Galois representations attached to type $(1, \chi)$ modular forms

Thesis advisor: Prof. Adrian Iovita

Master thesis by:
Andrea Ferraguti

Facoltà di Scienze MM.FF.NN.
Corso di Laurea in Matematica

Concordia University
Department of Mathematics & Statistics
Faculty of Arts and Science

Academic year 2010/2011

Contents

Introduction

This thesis is intended to explain a result found by P.Deligne and J.-P.Serre on Galois representation attached to some particular eigenforms of weight 1. Let $M_1(N,\chi)$ be the space of modular forms of weight 1 and level N, where χ is an odd Dirichlet character modulo N and let $S_1(N,\chi)$ be the subspace of cuspforms. If $f \in S_1(N,\chi)$ is a normalized eigenform, then its associated completed L-function $\Lambda(s,f)$ satisfies the functional equation

$$\Lambda(1-s,f) = c\Lambda(s,\overline{f})$$

for some constant $c \in \mathbb{C}$. On the other hand, if ρ is an odd, 2-dimensional irreducible complex Galois representations, then its completed L-function $\Lambda(s,\rho)$ satisfies an analogous functional equation

$$\Lambda(1-s,\rho) = W(\rho)\Lambda(s,\rho^*)$$

where $W(\rho) \in \mathbb{C}$ is a constant and ρ^* is the contragradient representation. This suggests that there could exist a correspondence between these two classes of objects, and this is exactly what has been proven by Deligne and Serre. After reviewing and explaining the paper where the main theorem about this correspondence is proved, we illustrate some examples found by J.-P.Serre on Galois representations with odd conductor and their corresponding eigenforms.

In the first chapter we review the theory of classical modular forms and Hecke operators, focusing in particular on the structure of the χ-eigenspaces $M_k(N,\chi)$ of modular forms of weight k, level N and Dirichlet character χ modulo N. Those χ-eigenspaces are invariant under the action of the T_p Hecke operators, for primes $p \nmid N$ and therefore they have a basis of normalized eigenforms.

The second chapter is completely dedicated to the study of Galois representations. In particular, we show that continuity implies that complex representations have finite image and therefore they must factor through the Galois group of some finite Galois extension $L/\mathbb{Q}$. So every complex representation induces a representation of a finite Galois group $\mathrm{Gal}(L/\mathbb{Q})$. Thus we can apply Serre's theory of conductor to those representations, and it is straightforward to define the Artin conductor of a Galois representation as a measure of its ramification. When we construct a Galois representation of this kind starting from a modular form, the Artin conductor is exactly the level of the modular form we are starting with.

In the third chapter we finally state and prove the main theorem:

Theorem 0.1. Let $N \in \mathbb{N}$, $\chi \in \mathbb{Z}/N\mathbb{Z}$ an odd Dirichlet character and let $0 \neq f = \sum_{n=0}^{+\infty} a_n q^n \in M_1(N,\chi)$ be a normalized eigenform for the Hecke operators T_p such that $p \nmid N$. Then there exists a 2-dimensional complex Galois representation

$$\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$$

that is unramified at all primes that do not divide N and such that

$$\mathrm{Tr}(\mathrm{Frob}_p) = a_p \quad \text{and} \quad \det(\mathrm{Frob}_p) = \chi(p)$$

for all primes $p \nmid N$.
Such a representation is irreducible if and only if f is a cusp form.

Note that the proof of this theorem strongly relies on the similar result found by Deligne for eigenforms of weight ≥ 2, constructed passing through the étale cohomology of the appropriate modular curve. However, the representations attached to those modular forms are l-adic and in general they do not have finite image: this is a phenomenon unique to weight 1 forms. Using a former result of Weil and Langlands, the Deligne-Serre theorem gives a bijection[1] between the set of normalized weight 1 cuspidal newforms of level N and Dirichlet character χ and the isomorphism classes of complex, irreducible 2-dimensional odd Galois representations with conductor N and determinant χ.
The fourth chapter is dedicated to show how one can compute the dimension of the space $S_1^+(N,\chi)$ by counting the number of isomorphism classes of 2-dimensional, odd, irreducible complex Galois representations with conductor N and determinant χ. This method passes through a characterization of complex Galois representations via their image in $\mathrm{PGL}_2(\mathbb{C})$. Finite subgroups of $\mathrm{PGL}_2(\mathbb{C})$ are indeed of a very special kind: they can be just cyclic, dihedral or isomorphic to S_4, A_4 or A_5. First we show that given a continuous projective representation $\overline{\rho}\colon G_{\mathbb{Q}} \to \mathrm{PGL}_n(\mathbb{C})$, one can always find a continuous lifting to $\mathrm{GL}_2(\mathbb{C})$, essentially because of the triviality of $H^2(G_{\mathbb{Q}}, \mathbb{C}^*)$. Then we give a formula for the dimension of $S_1^+(p,\chi)$ for p prime and χ the Legendre symbol modulo p in function of the number of nonisomorphic Galois representations with image isomorphic to D_{2n}, S_4 or A_5.

[1]Now that the Artin conjecture has been established for all odd 2-dimensional representations.

Chapter 1

Modular forms and Hecke operators

1.1 Modular forms and cusp forms

In this section we'll describe, following [DJ05], the basic theory of (classical) modular forms.
The *modular group* is the group $\mathrm{SL}_2(\mathbb{Z})$, namely

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z},\ ad - bc = 1 \right\}$$

For brevity, from now on we'll denote the modular group $\mathrm{SL}_2(\mathbb{Z})$ with Γ. One can show that the modular group is generated by the matrices

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

The *upper half plane* is

$$\mathcal{H} = \{\tau \in \mathbb{C} \colon \Im(\tau) > 0\}$$

where $\Im(\tau)$ denotes the imaginary part of τ.
The starting point of the theory of modular forms is the observation that the modular group acts on $\mathcal{H}$ via the map

$$\Gamma \times \mathcal{H} \to \mathcal{H}$$

$$(\gamma, \tau) \mapsto \gamma(\tau) = \frac{a\tau + b}{c\tau + d}$$

where $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$.
This follows from the fact that $\forall\, \tau \in \mathcal{H}$ we have

$$\Im(\gamma(\tau)) = \frac{\Im(\tau)}{|c\tau + d|^2}$$

It's easy to check that $\gamma(\gamma'(\tau)) = (\gamma\gamma')(\tau)\ \forall\, \gamma, \gamma' \in \Gamma$.

Remark 1.1. One could notice that if $\gamma \in \Gamma$, then the action of $-\gamma$ on $\mathcal{H}$ is the same as the action of γ. So we can pass to the quotient and say that we have an action

$$\Gamma/\{\pm I\} \times \mathcal{H} \to \mathcal{H}$$

Roughly speaking, we want to describe a modular form as a weight k Γ-invariant complex holomorphic function. But this would not be the most natural possible construction. Indeed, one can think of elements of Γ as automorphisms of the Riemann sphere $\widehat{\mathbb{C}}$, by setting $\gamma(\infty) = a/c$ and $\gamma(-d/c) = \infty$. One natural question that one can ask is how to define the holomorphy of a modular forms at ∞. To do this, observe that there is a a natural action of Γ on $\mathbb{P}^1(\mathbb{Q})$, via the map

$$\Gamma \times \mathbb{P}^1(\mathbb{Q}) \to \mathbb{P}^1(\mathbb{Q})$$
$$(\gamma, (x\colon y)) \mapsto \gamma \begin{pmatrix} x \\ y \end{pmatrix} = (ax + by\colon cx + dy)$$

where $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. This action agrees with what we said above, namely that ∞ should be mapped to a/c and $-d/c$ should be mapped to ∞, because if we think to $\mathbb{P}^1(\mathbb{Q})$ as $\mathbb{Q} \cup \{\infty\}$ we identify $(1\colon 0)$ with ∞ and $(0\colon 1)$ and 0. We will say that two points $(x\colon y), (z\colon t) \in \mathbb{P}^1(\mathbb{Q})$ are Γ-*equivalent* if there exists $\gamma \in \Gamma$ s.t. $\gamma((x\colon y)) = (z\colon t)$. It's clear that being Γ-equivalent is an equivalence relation.

Definition 1.2. The *cusps* of the modular group are the Γ-equivalence classes of points of $\mathbb{P}^1(\mathbb{Q})$.

Remark 1.3. Γ has just 1 cusp, i.e. any two points of $\mathbb{P}^1(\mathbb{Q})$ are Γ-equivalent. Indeed, to check this it's enough to show that every point is Γ-equivalent to $(1\colon 0)$. If $(x\colon y) \in \mathbb{P}^1(\mathbb{Q})$, we can assume without loss of generality that $x, y \in \mathbb{Z}$ and that $(x, y) = 1$. So by Bezout's identity there exist $a, b \in \mathbb{Z}$ s.t. $ax + by = 1$. This tells us that

$$\begin{pmatrix} a & b \\ -y & x \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

with clearly $\begin{pmatrix} a & b \\ -y & x \end{pmatrix} \in \Gamma$.

One could now think that all this machinery is really useless. However, we'll see that this is not the case when we'll speak of congruence subgroups.
The next step is to clarify what we mean by being "weight k Γ-invariant".

Definition 1.4. Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{Q}) = \{\alpha \in \mathrm{GL}_2(\mathbb{Q})\colon \det \alpha > 0\}$.
The *factor of automorphy* $j(\gamma, -)\colon \mathcal{H} \to \mathbb{C}$ is given by

$$\tau \mapsto j(\gamma, \tau) \coloneqq c\tau + d$$

For any integer k, the *weight k-operator* $[\gamma]_k$ is the operator

$$[\gamma]_k\colon \{f\colon \mathcal{H} \to \mathbb{C}\} \to \{f\colon \mathcal{H} \to \mathbb{C}\}$$
$$f \mapsto f[\gamma]_k = (\det \gamma)^{k-1} (j(\gamma, \tau))^{-k} f(\gamma(\tau))$$

The weight-k operator and the factor of automorphy have some nice properties, as stated by the following

Lemma 1.5. For all $\gamma, \gamma' \in \Gamma$ and $\tau \in \mathcal{H}$,

a) $j(\gamma\gamma', \tau) = j(\gamma, \gamma'(\tau))j(\gamma', \tau)$;

b) $[\gamma\gamma']_k = [\gamma]_k[\gamma']_k$ (as operators);

c) $\Im(\gamma(\tau)) = \dfrac{\Im(\tau)}{|j(\gamma, \tau)|^2}$;

d) $\dfrac{d\gamma(\tau)}{d\tau} = \dfrac{1}{j(\gamma, \tau)^2}$.

Remark 1.6. Since the factor of automorphy is never 0 or infinity on $\mathcal{H}$, $f[\gamma]_k$ has the same number of zeroes and poles as f on $\mathcal{H}$, counted with multiplicities.

Now it should be clear that by weight k invariancy we mean invariancy under the action of the weight k-operator. So let's state our

Definition 1.7. Let $f\colon \mathcal{H} \to \mathbb{C}$ a meromorphic function, $k \in \mathbb{Z}$. f is called *weakly modular of weight* k if

$$f[\gamma]_k = f$$

for all $\gamma \in \Gamma$, namely if

$$f(\gamma(\tau)) = (c\tau + d)^k f(\tau)$$

for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ and $\tau \in \mathcal{H}$.

Remark 1.8. Setting $\gamma = -I$ and letting k be an odd integer, we find that if f is weakly modular of weight k, then $f = (-1)^k f$, so $f = 0$ if k is odd. Therefore there are no weakly modular function of odd weight.

Now we would like to understand how to define holomorphy at infinity. Since Γ contains the matrix $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ that acts on H mapping $\tau \mapsto \tau + 1$, any weakly modular function f must satisfy the equation

$$f(\tau + 1) = f(\tau)$$

for any $\tau \in \mathcal{H}$. Now set $D = \{q \in \mathbb{C}\colon |q| < 1\}$ and $D' = D \setminus \{0\}$. Then we have a holomorphic map

$$\begin{aligned} \mathcal{H} &\to D' \\ \tau &\mapsto e^{2\pi i\tau} = q \end{aligned}$$

and the map

$$\begin{aligned} g\colon D' &\to \mathbb{C} \\ q &\mapsto f\left(\frac{\log q}{2\pi i}\right) \end{aligned}$$

is well defined and $f(\tau) = g(e^{2\pi i\tau})$. Now if f is holomorphic on $\mathcal{H}$, then g is holomorphic on D' and so g has a Laurent expansion $g(q) = \sum_{n\in\mathbb{Z}} a_n q^n$ for $q \in D'$. The relation $|q| = e^{-2\pi\Im(\tau)}$ tells us that $q \to 0$ as $\Im(\tau) \to \infty$. So we can finally say that f is *holomorphic at* ∞ if g extends holomorphically to $q = 0$, i.e. if its Laurent series sums over $n \in \mathbb{N}$. This means that f has a *Fourier expansion*

$$f(\tau) = \sum_{n=0}^{+\infty} a_n q^n$$

with $a_n \in \mathbb{C}$ for all n.

Definition 1.9. Let $k \in \mathbb{Z}$. A function $f\colon \mathcal{H} \to \mathbb{C}$ is called *modular form of weight k* if

i) f is holomorphic on $\mathcal{H}$;

ii) f is weakly modular of weight k;

iii) f is holomorphic at infinity.

The set of modular forms of weight k is denoted with $M_k(\Gamma)$.

Remarks 1.10.

1) The zero function on $\mathcal{H}$ is a modular form of every weight; constant functions are modular forms of weight 0.

2) $M_k(\Gamma)$ is a vector space over $\mathbb{C}$. It can be shown that its dimension is finite for all k.

3) Since it's clear by definition that the product of a modular form of weight k and a modular form of weight l is a modular form of weight $k+l$, the $\mathbb{C}$-vector space
$$M(\Gamma) = \bigoplus_{k\in\mathbb{Z}} M_k(\Gamma)$$
has a structure of graded ring.

Definition 1.11. If $f \in M_k(\Gamma)$ for some k, we set $f(\infty) = a_0$ if $\sum_{n=0}^{+\infty} a_n q^n$ is the Fourier expansion of f. We say that f is a *cusp form* if $a_0 = 0$. The set of cusp forms of weight k will be denoted with $S_k(\Gamma)$.

