter we give a short overview of the evidence that has been accumulated for Serre's conjecture. As might be clear from the previous chapters, most of the results that have been obtained have been in the direction of proving that the strong and weak conjectures of Serre are equivalent. We know very little about the conjecture itself, and it has been proved only when the image of the Galois representation is very small. In §1.2 we showed how Galois representations arising from elliptic curves provides some evidence for Serre's conjecture. This gives us at least an infinite number of examples where the conjecture is true. In §5.1 we will examine a consequence of Serre's conjecture for which there is some supporting evidence. In §5.2 we examine the case when we have a Galois representation to $\mathrm{GL}_2(\mathbb{F}_3)$, here Serre's conjecture can be proved. This case also played a pivotal role in the proof of Fermat's Last theorem.

5.1. A consequence of Serre's conjecture

Suppose we have an odd irreducible continuous representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\ell)$ that is unramified outside ℓ. Then Serre's recipe gives 1 for the level, and the nebentypus character as a consequence must be trivial. Now techniques we have seen and used in the previous chapters tell us, that if we look at twists by a cyclotomic character, we will get a representation that has weight $\leq \ell + 1$ (see §4.2), but the same level and nebentypus. Now suppose $\ell < 11$, in this case $\dim S_k(\Gamma_0(1)) = 0$. Thus there are no non-zero Galois representations of weight $\ell < 11$ that are unramified outside ℓ. That this is The case for $\ell = 2$ was proved by Tate in a letter to Serre. The proof idea is to get an upper bound for the number field through which this representation factors and then use Minkowski's bound to get a bound on the degree. Then an explicit calculation then shows all of these fields to be solvable, which is then handled by Class field theory [**Tat94**]. The case $\ell = 3$ was treated by Serre using similar methods ([**Ser75**] §3, see also the notes in his Œuvres for article 104.) The case $\ell = 5$ has been proved under the Generalized Riemann Hypothesis by Brueggeman [**Bru99**].

5.2. The case of $\mathrm{GL}_2(\mathbb{F}_3)$

In §5.3 of [**Ser87**], Serre proves the conjecture when the image of the representation is in $\mathrm{GL}_2(\mathbb{F}_3)$. In this section we will outline the proof of this theorem. More precisely,

THEOREM 5.2.1. *Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_3)$ is an odd irreducible representation, then there is a cuspidal eigenform*

$$f = \sum_{1 \leq n} a_n q^n$$

of weight 2, and a prime λ of $\overline{\mathbb{Q}}$ lying above 3 such that

$$a_q \equiv \mathrm{Tr}\ (\rho(\mathrm{Frob}_q)) \mod \lambda$$

for all but finitely many primes q.

The critical point is the use of the following theorem due to Langlands and Tunnell.

THEOREM 5.2.2 ([**Lan80, Tun81**]). *Suppose $\sigma : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$ is a continuous, odd, irreducible representation whose image in $\mathrm{PGL}_2(\mathbb{C})$ is a solvable group. Then there is a normalized cuspidal eigenform $g = \sum_{1\leq n} b_n q^n$ of weight 1 and level N and nebentypus ψ, such that $b_p = \mathrm{Tr}\ (\sigma(\mathrm{Frob}_p))$ for all but finitely many primes p.*

The work of Langlands and Tunnell produces an automorphic representation not the modular form, we refer to [**Gel97**] §4.2 for the steps needed to construct the form $g(z)$ from the automorphic representation.

Proof : (of 5.2.1). The idea is to lift ρ to a representation to $\mathrm{GL}_2(\mathbb{C})$, then apply Theorem 5.2.2 to get a weight 1 eigenform. Then use the techniques used in [**DeS74**] to get a weight 2 eigenform that gives rise to an isomorphic representation. The lifting can be explicitly achieved by giving a specific injective homomorphism

$$\Psi : \mathrm{GL}_2(\mathbb{F}_3) \to \mathrm{GL}_2(\mathbb{Z}(\sqrt{-2}))$$

by

$$\Psi\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$$

and

$$\Psi\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ -\sqrt{-2} & -1+\sqrt{-2} \end{pmatrix}.$$