As in the case of all modular forms, $S_k(\Gamma)$ is a vector space over $\mathbb{C}$ (obviously finite dimensional), and
$$S(\Gamma) = \bigoplus_{k\in\mathbb{Z}} S_k(\Gamma)$$
is a graded ideal of $M(\Gamma)$.
The first, and very important, examples of nontrivial modular forms are given by the *Eisenstein series of weight k*. Let $k \in 2\mathbb{Z}$, $k > 2$ and set

$$G_k(\tau) = \sum_{(0,0)\neq(c,d)\in\mathbb{Z}^2} \frac{1}{(c\tau+d)^k}$$

One can check that $G_k(\tau)$ converges absolutely and uniformly on compact subsets of $\mathcal{H}$, and therefore it defines an holomorphic function on $\mathcal{H}$, that is holomorphic at cusps but doesn't vanish there. In fact, we have the following Fourier expansion for $G_k(\tau)$:
$$G_k(\tau) = 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!} \sum_{n=1}^{+\infty} \sigma_{k-1}(n) q^n$$
where $\zeta(\cdot)$ is the Riemann zeta function and $\sigma_k(n) = \sum_{0\leq d|n} d^k$. Since $\zeta(s) \neq 0$ for all $s \in \mathbb{C}$ s.t. $\Re(s) > 1$, $G_k(\tau)$ is not a cusp form.

Definition 1.12. The *normalized Eisenstein series of weight k* is defined as $E_k(\tau) := \dfrac{G_k(\tau)}{2\zeta(k)}$ for any $k \in 2\mathbb{Z}$, $k > 2$.

The second most important example of a nontrivial modular form is given by the *modular discriminant*. Such a function is given by

$$\Delta(\tau) := (60G_4(\tau))^3 - 27(140G_6(\tau))^2$$

This is a cusp form of weight 12, and it spans the space $S_{12}(\Gamma)$. Moreover, one can prove that

$$\Delta(\tau) = (2\pi)^{12}\eta^{24}(\tau)$$

where

$$\eta^{24}(\tau) = q\prod_{n=1}^{+\infty}(1-q^n)^{24}$$

is the *Dedekind eta function*.

1.2 Modular forms for congruence subgroups

The first natural question one can ask is: what if we consider, instead of the whole modular group, a proper subgroup? So let's state the following

Definition 1.13. Let N be a positive integer. The *principal congruence subgroup of level N* is

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \colon \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N \right\}$$

A subgroup $\Gamma' \leq \Gamma$ is called a *congruence subgroup of level N* if $\Gamma(N) \subseteq \Gamma'$ for some $N \in \mathbb{N}$.

The following facts hold:

1) $\Gamma(1) = \Gamma$.

2) If $\Gamma' \leq \Gamma$ is a congruence subgroup of level N, then Γ' is a congruence subgroup of level M for any $M \in \mathbb{N}$ s.t. $N \mid M$.

3) $\Gamma(N)$ is the kernel of the natural homomorphism $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. In fact this map surjects, inducing an isomorphism $\Gamma/\Gamma(N) \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ and showing that $\Gamma(N) \trianglelefteq \Gamma$ and that $[\Gamma\colon \Gamma(N)] < \infty$.[1] This also implies that $[\Gamma\colon \Gamma'] < \infty$ for any congruence subgroup Γ'.

4) If Γ' is a congruence subgroup of level N and $\alpha \in \Gamma$, then $\alpha^{-1}\Gamma'\alpha$ is again a congruence subgroup of level N. This follows from the fact $\Gamma(N)$ is a normal subgroup of Γ and so $\Gamma(N) = \alpha^{-1}\Gamma(N)\alpha \subseteq \alpha^{-1}\Gamma'\alpha$, implying the claim.

[1] In fact we have that $[\Gamma\colon \Gamma(N)] = N^3 \prod_{p \mid N}\left(1 - \frac{1}{p^2}\right)$

The most important examples of congruence subgroups (of level N) are

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \colon \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod N \right\}$$

and

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \colon \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod N \right\}$$

Clearly one has

$$\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N) \subseteq \Gamma$$

Remarks 1.14. Fix $N \in \mathbb{N}$.

1) There is a group homomorphism

$$\Gamma_1(N) \to \mathbb{Z}/N\mathbb{Z}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto b \mod N$$

that is surjective. Its kernel is just $\Gamma(N)$, so $\Gamma(N) \trianglelefteq \Gamma_1(N)$, $[\Gamma_1(N) \colon \Gamma(N)] = N$ and we have an isomorphism

$$\Gamma_1(N)/\Gamma(N) \to \mathbb{Z}/N\mathbb{Z}$$

2) There is a group homomorphism

$$\Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^*$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d \mod N$$

that is surjective and has kernel $\Gamma_1(N)$. So $\Gamma_1(N) \trianglelefteq \Gamma_0(N)$, $[\Gamma_0(N) \colon \Gamma_1(N)] = \varphi(N)$ and we have an isomorphism

$$\Gamma_0(N)/\Gamma_1(N) \to (\mathbb{Z}/N\mathbb{Z})^*$$

$$\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right] \mapsto d$$

So we want to think about modular forms for some congruence subgroup Γ' as holomorphic functions $f \colon \mathcal{H} \to \infty$ s.t. $f[\gamma']_k = f$ for all $\gamma' \in \Gamma'$ that are holomorphic at the cusps. So it's straightforward to introduce the following

Definition 1.15. Let $\Gamma' \leq \Gamma$ be a congruence subgroup. The *cusps* of Γ' are Γ'-equivalence classes of points of $\mathbb{P}^1(\mathbb{Q})$.

Notice that the number of cusps of any congruence subgroup is finite, because it is at most $[\Gamma \colon \Gamma']$.
But what about Fourier expansions? A congruence subgroup Γ' may not contain the element $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, however it must contain an element in the form $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$ for some minimal $h \in \mathbb{N}$. Since the action of this element on points of $\mathcal{H}$ is just

the translation by h, it follows that a weakly modular $f\colon \mathcal{H} \to \mathbb{C}$ with respect to Γ' corresponds to a function

$$g\colon D' \to \mathbb{C}$$

where D' is the punctured disk but $f(\tau) = g(q_h)$ where $q_h = e^{2\pi i\tau/h}$. Hence if f is holomorphic, then so is g and f has a Laurent expansion

$$f(\tau) = \sum_{n\in\mathbb{Z}} a_n q_h^n$$

We'll say that f is holomorphic at infinity with respect to Γ' if g can be extended holomorphically in 0, i.e. if the Fourier expansion of f starts with $n = 0$.
Now, we want a modular form for Γ' to be holomorphic at every cusp, and if $\Gamma' \neq \Gamma$, there might be more than one cusp. Any cusp s takes the form $\alpha(\infty)$ for some $\alpha \in \Gamma$, so that holomorphy at s is defined by holomorphy at ∞ of $f[\alpha]_k$. Since such a modular form is holomorphic on $\mathcal{H}$ and weakly modular with respect to the congruence subgroup $\alpha^{-1}\Gamma\alpha$, the notion of its holomorphy at ∞ makes sense.

Definition 1.16. Let $\Gamma' \leq \Gamma$ be a congruence subgroup and $k \in \mathbb{Z}$. A *modular form of weight k with respect to* Γ' is a function $f\colon \mathcal{H} \to \mathbb{C}$ such that

i) f is holomorphic on $\mathcal{H}$;

ii) $f[\alpha]_k = f$ for all $\alpha \in \Gamma'$;

iii) $f[\alpha]_k$ is holomorphic at ∞ for all $\alpha \in \Gamma$.

If $a_0 = 0$ in the Fourier expansion of $f[\alpha]_k$ for all $\alpha \in \Gamma$, we say that f is a *cusp form of weight k with respect to* Γ'. The sets of modular forms and cusp forms of weight k with respect to Γ' will be denoted respectively by $M_k(\Gamma')$ and by $S_k(\Gamma')$.

Remarks 1.17. Let $\Gamma' \leq \Gamma$ be a congruence subgroup.

1) $M_k(\Gamma')$ and $S_k(\Gamma')$ are $\mathbb{C}$-vector spaces.

2) If $-I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \notin \Gamma'$, there could exist nonzero modular forms of odd weight with respect to Γ'.

3) If $\Gamma' \leq \Gamma''$ for some other congruence subgroup Γ'', then $M_k(\Gamma'') \subseteq M_k(\Gamma')$ and $S_k(\Gamma'') \subseteq S_k(\Gamma')$.

4) As in the case of the full modular group,

$$M(\Gamma') = \bigoplus_{k\in\mathbb{Z}} M_k(\Gamma')$$

is a graded ring and

$$S(\Gamma') = \bigoplus_{k\in\mathbb{Z}} S_k(\Gamma')$$

is a graded ideal of $M(\Gamma')$.

Remark 1.18. Since for all $N \in \mathbb{N}$, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_1(N)$, modular forms for $\Gamma_1(N)$ and for $\Gamma_0(N)$ have a Fourier expansion of the type

$$f(q) = \sum_{n=0}^{+\infty} a_n q^n$$

The main object of study in this thesis is a particular class of modular forms for $\Gamma_1(N)$. To define them, we need a bit more work, starting from Dirichlet characters.

Definition 1.19. Let G be a finite abelian group written multiplicatively. A *character* of G is just a homomorphism

$$\chi \colon G \to (\mathbb{C}^*, \cdot)$$

where $\cdot$ is the usual multiplication of complex numbers.
The set of all characters of G clearly forms a group that will be denoted by $\widehat{G}$. Such a group will be called the *dual group* of G. The unit of the dual group is the *trivial character*, namely the character

$$\mathbb{1}_G \colon G \to \mathbb{C}^*$$

$$g \mapsto 1$$

Since a character χ is a homomorphism and G is finite, the values taken by χ are complex roots of unity. Therefore the inverse of χ in $\widehat{G}$ is its conjugate, namely the character

$$\overline{\chi} \colon G \to \mathbb{C}^*$$
$$g \mapsto \overline{\chi(g)}$$

Proposition 1.20. Let G be a finite abelian group.

i) $\widehat{G}$ is non canonically isomorphic to G (and so in particular $|G| = |\widehat{G}|$).

ii) There is a canonical isomorphism

$$G \to \widehat{\widehat{G}}$$

$$g \mapsto \chi_g$$

where $\chi_g(\psi) := \psi(g)$ for all $\psi \in \widehat{G}$.

Definition 1.21. Let $N \in \mathbb{N}$. A *Dirichlet character modulo N* is a character of the multiplicative group $(\mathbb{Z}/N\mathbb{Z})^*$.

From now on, G_N will denote the multiplicative group $(\mathbb{Z}/N\mathbb{Z})^*$, $\widehat{G}_N$ its dual and $\mathbb{1}_N$ will denote the trivial character modulo N.

Proposition 1.22 (orthogonality relations)**.** Let $N \in \mathbb{N}$. Then we have the following relations:

$$\sum_{g \in G_N} \chi(g) = \begin{cases} \varphi(N) & \text{if } \chi = \mathbb{1}_N \\ 0 & \text{otherwise} \end{cases} \qquad \sum_{\chi \in \widehat{G}_N} \chi(g) = \begin{cases} \varphi(N) & \text{if } g = 1 \\ 0 & \text{otherwise} \end{cases}$$

Proof. We will only show the first relation, since the second one is just the first applied to $\widehat{G}_N$. If $\chi = \mathbb{1}_N$ the claim is obvious. Otherwise, choose $h \in G_N$ s.t. $\chi(h) \neq 1$. Then the product gh runs over all G_N as g runs over G_N, because G_N is finite. So we have

$$\sum_{g\in G_N} \chi(g) = \sum_{g\in G_N} \chi(gh) = \left(\sum_{g\in G_N} \chi(g)\right) \chi(h) \Longrightarrow (\chi(h)-1) \sum_{g\in G_N} \chi(g) = 0$$

and this implies $\sum_{g\in G_N} \chi(g) = 0$ since by assumption $\chi(h) \neq 1$. □

Let $N \in \mathbb{N}$ and $d \in \mathbb{N}$ s.t. $d \mid N$. Then every character modulo d lifts to a character modulo N. Indeed, if $\chi_d \in \widehat{G}_d$ and $\pi_{N,d} \colon G_N \to G_d$ is the natural projection, it's enough to define $\chi_N \coloneqq \chi_d \circ \pi_{N,d}$, namely we set $\chi_N(n) \coloneqq \chi_d(n \mod d)$ for all n relatively prime to N. For example, let χ_4 be the only nontrivial character modulo 4, namely

$$\chi_4 \colon G_4 \to \mathbb{C}^*$$
$$-1 \mapsto -1$$

This character lifts to

$$\widetilde{\chi} \colon G_{12} \to \mathbb{C}^*$$
$$5 \mapsto 1$$
$$7 \mapsto -1$$
$$11 \mapsto -1$$

The inverse construction, namely going from modulo N to modulo d for some $d \mid N$ is not always possible. For instance, the character modulo 8 given by

$$\chi_8 \colon G_8 \to \mathbb{C}^*$$
$$3 \mapsto 1$$
$$5 \mapsto -1$$
$$7 \mapsto -1$$

cannot be defined modulo 4, because if it were possible, we should have $\chi_8(5) = 1$ since $5 \equiv 1 \mod 4$.
This motivates the following

Definition 1.23. Let $\chi \in \widehat{G}_N$ be a Dirichlet character. The *conductor* of χ is the smallest positive divisor d of N s.t. $\chi = \chi_d \circ \pi_{N,d}$ for some $\chi_d \in \widehat{G}_d$. Equivalently, the conductor is the smallest positive divisor of N s.t. χ is trivial on $\ker \pi_{N,d}$. χ is said to be *primitive* if its conductor is N.

A character modulo N is called *odd* if $\chi(-1) = -1$. Otherwise, namely if $\chi(-1) = 1$, it's called *even*.
The only character with conductor 1 is the trivial one, and the trivial character modulo N is primitive iff $N = 1$.
Every character χ modulo N extends to a completely multiplicative function

$$\overline{\chi} \colon \mathbb{Z} \to \mathbb{C}$$

$$n \mapsto \begin{cases} \chi(n) & \text{if } (n, N) = 1 \\ 0 & \text{otherwise} \end{cases}$$

We are now ready to define type (k, χ) modular forms. Fix a level $N \in \mathbb{N}$ and an element $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$. Then recall that, by remark 1.14, $\Gamma_0(N) \trianglelefteq \Gamma_1(N)$, so that $M_k(\Gamma_1(N)) \subseteq M_k(\Gamma_0(N))$. This implies that the weight-k operator defines a map

$$M_k(\Gamma_1(N)) \to M_k(\Gamma_1(N))$$

$$f \mapsto f[\alpha]_k$$

Indeed, choose $\gamma \in \Gamma_1(N)$. By the normality of $\Gamma_1(N)$ in $\Gamma_0(N)$ we have that $\alpha^{-1}\Gamma_1(N)\alpha = \Gamma_1(N)$, so there exists $\gamma' \in \Gamma_1(N)$ s.t. $\alpha\gamma = \gamma'\alpha$. By lemma 1.5, we have that

$$(f[\alpha]_k)[\gamma_k] = f[\alpha\gamma]_k = f[\gamma'\alpha]_k = (f[\gamma'_k])[\alpha]_k = f[\alpha]_k$$

because $f \in M_k(\Gamma_1(N))$. Again by lemma 1.5, we can define a group action

$$\Gamma_0(N) \times M_k(\Gamma_1(N)) \to M_k(\Gamma_1(N))$$

$$(\alpha, f) \mapsto f[\alpha]_k$$

Now one can notice that $\Gamma_1(N)$ acts trivially on $M_k(\Gamma_1(N))$ via this map. So passing to the quotient we get an action

$$\Gamma_0(N)/\Gamma_1(N) \times M_k(\Gamma_1(N)) \to M_k(\Gamma_1(N))$$

Since we have shown in remark 1.14 that $\Gamma_0(N)/\Gamma_1(N) \cong \mathbb{Z}/N\mathbb{Z}$ via the map that sends $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d \mod N$, we have that $f[\alpha]_k$ depends only on $d \mod N$ and so it makes sense to write

$$f[\alpha]_k = \langle d \rangle f$$

Definition 1.24. The $\mathbb{C}$-linear map

$$\langle d \rangle \colon M_k(\Gamma_1(N)) \to M_k(\Gamma_1(N))$$

$$f \mapsto \langle d \rangle f$$

for $d \in \mathbb{N}$ is called *diamond operator*, where by definition we set $\langle d \rangle = 0$ if $(N, d) > 1$.

Obviously, $\langle 1 \rangle f = f$, since $\langle 1 \rangle f = f[I]_k$, where I is the identity matrix.

Proposition 1.25. The map

$$\langle - \rangle \colon \mathbb{N} \to \hom_{\mathbb{C}}(M_k(\Gamma_1(N)), M_k(\Gamma_1(N)))$$

$$n \mapsto \langle n \rangle$$

is completely multiplicative. Hence

$$\langle m \rangle \langle n \rangle = \langle n \rangle \langle m \rangle = \langle mn \rangle$$

for all $m, n \in \mathbb{N}$.

Definition 1.26. With the same notations as above, let $\chi \in \widehat{G}_N$ be a Dirichlet character with the same parity of k, i.e. such that $\chi(-1) = (-1)^k$. We'll call *modular form of type* (k, χ) *on* $\Gamma_0(N)$ an element $f \in M_k(\Gamma_1(N))$ s.t.

$$\langle d \rangle f = \chi(d) f$$

for all $d \in G_N$, i.e. such that

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = \chi(d)(c\tau + d)^k f(\tau)$$

for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$.
We'll denote the set of type (k, χ) modular forms of level N by $M_k(N, \chi)$.
In an analogous way we can define the space $S_k(N, \chi)$ of type (k, χ) cusp forms.

Notice that since $-I \in \Gamma_0(N)$, if χ and k would not have the same parity, then it would follow $M_k(N, \chi) = \{0\}$.
One can show that $M_k(N, \chi)$ is a finite dimensional $\mathbb{C}$-vector space and $S_k(N, \chi)$ is a proper subspace. If $\chi = \mathbb{1}_N$ then clearly $M_k(N, \chi) = M_k(\Gamma_0(N))$.

Proposition 1.27. There exist decompositions of vector spaces

$$M_k(\Gamma_1(N)) = \bigoplus_{\chi \in \widehat{G}_N} M_k(N, \chi) \qquad S_k(\Gamma_1(N)) = \bigoplus_{\chi \in \widehat{G}_N} S_k(N, \chi)$$

Proof. For each character $\chi \bmod N$, define the operator

$$\pi_\chi = \frac{1}{\varphi(N)} \sum_{d \in G_N} \overline{\chi}(d) \langle d \rangle \colon M_k(\Gamma_1(N)) \to M_k(\Gamma_1(N))$$

This is clearly a $\mathbb{C}$-linear operator on $M_k(\Gamma_1(N))$. Now take $f \in M_k(\Gamma_1(N))$ and $e \in G_N$. One has:

$$\langle e \rangle \pi_\chi(f) = \langle e \rangle \frac{1}{\phi(N)} \sum_{d \in G_N} \overline{\chi}(d) \langle d \rangle f = \frac{1}{\phi(N)} \sum_{d \in G_N} \overline{\chi}(d) \langle de \rangle f =$$

$$= \frac{1}{\phi(N)} \sum_{d \in G_N} \chi(e) \overline{\chi}(de) \langle de \rangle f = \chi(e) \pi_\chi(f)$$

because as d runs over all G_N, so does de for any fixed e. This proves by definition that $\pi_\chi(M_k(\Gamma_1(N))) \subseteq M_k(N, \chi)$. Moreover, if $f \in M_k(N, \chi)$ then

$$\pi_\chi(f) = \frac{1}{\phi(N)} \sum_{d \in G_N} \overline{\chi}(d) \chi(d) f = f$$

and so π_χ is the identity on $M_k(N, \chi)$. Therefore π_χ is the projection onto $M_k(N, \chi)$. Now note that

$$\sum_{\chi \in \widehat{G}_N} \pi_\chi = \frac{1}{\phi(N)} \sum_{\chi \in \widehat{G}_N} \sum_{d \in G_N} \overline{\chi(d)} \langle d \rangle = \frac{1}{\phi(N)} \sum_{d \in G_N} \langle d \rangle \sum_{\chi \in \widehat{G}_N} \overline{\chi}(d) = \langle 1 \rangle$$

where the last equality is due to the orthogonality relations. So $\sum_\chi \pi_\chi$ is the identity on $M_k(\Gamma_1(N))$ and this tells us that the subspaces $M_k(N,\chi)$ span $M_k(\Gamma_1(N))$. Indeed, take any $f \in M_k(\Gamma_1(N))$. Then

$$f = \sum_\chi \pi_\chi(f) = \sum_\chi \alpha_\chi f_\chi$$

where the $\alpha_\chi \in \mathbb{C}$ and $f_\chi \in M_k(N,\chi)$.
Finally, if $\chi \neq \chi'$ are distinct characters modulo N,

$$\pi_\chi \circ \pi_{\chi'} = \frac{1}{\phi(N)} \left(\sum_{d \in G_n} \overline{\chi}(d)\langle d \rangle \right) \frac{1}{\phi(N)} \left(\sum_{e \in G_n} \overline{\chi'}(e)\langle e \rangle \right) =$$

$$= \frac{1}{\phi(N)^2} \sum_{n \in G_N} \langle n \rangle \sum_{de=n} \overline{\chi}(d)\overline{\chi'}(e) = \frac{1}{\phi(N)^2} \sum_{n \in N} \langle n \rangle \overline{\chi}(n) \sum_{e \in G_n} \overline{\chi}(e^{-1})\overline{\chi'}(e) =$$

$$= \frac{1}{\phi(N)^2} \sum_{n \in N} \langle n \rangle \overline{\chi}(n) \sum_{e \in G_N} (\chi\overline{\chi'})(e) = 0$$

because of the orthogonality relations. This last property implies that $M_k(N,\chi) \cap M_k(N,\chi') = \{0\}$ for $\chi \neq \chi'$, because if f would lie in the intersection, then $(\pi_\chi \circ \pi_{\chi'})(f) = f$ since as we showed, π_χ is the identity on $M_k(N,\chi)$ for every χ. The operators π_χ restrict to $S_k(\Gamma_1(N))$ and hence the proof of the second decomposition goes in the same way. □

Note that by definition, the diamond operators respect the decomposition described in the proposition, i.e. if $\chi \in \widehat{G}_N$ and $n \in \mathbb{N}$, then

$$\langle n \rangle (M_k(N,\chi)) \subseteq M_k(N,\chi)$$

Definition 1.28. The *weight k Eisenstein space* of $\Gamma_1(N)$ is the quotient vector space

$$\mathscr{E}_k(\Gamma_1(N)) := M_k(\Gamma_1(N))/S_k(\Gamma_1(N))$$

Analogously, if $\chi \in \widehat{G}_N$, then we set

$$\mathscr{E}_k(N,\chi) := M_k(N,\chi)/S_k(N,\chi)$$

By proposition 1.27, we have a decomposition of vector spaces

$$\mathscr{E}_k(\Gamma_1(N)) = \bigoplus_{\chi \in \widehat{G}_N} \mathscr{E}_k(N,\chi)$$

1.3 Hecke operators

Let $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$, where $\mathrm{GL}_2^+(\mathbb{Q}) = \{\beta \in \mathrm{GL}_2(\mathbb{Q})\colon \det \beta > 0\}$. Let Γ_1, Γ_2 be congruence subgroups of Γ. Then the set

$$\Gamma_1 \alpha \Gamma_2 = \{\gamma_1 \alpha \gamma_2 \colon \gamma_1 \in \Gamma_1,\, \gamma_2 \in \Gamma_2\}$$

is called *double coset*.
The group Γ_1 acts on the double coset $\Gamma_1\alpha\Gamma_2$ by left multiplication, so we have a decomposition

$$\Gamma_1\backslash\Gamma_1\alpha\Gamma_2 = \bigcup_j \Gamma_1\beta_j$$

for some choice of representatives $\beta_j \in \Gamma_1\alpha\Gamma_2$. The key point is that this decomposition is finite, as shown by the following lemma, and this will allow us to define an important operator on $M_k(\Gamma_1(N))$.

Lemma 1.29. Let $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$, $\Gamma_1, \Gamma_2 \leq \Gamma$ two congruence subgroups.

i) Γ_1 and Γ_2 are *commensurable*, i.e. the indexes $[\Gamma_1 \colon \Gamma_1 \cap \Gamma_2]$, $[\Gamma_2 \colon \Gamma_1 \cap \Gamma_2]$ are both finite.

ii) The set $\alpha^{-1}\Gamma_1\alpha \cap \mathrm{SL}_2(\mathbb{Z})$ is a congruence subgroup.

iii) Set $\Gamma_3 = \alpha^{-1}\Gamma_1\alpha \cap \Gamma_2$, a subgroup of Γ_2. Then the map

$$\Gamma_2 \to \Gamma_1\alpha\Gamma_2$$

$$\gamma_2 \mapsto \alpha\gamma_2$$

induces a natural bijection from the coset space $\Gamma_3\backslash\Gamma_2$ to the orbit space $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$. Hence $\{\gamma_{2,j}\}$ is a set of coset representatives for $\Gamma_3\backslash\Gamma_2$ if and only if $\{\alpha\gamma_{2,j}\}$ is a set of orbit representatives for $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$.

Corollary 1.30. The orbit space $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$ is finite.

Proof. By point ii), $\alpha^{-1}\Gamma_1\alpha$ is a congruence subgroup, so by point i) the set $\Gamma_3\backslash\Gamma_2$ is finite and therefore by point iii) the claim follows. □

Definition 1.31. Let $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$, $\Gamma_1, \Gamma_2 \leq \Gamma$ be congruence subgroups. The *double coset operator*, or *weight-k* $\Gamma_1\alpha\Gamma_2$ *operator* takes modular forms $f \in M_k(\Gamma_1(N))$ to

$$f[\Gamma_1\alpha\Gamma_2]_k \coloneqq \sum_j f[\beta_j]_k$$

where $\{\beta\}_j$ is a set of orbit representatives, namely $\Gamma_1\alpha\Gamma_2 = \bigcup_j \Gamma_1\beta_j$ is a disjoint union.

Proposition 1.32.

i) The double coset operator is well defined, i.e. is independent from the choice of representatives.

ii) The double coset operator defines a $\mathbb{C}$-linear map

$$[\Gamma_1\alpha\Gamma_2]_k \colon M_k(\Gamma_1) \to M_k(\Gamma_2)$$

Moreover, it restricts to a map

$$[\Gamma_1\alpha\Gamma_2]_k \colon S_k(\Gamma_1) \to S_k(\Gamma_2)$$

Definition 1.33. Let $p \in \mathbb{N}$ be a prime, set $\alpha = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{Q})$ and $\Gamma_1 = \Gamma_2 = \Gamma_1(N)$. The *Hecke operator* T_p is given by

$$T_p \colon M_k(\Gamma_1(N)) \to M_k(\Gamma_1(N))$$
$$f \mapsto T_p f \coloneqq f[\Gamma_1(N)\alpha\Gamma_1(N)]_k$$

Proposition 1.34. The T_p operator on $M_k(\Gamma_1(N))$ is given by

$$T_p f = \begin{cases} \sum_{j=0}^{p-1} f[\begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}]_k & \text{if } p \mid N \\ \sum_{j=0}^{p-1} f[\begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}]_k + f[\begin{pmatrix} m & n \\ N & p \end{pmatrix}\begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}]_k & \text{if } p \nmid N \text{ and } mp - nN = 1 \end{cases}$$

The thing we are really interested in is how Hecke operators act on the Fourier expansion of modular forms. This is given by the following

Theorem 1.35. Let $N, p \in \mathbb{N}$ with p prime, $\chi \in \widehat{G}_N$ and $f \in M_k(N, \chi)$, so that f has a Fourier expansion of the form

$$f(q) = \sum_{n=0}^{+\infty} a_n q^n$$

Then $T_p f \in M_k(N, \chi)$ and we have

$$(T_p f)(q) = \sum_{n=0}^{+\infty} a_{np}(f) q^n + \chi(p) p^{k-1} \sum_{n=0}^{+\infty} a_n(f) q^{np} =$$

$$= \sum_{n=0}^{+\infty} (a_{np}(f) + \chi(p) p^{k-1} a_{n/p}(f)) q^n$$

where we set $a_{n/p}(f) = 0$ if $p \nmid n$ and χ is regarded as a function $\mathbb{N} \to \mathbb{C}$. In other words, for $f \in M_k(N, \chi)$ we have

$$a_n(T_p f) = a_{np}(f) + \chi(p) p^{k-1} a_{n/p}(f)$$

The definition of the Hecke operators can be extended to all $n \in \mathbb{N}$, via the following theorem.