Since the matrices $\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$ generates $\mathrm{GL}_2(\mathbb{F}_3)$, this defines the map. It is easy to verify that this gives rise to a homomorphism that is the identity $\mod (1+\sqrt{-2})$. In particular, $\mathrm{Tr}\ (\Psi(g)) \equiv \mathrm{Tr}\ (g) \mod (1+\sqrt{-2})$. Further, the "lifted" representation satisfies all the hypotheses of Theorem 5.2.2. Thus we get a weight 1 cuspidal eigenform g with the properties claimed by Theorem 5.2.2. Now pick an eisenstein series E of weight 1 such that $E \equiv 1 \mod 3$. Now Eg has weight 2, some level and character that gives rise to ρ (but is not an eigenform!). For concreteness take

$$E = 1 + 6\sum_{1\leq n}\left(\sum_{d|n}\chi(d)\right)q^n$$

where

$$\chi(d) = \begin{cases} 0, & \text{if } d \equiv 0 \mod 3 \\ 1, & \text{if } d \equiv 1 \mod 3 \\ -1, & \text{if } d \equiv -1 \mod 3. \end{cases}$$

Though Eg is an eigenform mod 3 it by itself is not one, but this is no problem (we have encountered exactly this situation in §3.3). We use the lemma of Deligne-Serre ([**DeS74**] Lemma 6.11) to conclude that there exists an *eigenform* of weight 2 that is congruent modulo some prime lying over 3 to Eg. This finishes the proof. □

Representations with image in $\mathrm{GL}_2(\mathbb{F}_4)$ and $\mathrm{GL}_2(\mathbb{F}_5)$ have been handled under some restrictions by the work of Sheperd-Barron and Taylor [**ShT97**].

Bibliography

[Art30] Artin, Emil; *Zur Theorie der* L*-Reihen mit allgemeinen Gruppencharakteren*, Hamb. Abh. **8**, 292-306, 1930.

[AtL78] Atkin, A.; Li, W.; *Twists of newforms and pseudo-eigenvalues of* W*-operators*, Invent. Math., **48**, 221-243, 1978.

[Bos03] Boston, Nigel; *The proof of Fermat's Last Theorem*, under preparation, 2003.

[BCDF00] Breuil, C.; Conrad, B.; Diamond, F.; Taylor, R.; *On the modularity of elliptic curves over* $\mathbb{Q}$*, or Wild* 3*-adic exercises*, preprint 2000.

[Bru99] Brueggeman, Sharon; *The non-existence of certain Galois extensions unramified outside* 5, J. of Number Theory., **75**, 47-52, 1999.

[Bum97] Bump, Daniel; *Automorphic Forms and Representations*, Cambridge Advanced Studies in Math., **55**, Cambridge University Press, 1997.

[Car86] Carayol, Henri; *Sur les représentations* ℓ*-adiques associées aux formes modulaires de Hilbert*, Ann. Sci. École Norm. Sup., (4^{eb}) série **19**, 409-468.

[Car89] Carayol, Henri; *Sur les repreésentations Galoisiennes modulo* ℓ *attachées aux formes modulaires*, Duke Math. J., **59**, No. 3, 785-801, 1989.

[Con99] Conrad, Brian; *Modular forms, Cohomology and the Ramanujan Conjecture*, under preparation.

[Del69] Deligne, Pierre; *Formes modulaires et représentations* ℓ*-adiques*, Sém. Bourbaki no. 355, 1968/69, Springer-Verlag, Lecture Notes in Mathematics, Vol. 179, 139-172, 1971.

[Del73] Deligne, Pierre; *Formes modulaires et représentations* ℓ*-adiques*, Springer Lecture Notes in Mathematics, Vol. 349, 1973.

[DeS74] Deligne, Pierre; Serre, Jean-Pierre; *Formes modulaires de poids* 1, Ann. Sci. École Norm. Sup., (4^{eb}), série **7**, 507-530, 1975.

[Edi92] Edixhoven, Bas; *The weight in Serre's conjectures on modular forms*, Invent. Math., **109**, 563-594, 1992.

[Gel97] Gelbart, Stephen; *Three lectures on the Modularity of* $\overline{\rho}_{E,3}$ *and the Langlands Reciprocity Conjecture*, in Modular Forms and Fermat's Last Theorem, eds. Gary Cornell, Joseph Silverman, Glenn Stevens, Springer-Verlag, 1997.

[GrH78] Griffiths, Phillip; Harris, Joseph; *Principles of Algebraic Geometry*, Wiley Classics Library, 1994 reprint of 1978 original, John Wiley & Sons, 1978.

[Gro90] Gross, Benedict, H.; *A Tameness criterion for Galois representations associated to modular forms (*mod p*)*, Duke Math. J. **61**, no. 2, 445 - 517, 1990.

[Iha67] Ihara, Yasutaka; *Hecke polynomials as congruence zêta functions in elliptic modular case*, Ann. of Math. (2), **85**, 267-295, 1967.