Theorem 1.36. Set $T_1 = 1$ (the identity operator). Let $r, p \in \mathbb{N}$ with p prime and $r \geq 2$. Define

$$T_{p^r} = T_p T_{p^{r-1}} - p^{k-1} \langle p \rangle T_{p^{r-2}}$$

Then we have:

i) $T_{p^r} T_{q^s} = T_{q^s} T_{p^r}$ if p, q are distinct primes and $r, s \in \mathbb{N}$.

ii) For any $n \in \mathbb{N}$, set $T_n = \prod_i T_{p_i^{\alpha_i}}$ where $n = \prod_i p_i^{\alpha_i}$ is the prime factorization of n. Then $T_m T_n = T_n T_m$ for all $m, n \in \mathbb{N}$ and $T_m T_n = T_{mn}$ if $(m, n) = 1$.

iii) $T_p \langle d \rangle = \langle d \rangle T_p$ for all $d \in \mathbb{N}$.

iv) Fix $n, N \in \mathbb{N}$ and $\chi \in \widehat{G}_N$. Then for every $f \in M_k(N, \chi)$ we have that $T_n f \in M_k(N, \chi)$ and

$$T_n f = \sum_{m=0}^{+\infty} a_m(T_n f) q^m$$

where

$$a_m(T_n f) = \sum_{d|(m,n)} \chi(d) d^{k-1} a_{mn/d^2}(f)$$

1.4 Oldforms, newforms and eigenforms

The first step to do in order to understand newforms is to define an inner product on the space $S_k(\Gamma_1(N))$.
The *hyperbolic measure* on $\mathcal{H}$ is given by

$$d\mu(\tau) = \frac{dxdy}{y^2}$$

if $\tau = x + iy \in \mathcal{H}$.
Such a measure is $\mathrm{GL}_2^+(\mathbb{R})$-invariant, i.e. $d\mu(\alpha(\tau)) = d\mu(\tau)$ for all $\tau \in \mathcal{H}$ and all $\alpha \in \mathrm{GL}_2^+(\mathbb{R})$. If $\Gamma' \leq \Gamma$ be a congruence subgroup and $X(\Gamma')$ is a fundamental domain for the action of Γ' on $\mathcal{H}$, we define *volume* of Γ' the integral

$$V_{\Gamma'} := \int_{X(\Gamma')} d\mu(\tau)$$

Theorem 1.37. Let $\Gamma' \leq \Gamma$ be a congruence subgroup. The map

$$\langle -, - \rangle_{\Gamma'} \colon S_k(\Gamma') \times S_k(\Gamma') \to \mathbb{C}$$

$$(f, g) \mapsto \langle f, g \rangle_{\Gamma'} = \frac{1}{V_{\Gamma'}} \int_{X(\Gamma')} f(\tau) \overline{g(\tau)} (\Im(\tau)^k) d\mu(\tau)$$

is well defined, positive definite and turns $S_k(\Gamma')$ into an Hermitian space. This map is called *Petersson inner product.*[2]

Now recall the following

Definition 1.38. let V be a complex inner product space and T a linear operator on V. The *adjoint* of T is the linear operator defined by

$$\langle Tv, w \rangle = \langle v, T^* w \rangle$$

A linear operator T is called *normal* if it commutes with its adjoint.

Theorem 1.39. Let $p \in \mathbb{N}$ be a prime s.t. $p \nmid N$. Then in the inner product space $S_k(\Gamma_1(N))$, the Hecke operators $\langle p \rangle$ and T_p have adjoints

$$\langle p \rangle^* = \langle p \rangle^{-1} \qquad T_p^* = \langle p \rangle^{-1} T_p$$

Then it follows by theorem 1.36 that $\langle p \rangle$ and T_p are normal.

[2]More generally, it can be shown that the integral defining the Petersson inner product converges if at least one between f and g is a cusp form and the inner product of a cusp form and an Eisenstein series is always 0. This tells us that, using a slight abuse of language, the spaces $S_k(\Gamma_1(N))$ and $\mathscr{E}_k(\Gamma_1(N))$ are orthogonal with respect to the Petersson inner product.

The spectral theorem of linear algebra easily implies the following fundamental

Theorem 1.40. The space $S_k(\Gamma_1(N))$ has an orthogonal basis of simultaneous eigenvectors for the Hecke operators $\{\langle n\rangle, T_n \colon (n,N)=1\}$.

Definition 1.41. A nonzero modular form $f \in M_k(\Gamma_1(N))$ that is a simultaneous eigenvector for all Hecke operators $\langle n\rangle$ and T_n, for $n \in \mathbb{Z}^+$ is called *eigenform*. An eigenform is said to be *normalized* if $a_1 = 1$ in its Fourier expansion.

To conclude the section we will show how one can decompose $S_k(\Gamma_1(N))$ into two subspaces orthogonal with respect to the Petersson inner product.
First, notice that if $M, N \in \mathbb{N}$ are s.t. $M \mid N$, then $\Gamma_1(N) \subseteq \Gamma_1(M)$ and so $S_k(\Gamma_1(M)) \subseteq S_k(\Gamma_1(N))$. Now suppose $d \in \mathbb{N}$ is s.t. $d \mid N/M$. Then set $\alpha_d = \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix}$ so that we can define a $\mathbb{C}$-linear map

$$S_k(\Gamma_1(M)) \to S_k(\Gamma_1(N))$$
$$f(\tau) \mapsto f(\tau)[\alpha_d]_k = d^{k-1} f(d\tau)$$

which is injective (it is an easy computation). By this observation, it will be natural to look at the subspace of $S_k(\Gamma_1(N))$ spanned by forms "coming from a lower level".

Definition 1.42. For any divisor d of N, let's define a map

$$i_d \colon S_k(\Gamma_1(N/d)) \times S_k(\Gamma_1(N/d)) \to S_k(\Gamma_1(N))$$
$$(f,g) \mapsto f + g[\alpha_d]_k$$

The subspace of *oldforms at level* N is

$$S_k(\Gamma_1(N))^{old} = \sum_{d \mid N} i_d(S_k(\Gamma_1(N/d)) \times S_k(\Gamma_1(N/d)))$$

and the space of *newforms at level* N is its orthogonal complement with respect to the Petersson inner product, i.e.

$$S_k(\Gamma_1(N))^{new} = (S_k(\Gamma_1(N))^{old})^{\perp}$$

Proposition 1.43. The subspaces $S_k(\Gamma_1(N))^{old}$ and $S_k(\Gamma_1(N))^{new}$ are stable under all Hecke operators.

Corollary 1.44. The subspaces $S_k(\Gamma_1(N))^{old}$ and $S_k(\Gamma_1(N))^{new}$ have orthogonal bases of eigenforms for the Hecke operators T_n and $\langle n\rangle$ for all $n \in \mathbb{N}$ such that $(n,N)=1$.

It can be shown that the condition $(n,N)=1$ can be removed from $S_k(\Gamma_1(N))^{new}$.

Definition 1.45. A *newform* is a normalized eigenform in $S_k(\Gamma_1(N))^{new}$.

Remark 1.46. By theorem 1.35, it's clear that if $f = \sum_{n=0}^{+\infty} a_n q^n$ is any eigenform in $S_k(\Gamma_1(N))$ and p is a prime, then since we have $T_p f = \lambda_p f$ for some $\lambda_p \in \mathbb{C}$, $\lambda_p = a_1^{-1} a_p$.[3] Hence if f is normalized, its p-th coefficient is an eigenvalue of T_p.

[3] As next theorem says, one always has $a_1 \neq 0$ for an eigenform.

It is useful to note that the converse also holds.

Theorem 1.47. Let $f \in M_k(N, \chi)$. Then f is a normalized eigenform if and only if its Fourier coefficients satisfy the following conditions

i) $a_1 = 1$;

ii) $a_{p^r} = a_p a_{p^{r-1}} - \chi(p) a_{p^{r-2}}$ for all primes p and $r \geq 2$;

iii) $a_{mn} = a_m a_n$ for all $m, n \in \mathbb{N}$ s.t. $(m, n) = 1$.

Now it will be straightforward to define newforms on $S_k(N, \chi)$. More details can be found in [Li75].
So fix $M, N \in \mathbb{N}$ and $\chi \in \widehat{G}_M$. The main observation is that if $M \mid N$ and $d \mid N/M$, then the map $f \mapsto f[\alpha_d]_k$ restricts to a map

$$S_k(M, \chi) \to S_k(N, \chi)$$

$$f \mapsto f[\alpha_d]_k$$

where with a slight abuse of language we will use χ also to denote the extension of χ to G_N. To prove this, recall that $f \in S_k(M, \chi)$ means that $\langle e \rangle f = \chi(e) f$ for all $e \in G_M$. So choose any $\gamma = \begin{pmatrix} a & b \\ c & e \end{pmatrix} \in \Gamma_0(N)$ and note that

$$\alpha_d \gamma = \begin{pmatrix} da & db \\ c & e \end{pmatrix} = \begin{pmatrix} a & db \\ c/d & e \end{pmatrix} \alpha_d := \gamma' \alpha_d$$

where clearly $\gamma' \in \Gamma_0(M)$ because $N \mid c$ and so $M \mid c/d$. This calculation implies that

$$f[\alpha_d]_k[\gamma]_k = f[\alpha_d \gamma]_k = f[\gamma']_k[\alpha_d]_k = \chi(e) f[\alpha_d]_k$$

i.e. $f[\alpha_d] \in S_k(N, \chi)$.
Now fix $\chi \in \widehat{G}_N$ and consider the set $A = \{N_i \in \mathbb{N} \colon \chi \text{ can be defined mod } N_i\}$. Then we can define a subspace $S_k^-(N, \chi)$ as the span of the set

$$\{f_i[\alpha_{d_{ij}}] \colon f_i \in S(N_i, \chi) \text{ for some } N_i \in A, d_{ij} \mid N/N_i\}$$

Definition 1.48. The complement of $S_k^-(N, \chi)$ inside $S_k(N, \chi)$ is denoted by $S_k^+(N, \chi)$ and is called *space of newforms on* $S_k(N, \chi)$.

Remarks 1.49.

1) The subspaces $S_k^+(N, \chi)$ and $S_k^-(N\, \chi)$ are orthogonal under the Petersson inner product.

2) The Hecke operators T_p for p prime respect the decomposition of $S_k(N, \chi)$. Therefore we can find a basis for $S_k^+(N, \chi)$ made of eigenforms. The elements of this basis are called *newforms*. A newform will be called *normalized* if $a_1 = 1$ in its Fourier expansion.

3) If two newforms have the same eigenvalues λ_p for almost all p, then they differ by a constant factor (cfr. [Li75]). This is a very important result, since it tells us that the subspace of $S_k^+(N, \chi)$ relative to a collection of eigenvalues $\{\lambda_p\}_p$ has dimension 1.

4) Each element $f(\tau) \in S_k(N,\chi)$ can be written as

$$f(\tau) = \sum_i f_i(d_i\tau)$$

where $d_iN_i \mid N$, χ can be defined $\bmod N_i$ and $f_i \in S_k(N_i,\chi)$ is a newform. We will show this by induction. For $N = 2$, we have clearly that $S_k(2, \mathbb{1}_2) = S_k^+(N, \mathbb{1}_2)$ and so the result is obvious. Suppose it's true for every $2 \le r \le N$. Then take $f(\tau) \in S_k(N+1,\chi)$. We can then write $f(\tau) = g_1(\tau) + g_2(\tau)$, where $g_1 \in S_k^-(N+1,\chi)$ and $g_2 \in S_k(N+1,\chi)$. Then by definition $g_1(\tau) = \sum_i f_i(d_i\tau)$, for some $d_iN_i \mid N+1$, such that χ can be defined $\bmod N_i$ and $f_i(\tau) \in S_k(N_i,\chi)$. Now take $f_i(d_i\tau)$ and set $d_i\tau = \tau'$. Then $f_i(\tau') \in S_k(N_i,\chi)$ and so by induction hypothesis we have $f_i(\tau') = \sum_j g_{ij}(d_{ij}\tau')$ where $d_{ij}N_{ij} \mid N_i$, χ can be defined $\bmod N_{ij}$ and $g_{ij}(\tau') \in S_k^+(N_{ij},\chi)$. So we have what we wanted, since we can write

$$f_i(\tau') = f_i(d\tau) = \sum_j g_{ij}(d_{ij}d\tau)$$

where $d_{ij}dN_{ij} \mid N+1$, χ can be defined $\bmod N_{ij}$ and $g_{ij}(\tau)$ is a newform in $S_k(N_{ij},\chi)$. The claim follows from the fact that this is true for all i.

In conclusion, what we found is that any element $f \in M_k(N,\chi)$ can be written as

$$f(\tau) = E(\tau) + \sum_i f_i(d_i\tau)$$

where $E(\tau) \in \mathscr{E}_k(N,\chi)$ is an Eisenstein series and the f_i are as above. The last important result tells us that we can find a basis for the space $\mathscr{E}_1(N,\chi)$ made by normalized eigenforms for the Hecke operators T_p with $p \nmid N$. This will allow us to associate a Galois representation to any element of this basis, but it will be a *reducible* representation.

Theorem 1.50. Let $N \in \mathbb{N}$ and let $A_{N,1}$ be the set of all triples $(\{\psi,\varphi\},t)$ s.t.

a) ψ and φ are primitive characters modulo u and v respectively;

b) $(\psi\varphi)(-1) = -1$;[4]

c) $t \in \mathbb{N}$ is s.t. $tuv \mid N$.

Now set

$$E_1^{\psi,\varphi}(\tau) := \delta(\varphi)L(0,\psi) + \delta(\psi)L(0,\varphi) + 2\sum_{n=1}^{+\infty}\sigma_0^{\psi,\varphi}(n)q^n, \quad q = e^{2\pi i\tau}$$

where $\delta(\varphi) = 1$ iff $\varphi = \mathbb{1}_1$ and is 0 otherwise, while

$$\sigma_0^{\psi,\varphi} = \sum_{\substack{m|n \\ m>0}} \psi(n/m)\varphi(m)$$

and $L(s,\psi)$ is the L-function associated to ψ. If $E_1^{\psi,\varphi,t} := E_1^{\psi,\varphi}(t\tau)$, we have:

[4] When we compute such a product, we implicitly assume that we have raised ψ and φ to level N to make the product have sense.

i) The set

$$\mathcal{B}_1(\Gamma_1(N)) := \{E_1^{\psi,\varphi,t} \colon (\{\psi,\varphi\},t) \in A_{N,1}\}$$

is a basis of the space $\mathscr{E}_1(\Gamma_1(N))$. Moreover, for any character $\chi \mod N$, the set

$$\mathcal{B}_1(N,\chi) := \{E_1^{\psi,\varphi,t} \colon (\{\psi,\varphi\},t) \in A_{N,1}, \psi\varphi = \chi\}$$

is a basis of $\mathscr{E}_1(N,\chi)$.

ii) If $p \in \mathbb{N}$ is a prime s.t. $p \nmid N$, we have that

$$T_p E_1^{\psi,\varphi,t} = (\psi(p) + \varphi(p)) E_1^{\psi,\varphi,t}$$

for every $E_1^{\psi,\varphi,t} \in \mathcal{B}_1(N,\chi)$.

To conclude the chapter, we cite without proof this fundamental fact about newforms.

Theorem 1.51. Let $f = \sum_{n=1}^{+\infty} a_n q^n \in S_k(N,\chi)$, let σ be a automorphism of $\mathbb{C}$. Let $f^\sigma := \sum_{n=1}^{+\infty} a_n^\sigma q^n$. Then

i) $f^\sigma \in S_k(N,\chi^\sigma)$;

ii) if the a_n are algebraic, they have bounded denominators;

iii) the eigenvalues of the Hecke operators T_p lie in the ring of integers of a fixed algebraic number field.

Proof. See [Ser77b]. □

Chapter 2

Galois representations

2.1 The Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

Definition 2.1. The *absolute Galois group of* $\mathbb{Q}$ is the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, where $\overline{\mathbb{Q}}$ denotes an algebraic closure of $\mathbb{Q}$.

In this entire thesis, we fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$, so that when we will speak of $\overline{\mathbb{Q}}$ we will think of it as a subfield of $\mathbb{C}$. Also, the p-adic valuation on $\mathbb{Q}_p$ will be normalized, i.e. $v_p(p) = 1$. From now on, we set $G_{\mathbb{Q}} \coloneqq \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Furthermore, if $\sigma \in \mathrm{Gal}(F/K)$ for some fields $K \subseteq F$ and $x \in F$, we'll denote the image of x by σ by x^σ.
It is clear that $\overline{\mathbb{Q}}$ is the union of all Galois number fields. Indeed, if $x \in \overline{\mathbb{Q}}$, then $\mathbb{Q}(x)$ is a number field contained in $\overline{\mathbb{Q}}$ and so is its normal closure, which is Galois over $\mathbb{Q}$. Conversely if F is a Galois number field, each of its elements is algebraic over $\mathbb{Q}$, and so lies in $\overline{\mathbb{Q}}$. Moreover, the collection $\{\mathrm{Gal}(F/\mathbb{Q})\colon F/\mathbb{Q} \text{ is a finite Galois extension}\}$ is a projective system whose maps are the ones induced by inclusions, i.e. if $K \subseteq F$ is an extension of Galois number field we have a canonical restriction map

$$\mathrm{Gal}(F/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q})$$

$$\sigma \mapsto \sigma_K \coloneqq \sigma|_K$$

that is surjective.

Proposition 2.2. We have $G_{\mathbb{Q}} \cong \varprojlim_F \mathrm{Gal}(F/\mathbb{Q})$, where F runs over all finite Galois extensions of $\mathbb{Q}$.

Proof. Let $\sigma \in G_{\mathbb{Q}}$, let $F \subseteq \overline{\mathbb{Q}}$ be a Galois number field. Then $\sigma|_F$ lies in $\mathrm{Gal}(F/\mathbb{Q})$, because $F/\mathbb{Q}$ is Galois. Moreover, it's clear that if $K \subseteq F$ is another Galois number field, then $\sigma|_K = (\sigma|_F)_K$. Therefore σ define an element of $\varprojlim_F \mathrm{Gal}(F/\mathbb{Q})$ and the map obtained in this way is clearly injective. On the other hand, take an element $\{\sigma_F\} \in \varprojlim_F \mathrm{Gal}(F/\mathbb{Q})$. This comes from an element $\sigma \in G_{\mathbb{Q}}$ in an obvious way, namely if $x \in \overline{\mathbb{Q}}$ then $x \in F$ for some Galois number field F and so we set $x^\sigma \coloneqq x^{\sigma_F}$. This proves that the map is also surjective, and we are done. □

The group $G_{\mathbb{Q}}$ is then a *profinite group*, namely a projective limit of finite groups. Hence it carries a structure of topological group, the one induced by the inclusion

$$G_{\mathbb{Q}} = \varprojlim_{F}\{\mathrm{Gal}(F/\mathbb{Q})\} \subseteq \prod_{F} \mathrm{Gal}(F/\mathbb{Q}) := C$$

where the product is taken over all Galois number fields. Here we are considering the discrete topology on the finite Galois groups $\mathrm{Gal}(F/\mathbb{Q})$ and the product topology on C. By Tychonoff's theorem, C is a compact topological space. Moreover, $G_{\mathbb{Q}}$ is a closed subspace, because if $\{\sigma_F\} \in C \setminus G_{\mathbb{Q}}$, then by definition there exists an extension of number fields $K \subseteq L$ and two elements $\sigma_K \in \mathrm{Gal}(K/\mathbb{Q})$ and $\sigma_L \in \mathrm{Gal}(L/\mathbb{Q})$ such that $\sigma_L|_K \neq \sigma_K$. Therefore the set $\{\{\tau_F\} \in C \colon \tau_K = \sigma_K,\, \tau_L = \sigma_L\}$ is an open subspace that does not intersect $G_{\mathbb{Q}}$ and contains $\{\sigma_F\}$. So we proved that $G_{\mathbb{Q}}$ is compact. Moreover, one can see that $G_{\mathbb{Q}}$ is Hausdorff and totally disconnected, i.e. its only connected components are the points. The properties of being a Hausdorff, compact and totally disconnected topological group characterize completely profinite groups (see for example [CA67]).
The same result holds for any Galois extension F/K, in the sense that $\mathrm{Gal}(F/K) \cong \varprojlim_{L} \mathrm{Gal}(L/K)$ where L runs over all finite Galois extensions L/K s.t. $L \subseteq F$ and again $\mathrm{Gal}(F/K)$ is a topological group. So we can recall the main theorem of Galois theory for possibly infinite extensions.

Theorem 2.3 (Krull)**.** Let F/K be a Galois extension of fields, and $K \subseteq L \subseteq F$ a subextension. Then $\mathrm{Gal}(F/L)$ is a closed subgroup of $G := \mathrm{Gal}(F/K)$. Moreover, the maps

$$L \mapsto H := \mathrm{Gal}(F/L) \text{ and } H \mapsto L := F^H$$

yield an inclusion-reversing bijection between subfields $K \subseteq L \subseteq F$ and closed subgroups $H \subseteq G$, where by F^H we are denoting the subfield of F fixed pointwise by the elements of H. A subextension L/K is Galois over K if and only if $\mathrm{Gal}(F/L)$ is normal in $\mathrm{Gal}(F/K)$; in this case there is a natural isomorphism $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(F/K)/\mathrm{Gal}(F/L)$.

From now on, every time we will have a group G acting on a set X, we will denote the subset of pointwise fixed elements by X^G. Note that if $\sigma \in G$ and $Y \subseteq X$ is any subset, with Y^σ we denote the set $\{y^\sigma \colon y \in Y\}$, while $Y^{\{\sigma\}} = \{y \in Y \colon y^\sigma = y\}$.

Remark 2.4. By the theorem, we have that for any Galois number field $F/\mathbb{Q}$, the restriction map

$$\pi_F \colon G_{\mathbb{Q}} \to \mathrm{Gal}(F/\mathbb{Q})$$
$$\sigma \mapsto \sigma|_F$$

is surjective. This is a general fact about inverse limits of surjective systems, namely if $\{G_i\}_{i \in I}$ is an surjective system of groups, the projections

$$\varprojlim_{i \in I} G_i \to G_i$$
$$\{g_i\}_{i \in I} \mapsto g_i$$

are surjective.

Now, a system of open neighborhoods in $G_{\mathbb{Q}}$ for $1 = 1_{G_{\mathbb{Q}}}$ is the one generated by the kernels of the projections

$$G_{\mathbb{Q}} \to \mathrm{Gal}(F/\mathbb{Q})$$

as F runs over all Galois number fields. Since $G_{\mathbb{Q}}$ is a topological group, it follows that a system of open neighborhoods for any $\sigma \in G_{\mathbb{Q}}$ is generated by

$$U_\sigma(F) \coloneqq \sigma \cdot \ker(G_{\mathbb{Q}} \to \mathrm{Gal}(F/\mathbb{Q}))$$

as F runs over all Galois number fields. Clearly, $U_1(F)$ is an open normal subgroup of $G_{\mathbb{Q}}$ for every Galois number field F. But the converse also holds. Indeed, if $U \subseteq G_{\mathbb{Q}}$ is an open normal subgroup, then $U(F) \subseteq U$ for some Galois number field F. So we get a surjection

$$\mathrm{Gal}(F/\mathbb{Q}) = G_{\mathbb{Q}}/U(F) \to G_{\mathbb{Q}}/U$$

which by Galois theory main theorem implies that $G_{\mathbb{Q}}/U = \mathrm{Gal}(F'/\mathbb{Q})$ for some $F' \subseteq F$ and hence $U = U_1(F')$.
The next step is understanding maximal ideals of $\overline{\mathbb{Z}}$. Let $\mathfrak{p} \subseteq \overline{\mathbb{Z}}$ such an ideal. Let $\mathcal{O}_K \subseteq \overline{\mathbb{Z}}$ be any number ring. Since the extension $\mathcal{O}_K \subseteq \overline{\mathbb{Z}}$ is integral, the ideal $\mathfrak{p} \cap \mathcal{O}_K$ is maximal. Therefore in particular when $K = \mathbb{Q}$ we have that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ for some rational prime p. Conversely, given such a rational prime, the ideal $p\overline{\mathbb{Z}}$ is contained by Zorn's lemma in some maximal ideal $\mathfrak{p}$.
Since $\overline{\mathbb{Z}} = \bigcup_K \mathcal{O}_K$ for all number fields K, any maximal ideal $\mathfrak{p} \subseteq \overline{\mathbb{Z}}$ is given by $\mathfrak{p} = \bigcup_K \mathfrak{p}_K$ where $\mathfrak{p}_K = \mathfrak{p} \cap \mathcal{O}_K$ and the $\mathfrak{p}_K$ are compatible, in the sense that if $K' \subseteq K$ are two number fields, then $\mathfrak{p}_K \cap K' = \mathfrak{p}_{K'}$. Conversely, every such union defines a maximal ideal of $\overline{\mathbb{Z}}$.
It is easy to check that if $\mathfrak{p} \subseteq \overline{\mathbb{Z}}$ is a maximal ideal and $p = \mathfrak{p} \cap \mathbb{Z}$, then $\overline{\mathbb{Z}}/\mathfrak{p}$ is an algebraic closure of $\mathbb{F}_p$. From now on, we'll always identify $\overline{\mathbb{Z}}/\mathfrak{p}$ with $\overline{\mathbb{F}}_p$.
So let $p \in \mathbb{Z}$ be a prime and let $\mathfrak{p} \subseteq \overline{\mathbb{Z}}$ be any maximal ideal lying over p. Then we have a reduction map

$$\overline{\mathbb{Z}} \to \overline{\mathbb{F}}_p$$

whose kernel is $\mathfrak{p}$.