[Isa76] Isaacs, Martin; *Character theory of finite groups*, Academic Press, 1976.

[KaM85] Katz, Nicholas; Mazur, Barry; *Arithmetic Moduli of Elliptic Curves*, Annals of Mathematics Studies, Vol. 108, Princeton University Press, 1985.

[KSh65] Kuga, Michio; Shimura, Goro; *On the Zêta function of a fibre variety whose fibres are abelian varieties*, Ann. of Math (2), **82**, 478-539, 1965.

[JLa70] Jacquet, Hérve; Langlands, Robert, P.; *Automorphic Forms for* GL(2), Springer Lecture Notes in Math. vol. **114**, Springer-Verlag, 1970.

[Lan80] Langlands, Robert; *Base Change for* GL(2), Annals of Math. Studies, Vol. **96**, Princeton University Press, 1980.

[Li75] Li, W.; *Newforms and functional equations*, Math. Ann. **212**, 285-315, 1975.

[Liv89] Livné, Ron; *On the conductors of mod* ℓ *Galois representations coming from modular forms*, J. of Number Theory, **31**, 133-141, 1989.

[Mum70] Mumford, David; *Abelian Varieties*, Tata Institute of Fundamental Research Studies in Mathematics, No. 5, 1970.

[Rib90] Ribet, Kenneth; *On modular representation of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, Invent. Math., **100**, no. 2, 431-476, 1990.

[Rib94] Ribet, Kenneth; *Report on mod* ℓ *representations of* $\mathrm{Gal}\overline{\mathbb{Q}}/\mathbb{Q}$, Proc. Symp. in Pure Math., Vol. **55**, Part 2, 1994.

[RiS01] Ribet, Kenneth, A.; Stein, William; *Lectures on Serre's conjectures*, with appendices by Brian Conrad and Kevin Buzzard, in Arithmetic Algebraic Geometry ed. Brian Conrad, Karl Rubin, IAS Park City Mathematics Series, AMS. 2001.

[ShT97] Shepherd-Barron, N., I.; Taylor, Richard; *Mod* 2 *and mod* 5 *icosahedral representations*, J. Amer. Math. Soc., **10**, no. 2, 283-298, 1997.

[Ser67] Serre, Jean-Pierre; *Une interprétation des congruences relatives á la fonction* τ *de Ramanujan*, Sém. Delange-Pisot-Poitou, no. 14, 1967/68.

[Ser72] Serre, Jean-Pierre; *Propriétés galoisienned des points d'ordre fini des courbes elliptiques*, Invent. Math., **15**, 259-331, 1972.

[Ser73] Serre, Jean-Pierre; *Formes modulaires et fonctions zêta* p*-adiques*, Springer Lecture Notes in Mathematics, vol. **350**, 191-268, 1973.

[Ser75] Serre, Jean-Pierre; *Valeurs propres des opérateurs de Hecke modulo* l, Journées arith. Bordeaux, 1974, Astérisque, **24-25**, 109-117, 1975.

[Ser78] Serre, Jean-Pierre; *Représentations linéaires des groupes finis*, 3rd edition, Hermann, Paris, 1978.

[Ser79] Serre, Jean-Pierre; *Local Fields*, GTM Vol. 67, Springer-Verlag, 1979.

[Ser87] Serre, Jean-Pierre; *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}\overline{\mathbb{Q}}/\mathbb{Q}$, Duke Math. J., **54**, 179-230, (1987).

[SeT68] Serre, Jean-Pierre; Tate, John; *Good reduction of Abelian Varieties*, Ann. of Math. (2), **88**, Issue. 3, 492-517, 1968.

[Tat94] Tate, John; *On the non-existence of certain Galois representations of* $\mathbb{Q}$ *unramified outside* 2, Contemp. Math., **174**, A.M.S., 153-156, 1994.

[TWi95] Taylor, Richard; Wiles, Andrew; *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math., (2), **141**, no. 3, 553-572, 1995.

[Tun79] Tunnell, Jerry; *Report on the local Langlands' conjecture for* $\mathrm{GL}(2)$, in Proc. Symp. Pure Math., Vol. **33**, Part 2, 135-138, 1979.

[Tun81] Tunnell, Jerry; *Artin's conjecture for representations of octahedral type*, Bull. AMS. (N.S.), 173-175, 1981.

[Wil95] Wiles, Andrew; *Modular elliptic curves and Fermat's last theorem*, Ann. of Math., (2), **141**, no. 3, 443-551, 1995.