Definition 2.5. The *decomposition group of* $\mathfrak{p}$ is defined as

$$D_{\mathfrak{p}} = \{\sigma \in G_{\mathbb{Q}} \colon \mathfrak{p}^\sigma = \mathfrak{p}\}$$

One can also see that $D_{\mathfrak{p}} \cong \varprojlim_F D_{\mathfrak{p}_F}$ where F runs over all Galois number fields, $\mathfrak{p}_F \coloneqq \mathfrak{p} \cap F$ and $D_{\mathfrak{p}_F}$ is the decomposition group of $\mathfrak{p}_F$ in F. In fact, it's clear that we have a homomorphism

$$D_{\mathfrak{p}} \to \varprojlim_F D_{\mathfrak{p}_F}$$

$$\sigma \mapsto \{\sigma_F\}$$

which is injective. On the other hand any $\{\sigma_F\} \in \varprojlim_F D_{\mathfrak{p}_F}$ is by definition an element of $G_{\mathbb{Q}}$ and so the map is surjective too. Now the point is that if $F/\mathbb{Q}$ is a finite Galois extension, then for every rational prime p and every prime $\mathfrak{p} \subseteq F$ lying over p it's known (see for example [Ser79]) that there exists an isomorphism

$$D_{\mathfrak{p}_F} \xrightarrow{\sim} \mathrm{Gal}(F_{\mathfrak{p}}/\mathbb{Q}_p)$$

where $F_{\mathfrak{p}}$ denotes the completion of F with respect to the discrete valuation induced by $\mathfrak{p}$. This tells us that

$$D_{\mathfrak{p}} \cong \varprojlim_K \mathrm{Gal}(K/\mathbb{Q}_p)$$

where K runs over all the finite extensions of $\mathbb{Q}_p$. But again, it is easy to see that

$$\varprojlim_K \mathrm{Gal}(K/\mathbb{Q}_p) = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \coloneqq G_p$$

So what we found is that we can identify the decomposition group of any maximal ideal $\mathfrak{p} \subseteq \overline{\mathbb{Z}}$ with the local Galois group G_p. What happens if we choose another $\mathfrak{p}' \subseteq \overline{\mathbb{Z}}$ lying over p? We'll see in proposition 2.8 that there exists $\sigma \in G_{\mathbb{Q}}$ s.t. $\mathfrak{p}^{\sigma} = \mathfrak{p}'$ and $D_{\mathfrak{p}'} = \sigma^{-1} D_{\mathfrak{p}} \sigma$. This shows choosing another $\mathfrak{p}$ lying over p the embedding $G_p \hookrightarrow G_{\mathbb{Q}}$ changes by conjugation.
Any $\sigma \in D_{\mathfrak{p}}$ gives rise to a commutative diagram

$$\begin{array}{ccc} \overline{\mathbb{Z}} & \xrightarrow{\sigma} & \overline{\mathbb{Z}} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \overline{\mathbb{F}}_p & \xrightarrow{\widetilde{\sigma}} & \overline{\mathbb{F}}_p \end{array}$$

where $(x + \mathfrak{p})^{\widetilde{\sigma}} \coloneqq x^{\sigma} + \mathfrak{p}$. What we have is thus a map

$$D_{\mathfrak{p}} \to G_{\mathbb{F}_p} \coloneqq \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$$

$$\sigma \mapsto \widetilde{\sigma}$$

which is surjective.

Definition 2.6. The *inertia group of* $\mathfrak{p}$, denoted by $I_{\mathfrak{p}}$, is the kernel of the map $D_{\mathfrak{p}} \to G_{\mathbb{F}_p}$.

One has that

$$I_{\mathfrak{p}} = \{\sigma \in D_{\mathfrak{p}} \colon x^{\sigma} \equiv x \bmod \mathfrak{p} \ \forall\, x \in \overline{\mathbb{Z}}\}$$

Again, it is easy to see that $I_{\mathfrak{p}} \cong \varprojlim_F I_{\mathfrak{p}_F}$, namely the absolute inertia over p is the inverse limit over the inertia groups of p in the finite Galois extensions $F/\mathbb{Q}$. The group $G_{\mathbb{F}_p}$ is *procyclic*, i.e. it's the inverse limit of the cyclic groups $\mathbb{Z}/n\mathbb{Z}$ as n runs over $\mathbb{N}$. So

$$G_{\mathbb{F}_p} \cong \widehat{\mathbb{Z}} \cong \prod_{p \in \mathscr{P}} \mathbb{Z}_p$$

where $\mathscr{P}$ is the set of all rational primes. One can embed

$$\iota \colon \mathbb{Z} \hookrightarrow \widehat{\mathbb{Z}}$$

$$x \mapsto \{x + n\mathbb{Z}\}_{n \in \mathbb{N}}$$

The subgroup of $\widehat{\mathbb{Z}}$ generated by $\iota(1) \coloneqq \sigma_p$ is a dense subgroup.

Definition 2.7. Any preimage of σ_p via the reduction map

$$D_{\mathfrak{p}} \to G_{\mathbb{F}_p}$$

is denoted by $\mathrm{Frob}_{\mathfrak{p}}$ and is called *absolute Frobenius element over* p.

Clearly $\mathrm{Frob}_{\mathfrak{p}}$ is determined only up to $I_{\mathfrak{p}}$. However, any two maximal ideals of $\overline{\mathbb{Z}}$ lying over the same rational prime p are conjugate by some $\sigma \in G_{\mathbb{Q}}$, as explained by the following

Proposition 2.8. Let $\mathfrak{p}, \mathfrak{q} \subseteq \overline{\mathbb{Z}}$ be two maximal ideals s.t. $\mathfrak{p} \cap \mathbb{Z} = \mathfrak{q} \cap \mathbb{Z} = p\mathbb{Z}$. Then there exists $\sigma \in G_{\mathbb{Q}}$ s.t. $\mathfrak{p}^\sigma = \mathfrak{q}$.

Proof. Recall that

$$\mathfrak{p} = \bigcup_K \mathfrak{p}_K \qquad \mathfrak{q} = \bigcup_K \mathfrak{q}_K$$

where K runs over all Galois number fields, $\mathfrak{p}_K = \mathfrak{p} \cap K$, $\mathfrak{q}_K = \mathfrak{q} \cap K$ and the unions are compatible. Since for every K the ideals $\mathfrak{p}_K$ and $\mathfrak{q}_K$ lie both over the same prime p, there exists $\sigma_K \in \mathrm{Gal}(K/\mathbb{Q})$ s.t. $\mathfrak{p}_K^{\sigma_K} = \mathfrak{q}_K$. Now fix any Galois number field K and choose such an automorphism $\sigma_K \in \mathrm{Gal}(K/\mathbb{Q})$. By remark 2.4, there exists $\sigma \in G_{\mathbb{Q}}$ s.t. $\sigma|_K = \sigma_K$. The fact that the unions of primes defining $\mathfrak{p}$ and $\mathfrak{q}$ are compatible implies clearly that $\mathfrak{p}^\sigma = \mathfrak{q}$. □

This fact shows that if $\mathfrak{p}, \mathfrak{q} \subseteq \overline{\mathbb{Z}}$ lie over $p \in \mathbb{Z}$, then their decomposition groups are isomorphic via the map

$$\vartheta \colon D_{\mathfrak{p}} \to D_{\mathfrak{q}}$$

$$\tau \mapsto \sigma\tau\sigma^{-1}$$

where $\sigma \in G_{\mathbb{Q}}$ is s.t. $\mathfrak{p}^\sigma = \mathfrak{q}$. Then it follows that the Frobenius of the conjugate is the conjugate of the Frobenius, namely

$$\mathrm{Frob}_{\mathfrak{p}^\sigma} = \sigma \, \mathrm{Frob}_{\mathfrak{p}} \, \sigma^{-1}$$

Let's now recall a very important result

Theorem 2.9 (Chebotarev density theorem)**.** Let $K \subseteq L$ be a Galois extension of number fields, with $G = \mathrm{Gal}(L/K)$. Let $C \subseteq G$ be a conjugacy class. Then the set

$$S = \{\mathfrak{p} \colon \mathfrak{p} \subseteq \mathcal{O}_K \text{ is an unramified prime ideal of } \mathcal{O}_K \text{ s.t. } \mathrm{Frob}_{\mathfrak{p}} \in C\}$$

has density $\#C/\#G$.

Remarks 2.10.

1) The density mentioned in the theorem is the *natural density*, namely if S is a set of primes of $\mathcal{O}_K$ we set

$$d(S) := \lim_{x \to +\infty} \frac{\#\{\mathfrak{p} \colon \#(\mathcal{O}_K/\mathfrak{p}) \leq x, \mathfrak{p} \in S\}}{\#\{\mathfrak{p} \colon \#(\mathcal{O}_K/\mathfrak{p}) \leq x, \mathfrak{p} \text{ prime}\}}$$

2) From the theorem it follows easily that every element $\sigma \in G$ is the Frobenius of an infinite number of primes of K. In fact, it is clear that every finite set of primes has density 0, so if C is the conjugacy class of σ, since $\#C \geq 1$ there must exist an infinite number of primes $\mathfrak{p}$ s.t. $\mathrm{Frob}_{\mathfrak{p}} \in C$. But if $\tau^{-1}\sigma\tau = \mathrm{Frob}_{\mathfrak{p}}$, then $\sigma = \mathrm{Frob}_{\mathfrak{p}^{\tau}}$ and we're done.

Theorem 2.11. Suppose $S := \{p_1, \dots, p_n\} \subseteq \mathbb{Z}$ is a set of primes. For any maximal ideal $\mathfrak{p} \subseteq \overline{\mathbb{Z}}$ not lying over any of the p_i's, choose an absolute Frobenius $\mathrm{Frob}_{\mathfrak{p}}$. Then the set of such elements is dense in $G_{\mathbb{Q}}$.

Proof. Pick any $\sigma \in G_{\mathbb{Q}}$ and $F \subseteq \overline{\mathbb{Q}}$ Galois number field. We will show that $U_{\sigma}(F)$ contains some $\mathrm{Frob}_{\mathfrak{p}}$ with $\mathfrak{p} \cap \mathbb{Z} \notin S$. Indeed, look at the surjective map

$$G_{\mathbb{Q}} \to \mathrm{Gal}(F/\mathbb{Q})$$

The image of σ via this map, call it σ_F, is by Chebotarev density theorem, a Frobenius of infinite primes of F. So we can choose on of those primes, say $\mathfrak{p}_F$, not lying over any of the p_i's, because the set of primes of F lying over some of the p_i's is clearly finite. For the same reason, we can assume that $p = \mathfrak{p}_F \cap \mathbb{Z}$ doesn't ramify in F, so that $I_{\mathfrak{p}_F}$ is trivial. Now lift $\mathfrak{p}_F$ to a maximal ideal $\mathfrak{p} \subseteq \overline{\mathbb{Z}}$ and consider the following commutative diagram

$$\begin{array}{ccc}
G_{\mathbb{F}_p} & \longrightarrow & \mathrm{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p) \\
\uparrow & & \uparrow \cong \\
D_{\mathfrak{p}} & \xrightarrow{\pi_F|_{D_{\mathfrak{p}}}} & D_{\mathfrak{p}_F} \\
\downarrow & & \downarrow \\
G_{\mathbb{Q}} & \xrightarrow{\pi_F} & \mathrm{Gal}(F/\mathbb{Q})
\end{array}$$

where we have identified $F/\mathfrak{p}_F$ and $\mathbb{F}_{p^f}$, where f is the inertia degree of p in F. By our choice $\sigma_F \in D_{\mathfrak{p}_F}$ is mapped to the Frobenius of $\mathrm{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p)$. Such an element can clearly be lifted a topological generator of $G_{\mathbb{F}_{\mathfrak{p}}}$, say σ_p. Again, σ_p can be lifted to $\mathrm{Frob}_{\mathfrak{p}} \in D_{\mathfrak{p}}$ (the one chosen by hypothesis). So by the commutativity of the upper square, it follows that $\pi_F|_{D_{\mathfrak{p}}}(\mathrm{Frob}_{\mathfrak{p}})$ and σ_F differ by an element of the inertia group of $\mathfrak{p}_F$, which is trivial. Therefore $\pi_F|_{D_{\mathfrak{p}}}(\mathrm{Frob}_{\mathfrak{p}}) = \sigma_F$, but we know that $\sigma_F = \pi_F|_{D_{\mathfrak{p}}}(\sigma)$, namely

$$\pi_F|_{D_{\mathfrak{p}}}(\mathrm{Frob}_{\mathfrak{p}}\, \sigma^{-1}) = 1$$

This means that $\mathrm{Frob}_{\mathfrak{p}}\, \sigma^{-1}$ lies in the kernel of $\pi_F|_{D_{\mathfrak{p}}}$, and since obviously $\ker \pi_F|_{D_{\mathfrak{p}}} \subseteq \ker \pi_F$, we have proven that $\mathrm{Frob}_{\mathfrak{p}} = \sigma\tau$ for some $\tau \in \ker \pi_F$, i.e. $\mathrm{Frob}_{\mathfrak{p}} \in U_{\sigma}(F)$. □

2.2 Galois representations

Definition 2.12. An n-dimensional *Galois representation* is a continuous homomorphism

$$\rho \colon G_{\mathbb{Q}} \to \mathrm{GL}_n(K)$$

where K is a topological field, and the topology on $\mathrm{GL}_n(K)$ is the one induced by the inclusion $\mathrm{GL}_n(K) \hookrightarrow K^{n^2}$.
Two representations ρ, ρ' are said to be *equivalent* if there exists $M \in \mathrm{GL}_n(K)$ s.t.

$$\rho'(\sigma) = M^{-1}\rho(\sigma)M$$

for all $\sigma \in G_{\mathbb{Q}}$.

When $K = \mathbb{C}$, we will speak of a *complex Galois representation*, when K is an extension of $\mathbb{Q}_p$, we will call ρ a *p-adic Galois representation.*
The identity matrix of order n will always be denoted by I_n.

Remark 2.13. Since K is chosen to be a topological field, $\mathrm{GL}_n(K)$ turns into a topological group. If

$$\rho\colon G \to H$$

is a homomorphism of topological groups, to check the continuity of ρ it's enough to check that $\rho^{-1}(V)$ is open in $G_{\mathbb{Q}}$ for every V in a basis of open neighborhoods of the identity 1_H. In fact, for every $h \in H$, we have a homeomorphism

$$\varphi_h\colon H \to H$$

$$\sigma \mapsto h\sigma$$

and therefore $\rho^{-1}(hV) = (\varphi_h \circ \rho)^{-1}(hV)$ is open in G since hV is open in H.

Definition 2.14. Let $c \in G_{\mathbb{Q}}$ be a complex conjugation. A Galois representation $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{C})$ is said to be *odd* if $\det(\rho(c)) = -1$ while is said to be *even* if $\det(\rho(c)) = 1$.

The fundamental property the distinguishes complex Galois representation is the one stated by the following theorem.

Theorem 2.15. Let $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{C})$ be a complex Galois representation. Then $\operatorname{Im}\rho$ is finite and therefore ρ factors through $\mathrm{Gal}(F/\mathbb{Q})$ for some Galois number field F.

Proof. To prove the claim, it suffices to show that there exists an open neighborhood of I_n in $\mathrm{GL}_n(\mathbb{C})$ which doesn't contain nontrivial subgroups of $\mathrm{GL}_n(\mathbb{C})$. Indeed, if this is true, call U such a neighborhood. Clearly one must have that $\rho(G_{\mathbb{Q}}) \cap U = I_n$. Therefore $\rho^{-1}(U) = \ker\rho$, but on the other hand the continuity of ρ implies that $\ker\rho$ is open. Now the compactness of $G_{\mathbb{Q}}$ ensure that every open normal subgroup has finite index, and the claim follows.
So recall that the topology we are considering on $\mathrm{GL}_2(\mathbb{C})$ is the one induced by the norm defined as $\|M\| = \sup_{v\in\mathbb{C}^n\colon \|v\|=1} \|Mv\|$ for every $M \in \mathrm{Mat}_n(\mathbb{C})$. Now let $U = \{M \in \mathrm{Mat}_n(\mathbb{C})\colon \|M - I_n\| < 1/2\}$. Note that we cane suppose that every element in U is in its Jordan canonical form, because for each $A \in \mathrm{Mat}_n(\mathbb{C})$ one has

$$\|A^{-1}MA - I_n\| = \|A^{-1}(M - I_n)A\| \leq \|A^{-1}\|\|M - I_n\|\|A\| \leq \|M - I_n\|$$

Now take some $M \in \mathrm{GL}_n(\mathbb{C})$ such that $M \neq I_n$ and $M \in U$. If M has all the eigenvalues equal to 1, then its Jordan canonical form has to have at least a nondiagonal entry. This implies that for $N \in \mathbb{N}$ big enough, $\|M^N - I_n\| > 1/2$, so that U cannot contain the subgroup generated by M. So assume that M has an eigenvalue $\alpha \neq 1$. If $|\alpha| \neq 1$ then it's clear that for some $N \in \mathbb{Z}$ one has $|\alpha^N - 1| > 1/2$ so that $\|M^N - I_n\| > 1/2$. If $|\alpha| = 1$, say that α is in the (i,i)-th diagonal entry of M. Then consider the projection $\pi\colon \mathbb{C}^{n^2} \to \mathbb{C}$ that sends a matrix A to its (i,i)-th entry, so that $\pi(M) = \alpha$. It's clear that $\pi(U) \subseteq V := \{z \in \mathbb{C}\colon |z-1| < 1/2\}$. Therefore the argument of α cannot be greater in absolute value than $\arctan 1/2$ and choosing an appropriate $N \in \mathbb{N}$ one has that the argument of α^N is greater than such a number, so that V, and hence U, cannot contain the group generated by α. □

Note that the proof of this theorem doesn't rely strongly on the structure of $G_{\mathbb{Q}}$, except for the fact that by its compactness, an open normal subgroup have finite index. In fact, the same theorem is true for a continuous representation of any profinite group and we will use it when we will speak about representations of G_p.
We can easily invert the theorem: given a representation $\rho\colon \operatorname{Gal}(F/\mathbb{Q}) \to \operatorname{GL}_n(\mathbb{C})$ for some number field F, we can always compose this homomorphism, which is obviously continuous because $\operatorname{Gal}(F/\mathbb{Q})$ has the discrete topology, with the projection onto the quotient $G_{\mathbb{Q}} \twoheadrightarrow G_{\mathbb{Q}}/\operatorname{Gal}(\overline{\mathbb{Q}}/F) \cong \operatorname{Gal}(F/\mathbb{Q})$, which is continuous too, and get a Galois representation $\rho\colon G_{\mathbb{Q}} \to \operatorname{GL}_n(\mathbb{C})$.
Now, once we have a Galois representation $\rho\colon G_{\mathbb{Q}} \to \operatorname{GL}_n(K)$, a natural question would be to understand $\rho(\operatorname{Frob}_{\mathfrak{p}})$ for some prime $\mathfrak{p} \subseteq \overline{\mathbb{Z}}$. The problem is that $\operatorname{Frob}_{\mathfrak{p}}$ is defined only up to $I_{\mathfrak{p}}$, so the notion of $\rho(\operatorname{Frob}_{\mathfrak{p}})$ makes sense if and only if $I_{\mathfrak{p}} \subseteq \ker\rho$. Moreover, if $p \in \mathbb{Z}$ is a prime and $\mathfrak{p}, \mathfrak{p}' \subseteq \overline{\mathbb{Z}}$ are two primes lying over p, then $I_{\mathfrak{p}}$ and $I_{\mathfrak{p}'}$ are conjugate in $G_{\mathbb{Q}}$ so that $I_{\mathfrak{p}} \subseteq \ker\rho$ if and only if $I_{\mathfrak{p}'} \subseteq \ker\rho$ by the normality of $\ker\rho$ in $G_{\mathbb{Q}}$. Therefore it makes sense to state the following

Definition 2.16. Let $p \in \mathbb{Z}$ be a prime, $\rho\colon G_{\mathbb{Q}} \to \operatorname{GL}_n(K)$ be a Galois representation. We say that ρ is *unramified* at p if $I_{\mathfrak{p}} \subseteq \ker\rho$ for some $\mathfrak{p} \subseteq \overline{\mathbb{Z}}$ lying over p.

Remarks 2.17.

1) If a Galois representation ρ is unramified at all primes except for a finite number, then the values $\rho(\operatorname{Frob}_{\mathfrak{p}})$, when they are defined, determine completely ρ. In fact, by theorem 2.11, such $\operatorname{Frob}_{\mathfrak{p}}$ are dense in $G_{\mathbb{Q}}$ and so if $\sigma \in G_{\mathbb{Q}}$ we can always find a sequence $\operatorname{Frob}_{\mathfrak{p}_i}$ that tends to σ (in the topology of $G_{\mathbb{Q}}$), and the continuity of ρ forces $\rho(\sigma)$ to be the limit of the $\rho(\operatorname{Frob}_{\mathfrak{p}_i})$.

2) Every complex Galois representation $\rho\colon G_{\mathbb{Q}} \to \operatorname{GL}_n(\mathbb{C})$ is unramified outside a finite set of primes. More precisely, let $F = \overline{\mathbb{Q}}^{\ker\rho}$ and $\rho'\colon \operatorname{Gal}(F/\mathbb{Q}) \to \operatorname{GL}_n(\mathbb{C})$ be the corresponding faithful representation. We claim that ρ is ramified at p iff p ramifies in F. In fact, suppose that ρ is unramified at p. This means that ρ is trivial on $I_{\mathfrak{p}}$ for any maximal ideal $\mathfrak{p} \subseteq \overline{\mathbb{Z}}$ lying over p. Since there exists a surjection $I_{\mathfrak{p}} \to I_{\mathfrak{p}_F}$ (see remark 2.4) where $\mathfrak{p}_F := \mathfrak{p} \cap F$, if $I_{\mathfrak{p}_F}$ were nontrivial then $\rho(\sigma) \neq I_n$ for some $\sigma \in I_{\mathfrak{p}_F}$ because the induced representation of $\operatorname{Gal}(F/\mathbb{Q})$ is faithful by construction and so we could lift σ to some $\sigma' \in G_{\mathbb{Q}}$ s.t. $\rho(\sigma') \neq I_n$, contradiction.
Conversely suppose that p does not ramify in F. If ρ were ramified at p, then there would exist $\sigma \in I_{\mathfrak{p}} \subseteq G_{\mathbb{Q}}$ such that $\rho(\sigma) \neq I_n$. But then we would have $\rho'(\sigma|_F) \neq I_n$ and this is impossible since $\sigma|_F \in I_{\mathfrak{p}_F}$ which is trivial.

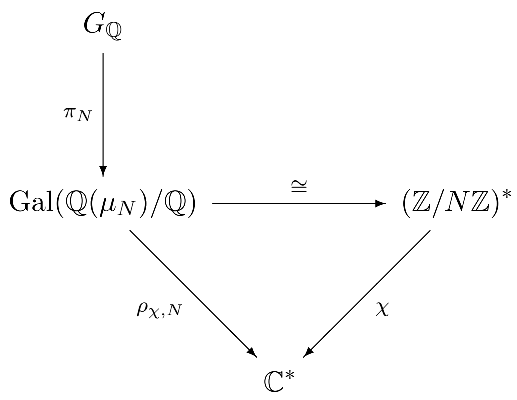
This fact shows also that a Galois representation is unramified everywhere if and only if it is trivial, because there always exists a ramified prime in F unless $F = \mathbb{Q}$.

3) It's also possible to define ramification at the infinite prime of $\mathbb{Q}$ of a Galois representation ρ. In fact, by convention one has that $D_\infty = \mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{1, c\} = I_\infty$ where c is a complex conjugation and so it makes sense to say that ρ is unramified at ∞ iff $\rho(c) \neq I_n$. For 1-dimensional representations, being ramified at ∞ means being odd, while being unramified means being even. When $n = 2$, an odd Galois representation is necessarily ramified at ∞, while an even one can be ramified or unramified at ∞.

Examples 2.18.

i) Of course one can always define the *trivial representation*, denoted by $\mathbb{1}$, mapping the whole $G_\mathbb{Q}$ to the identity. Such a representation is of course unramified everywhere.

ii) Let $K = \mathbb{C}$ and $n = 1$, so that $\mathrm{GL}_1(\mathbb{C}) = \mathbb{C}^*$. Let χ be a primitive Dirichlet character modulo $N \in \mathbb{N}$. Now consider the following diagram



where μ_N is a primitive N-th root of unity and $\rho_{\chi,N}$ is the unique map that makes the diagram commute. The composition

$$\rho_\chi \coloneqq \rho_{\chi,N} \circ \pi_N$$

yields a complex Galois representation. In fact, the image of ρ_χ is finite and so to check that the map is continuous it's enough, by remark 2.13, to check that $\rho_\chi^{-1}(1)$ is open. This is certainly true because $\ker \rho_{\chi,N} = \mathrm{Gal}(\mathbb{Q}(\mu_N)/F)$ for some Galois extension $\mathbb{Q} \subseteq F \subseteq \mathbb{Q}(\mu_N)$ and hence $\rho_\chi^{-1}(1) = \pi_N^{-1}(\ker \rho_{\chi,N}) = \mathrm{Gal}(F/\mathbb{Q}) = U(F)$ which we know to be an open subgroup of $G_\mathbb{Q}$.
Conversely, let $\rho\colon G_\mathbb{Q} \to \mathbb{C}^*$ be a continuous homomorphism with kernel $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$. By the Kronecker-Weber theorem, we can assume $F = \mathbb{Q}(\mu_N)$, so that we have the same commutative diagram as above, namely ρ is induced by some Dirichlet character modulo N. One can show that if ρ factors through $\mathbb{Q}(\mu_N)$ and $\mathbb{Q}(\mu_{N'})$, then it factors also through $\mathbb{Q}(\mu_d)$ where $d = (N, N')$. Therefore we can assume that χ is primitive. So we have a bijection between the set of 1-dimensional complex Galois representations and primitive Dirichlet characters modulo N. This correspondence can be

viewed as a consequence of global class field theory: each continuous character of $G_{\mathbb{Q}}$ can be composed with the global Artin map to obtain a character of the idéle class group of $\mathbb{Q}$, and viceversa.
Note that the complex conjugation c restricts to the automorphism $\mu_N \mapsto \mu_N^{-1}$ and this shows that $\chi(c) = -1$. More generally, an absolute Frobenius element $\mathrm{Frob}_{\mathfrak{p}}$ lying over a prime $p \nmid N$ maps to $p \bmod N$ and so $\chi(\mathrm{Frob}_{\mathfrak{p}}) = \chi(p)$.
By remark 2.17, this representation is ramified exactly at primes dividing N.

iii) Pick a prime l and consider the field $\mathbb{Q}(\mu_{l^\infty}) = \bigcup_{n\in\mathbb{N}} \mathbb{Q}(\mu_{l^n})$. Then it is easy to show that

$$G_{\mathbb{Q},l} := \mathrm{Gal}(\mathbb{Q}(\mu_{l^\infty})/\mathbb{Q}) \cong \mathbb{Z}_l^*$$

and since we have a surjection $G_{\mathbb{Q}} \to G_{\mathbb{Q},l}$, what we constructed is an l-adic representation

$$\chi_l \colon G_{\mathbb{Q}} \to \mathbb{Q}_l^*$$
$$\sigma \mapsto (m_1, m_2, \dots) \quad \text{where } \mu_{l^n}^{\sigma} = \mu_{l^n}^{m_n} \text{ for all } n$$

that is called *l-adic cyclotomic character of $G_{\mathbb{Q}}$*.

A phenomenon typical of l-adic Galois representation is the following, and we will need it at a certain point of our main proof.

Lemma 2.19. Let K be a finite extension of $\mathbb{Q}_l$ for some prime l, let $\rho \colon G_{\mathbb{Q}} \to \mathrm{GL}_n(K)$ be a Galois representation. Then ρ is equivalent to a Galois representation $\rho' \colon G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathcal{O}_K)$, where $\mathcal{O}_K$ is the valuation ring of K.

Proof. See [DJ05]. □

The definition of Galois representations we gave is good because it's very clear, but it doesn't allow us to construct many natural examples. For that purpose, we can restate the definition in the following equivalent way

Definition 2.20. Let K be a topological field, let $n \in \mathbb{N}$. An *n-dimensional Galois representation* is an $K[G_{\mathbb{Q}}]$-module which is n-dimensional as a K-vector space such that the action

$$G_{\mathbb{Q}} \times V \to V$$
$$(\sigma, v) \mapsto v^{\sigma}$$

is continuous.
Two representations V, V' are said to be *equivalent* if there exists a continuous $K[G_{\mathbb{Q}}]$-modules isomorphism $V \to V'$.

To see why this definition is equivalent to the previous one, first let $\rho \colon G_{\mathbb{Q}} \to \mathrm{GL}_n(K)$ be a Galois representation in the sense of 2.12. We can define a $G_{\mathbb{Q}}$-module structure on K^n by the map

$$G_{\mathbb{Q}} \times K^n \to K^n$$
$$(\sigma, v) \mapsto \rho(\sigma)v$$

This can be viewed as the composition of the maps

$$G_{\mathbb{Q}} \times K^n \to \mathrm{GL}_n(K) \times K^n$$

$$(\sigma, v) \mapsto (\rho(\sigma), v)$$

and

$$\mathrm{GL}_n(K) \times K^n \to K^n$$
$$(M, v) \mapsto Mv$$

The first map is continuous by hypothesis, and the second one is well-known to be continuous. Hence also their composition is continuous, and so we obtained a Galois representation in the sense of definition 2.20. Now suppose ρ, ρ' are two isomorphic Galois representations in the sense of definition 2.12. Then there exists $M \in \mathrm{GL}_n(K)$ s.t. $\rho(\sigma) = M^{-1}\rho'(\sigma)M$ for all $\sigma \in G_{\mathbb{Q}}$. We can define the map

$$\varphi\colon K^n \to K^n$$
$$v \mapsto Mv$$

which is clearly continuous. Moreover, for any $\sigma \in G_{\mathbb{Q}}$ one has

$$\varphi(v^\sigma) = \varphi(\rho(\sigma)v) = M(\rho(\sigma)v) = \rho(\sigma)'(Mv) = (Mv)^\sigma = \varphi(v)^\sigma$$

Viceversa, let V a n-dimensional K vector space which is endowed with a continuous action by $G_{\mathbb{Q}}$. Fix a basis $\mathcal{E} = \{e_1, \ldots, e_n\} \subseteq V$. Then every $\sigma \in G_{\mathbb{Q}}$ induces an automorphism of V, hence we have a map

$$\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_n(K)$$

that is an homomorphism since $G_{\mathbb{Q}}$ acts on V. To show that such a map is continuous, first recall that we are considering $\mathrm{GL}_n(K) \hookrightarrow K^{n^2}$ and the topology on $\mathrm{GL}_n(\mathbb{C})$ is the one induced by the inclusion. Now note that to give a continuous map $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{C})$ is equivalent to give a continuous map $\rho\colon G_{\mathbb{Q}} \to K^{n^2}$ such that $\rho(G_{\mathbb{Q}}) \subseteq \mathrm{GL}_n(\mathbb{C})$. By the universal property of the product, to give a continuous map $G_{\mathbb{Q}} \to K^{n^2}$ is equivalent to give n^2 continuous maps to the components of the product that make the obvious diagram commute. Clearly our n^2 maps must be, in order to make the diagram commute, the maps given by

$$\rho_{ij}\colon G_{\mathbb{Q}} \to K$$
$$\sigma \mapsto (\rho(\sigma))_{ij}$$

where $(\rho(\sigma))_{i,j}$ is the (i,j)-th entry of $\rho(\sigma)$. One sees immediately that

$$\rho_{ij}(\sigma) = \pi_j(\rho(\sigma)e_i)$$

where $\pi_j\colon K^n \to K$ is the projection to the j-th component, that is a continuous map. Since by hypothesis the action of $G_{\mathbb{Q}}$ on V is continuous, ρ_{ij} is continuous as composition of continuous maps.

Now let V' be a n-dimensional K vector spaces which is isomorphic to V as $G_{\mathbb{Q}}$-module. Fix a basis , $\mathcal{F} = \{f_1, \ldots, f_d\} \subseteq V'$ and write M for the matrix that represent the isomorphism of V and V' in the bases $\mathcal{E}, \mathcal{F}$. Then saying that multiplication by M induces an isomorphism that commute with the action means saying that for all $v \in V$ and $\sigma \in G_{\mathbb{Q}}$ one has

$$M(v^\sigma) = (Mv)^\sigma$$

namely that $M(\rho(\sigma)v) = \rho'(\sigma)(Mv)$ so that choosing $v = e_i$ for $i = 1, \ldots, d$ yields $\rho(\sigma) = M^{-1}\rho'(\sigma)M$ for all $\sigma \in G_{\mathbb{Q}}$.

Working with definition 2.20 gives us directly the following crucial example.

Example 2.21. Let E be an elliptic curve over $\mathbb{Q}$. For every prime $p \in \mathbb{Z}$ and $n \in \mathbb{N}$, we denote the subgroup of the p^n-torsion points over $\overline{\mathbb{Q}}$ by $E(\overline{\mathbb{Q}})[p^n]$. The group $G_{\mathbb{Q}}$ clearly acts on $E(\overline{\mathbb{Q}})[p^n]$; moreover, for all n there is a group homomorphism

$$E(\overline{\mathbb{Q}})[p^{n+1}] \to E(\overline{\mathbb{Q}})[p^n]$$

given by the multiplication by p which turns $\{E(\overline{\mathbb{Q}})[p^n]\}_{n\in\mathbb{N}}$ into a projective system. Since the action of $G_{\mathbb{Q}}$ is compatible with the transition maps, what we get is by the universal property of the inverse limit a (continuous) action of $G_{\mathbb{Q}}$ over $\varprojlim_{n\in\mathbb{N}} E(\overline{\mathbb{Q}})[p^n] := T_p(E)$, which is called the *p-adic Tate module of E*. Since $E(\overline{\mathbb{Q}})[p^n] \cong (\mathbb{Z}/p^n\mathbb{Z})^2$, we have that $T_p(E) \cong \mathbb{Z}_p^2$ and so we ended up with a 2-dimensional p-adic Galois representation associated to E.

An advantage of working with $K[G_{\mathbb{Q}}]$-modules instead of homomoprhism $G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{C})$ is that the category $G_{\mathbb{Q}}$**-mod** in which the objects are discrete abelian groups on which $G_{\mathbb{Q}}$ acts continuously, is an abelian category. Two basic construction can be made out of Galois representations, as described below.

Definition 2.22. Let $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_n(K)$, $\rho'\colon G_{\mathbb{Q}} \to \mathrm{GL}_m(K)$ be two Galois representations.
The *direct sum* of ρ and ρ' is the representations given by

$$\rho \oplus \rho'\colon G_{\mathbb{Q}} \to \mathrm{GL}_{n+m}(K)$$

$$\sigma \mapsto \begin{pmatrix} \rho(\sigma) & 0 \\ 0 & \rho'(\sigma) \end{pmatrix}$$

The *tensor product* of ρ and ρ' is the representation given by

$$\rho \otimes \rho'\colon G_{\mathbb{Q}} \to \mathrm{Aut}(K^n \otimes K^m)$$

$$\sigma \mapsto \rho(\sigma) \otimes \rho'(\sigma)$$

Definition 2.23. Suppose that V is an n-dimensional Galois representation. We say that V is *irreducible* if the only stable subspaces[1] of V are $0, V$.
A Galois representation $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_n(K)$ is said to be *semisiple* if it is isomorphic to a direct sum of irreducible Galois representation.

Since $G_{\mathbb{Q}}$ is not finite, it is not always true that Galois representations are semisimple. However, we will be interested in complex Galois representations and as we know from theorem 2.15 such representations have finite image, and so they can be thought as faithful representations of the finite group $\mathrm{Gal}(F/\mathbb{Q})$ for some Galois number field F. Therefore, complex Galois representations are automatically semisimple.
We are then ready to state the following fundamental

Theorem 2.24. Let $\rho, \rho'\colon G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{C})$ be two Galois representations s.t. $\mathrm{Tr}(\rho(\mathrm{Frob}_p)) = \mathrm{Tr}(\rho'(\mathrm{Frob}_p))$ for all primes $p \in \mathbb{Z}$ outside of a finite set S. Then ρ and ρ' are isomorphic.

[1]See appendix for the definition of stability.

Proof. By theorem 2.15, ρ, ρ' give rise to faithful representations of $\mathrm{Gal}(K/\mathbb{Q})$ and $\mathrm{Gal}(F/\mathbb{Q})$ respectively, where $K = \overline{\mathbb{Q}}^{\ker \rho}$ and $F = \overline{\mathbb{Q}}^{\ker \rho'}$. Since K, F are Galois number fields, so is FK and then we have surjections $\mathrm{Gal}(FK/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q})$, $\mathrm{Gal}(FK/\mathbb{Q}) \to \mathrm{Gal}(F, \mathbb{Q})$. Therefore we can assume that both ρ, ρ' factor through $\mathrm{Gal}(KF/\mathbb{Q}) \coloneqq G$. Now by Chebotarev density theorem, each $\sigma \in G$ is the Frobenius of infinite primes $p \in \mathbb{Q}$, so as in the proof of theorem 2.11 we can lift σ to the absolute Frobenius of a prime which doesn't lie in S. In this way, by hypothesis we know that $\mathrm{Tr}(\rho(\sigma)) = \mathrm{Tr}(\rho'(\sigma))$ for every $\sigma \in G$ and so by corollary A.13 it follows that ρ, ρ' are isomorphic as representations of G and so also as Galois representations. $\square$

2.3 Ramification and the Artin conductor

One natural question one could ask is "how much" a Galois representation is ramified. To understand what we mean by this, we shall start introducing the higher ramification groups, as done in [Ser79]. Throughout the rest of the section, K will be a field complete under a discrete valuation v_K (e.g. a finite extension of $\mathbb{Q}_p$), A_K will be its valuation ring with maximal ideal $\mathfrak{p}_K$, U_K the group of units of A_K and k the residue field. Moreover, L will be a finite separable extension of K, A_L will be its valuation ring with maximal ideal $\mathfrak{p}_L$, U_L the group of units and k_L the residue field. Finally, we assume k_L/k to be separable. Recall that we have the following

Proposition 2.25. Under the above hypothesis, there exists $x \in A_L$ s.t. $A_L = A_K[x]$.

Proof. See [Ser79]. $\square$

Now we add the hypothesis that L/K is Galois and we set $G \coloneqq \mathrm{Gal}(L/K)$. Moreover, we set $g = |G|$, so that $ef = g$ where f is the inertia degree and e the ramification index of L/K.

Lemma 2.26. Let $\sigma \in G$ and $i \geq -1$ be an integer. Then the following are equivalent:

a) σ acts trivially on $A_L/\mathfrak{p}_L^{i+1}$;

b) $v_L(a^\sigma - a) \geq i + 1$ for all $a \in A_L$;

c) $v_L(x^\sigma - x) \geq i + 1$, where $x \in A_L$ is s.t. $A_K[x] = A_L$.

Proof.
a)$\Longleftrightarrow$ b) If σ acts trivially on $A_L/\mathfrak{p}_L^{i+1}$, then a^σ and a lie in the same coset of A_L, therefore they differ by an element of $\mathfrak{p}_L^{i+1}$, and such an element has valuation $\geq i+1$. Conversely, if $v_L(a^\sigma - a) \geq i+1$, then there exists $b \in \mathfrak{p}_L^{i+1}$ s.t. $a^\sigma - a = b$ and therefore $a^\sigma \equiv a \bmod \mathfrak{p}_L^{i+1}$.
a)$\Longleftrightarrow$ c) If $x \in A_L$ generates A_L as an A_k-algebra, then $x_i \coloneqq x \bmod \mathfrak{p}_L^{i+1}$ generates $A_L/\mathfrak{p}_L^{i+1}$ as an A_k-algebra. Therefore $x_i^\sigma \equiv x_i \bmod \mathfrak{p}_L^{i+1}$ is a sufficient and necessary condition for σ to act trivially on $A_L/\mathfrak{p}_L^{i+1}$, by the same argument of point a). $\square$

Definition 2.27. For each integer $i \geq -1$, the *i-th ramification group* is defined as

$$G_i := \{\sigma \in G\colon \text{ satisfy a), b) or c) of the previous lemma}\}$$

It's clear that $G_{-1} = G$ and $G_0 \subseteq G$ is the usual inertia subgroup. Also, note that one can define

$$G_i := \ker(G \to \mathrm{Aut}(A_L/\mathfrak{p}_L^{i+1}))$$

for the obvious map $G \to \mathrm{Aut}(A_L/\mathfrak{p}_L^{i+1})$. This automatically shows that the G_i's are normal in G.

Proposition 2.28. The ramification groups form a descending chain of normal subgroups of G such that G_i is trivial for i big enough.

Proof. The only thing to prove is that the G_i's become eventually trivial. But looking at condition c) of lemma 2.26 it is clear that whenever $i \geq \sup_{\sigma \in G}\{v_L(x^\sigma - x)\}$ then G_i is trivial, and so we are done. □

Still denoting by x an A_K-generator of A_L, let's define the following function on G

$$i_G\colon G \to \mathbb{Z} \cup \{+\infty\}$$
$$\sigma \mapsto i_G(\sigma) := v_L(x^\sigma - x)$$

Clearly, if $\sigma \neq 1_G$ then $i_G(\sigma)$ is a nonnegative integer, while $i_G(1_G) = +\infty$. Moreover, the function i_G has the following properties:

i)
$$i_G(\sigma) \geq i + 1 \iff \sigma \in G_i$$

ii)
$$i_G(\tau^{-1}\sigma\tau) = i_G(\sigma)$$

iii)
$$i_G(\sigma\tau) \geq \inf\{i_G(\sigma), i_G(\tau)\}$$

Now suppose that H is a subgroup of G, and let $K' = L^H$ be the corresponding subextension of L/K.

Proposition 2.29. For every $\sigma \in H$, $i_H(\sigma) = i_G(\sigma)$ and $H_i = G_i \cap H$.

Proof. The fact that $i_H(\sigma) = i_G(\sigma)$ is clear. To see the second assertion, recall point a) of proposition 2.26: $\sigma \in H_i$ iff $\sigma \in H$ and σ acts trivially on $A_L/\mathfrak{p}_L^{i+1}$. The claim then follows. □

Corollary 2.30. If K^{ur} is the largest unramified extension of K inside L and $H = \mathrm{Gal}(L/K^{ur})$, then $H_i = G_i$ for all i.

Proof. The claim follows directly from the previous proposition and the fact that $H = G_0$. □

This last corollary reduces the study of ramification groups to the totally ramified case.
Our aim now is to introduce the Artin conductor of a Galois representation, that in some sense will measure its ramification. To do that, first we need to describe the *Artin representation* of G. This is done as follows: for $\sigma \in G$ define

$$a_G(\sigma) = \begin{cases} -f i_G(\sigma) & \text{if } \sigma \neq 1_G \\ f \sum_{\tau \neq 1_G} i_G(\tau) & \text{if } \sigma = 1_G \end{cases}$$

This implies that $\sum_{\sigma \in G} a_G(\sigma) = 0$, i.e. $(a_G, \mathbb{1}_G) = 0$[2]. One can prove that a_G is the character of a representation of G. We won't reproduce the proof here; we just say that it relies strongly on the following fundamental

Theorem 2.31 (Brauer-Tate)**.** Every character of a finite group G is a linear combination with integer coefficients of characters induced from characters of its elementary subgroups.[3]

Proof. See [Ser77a]. □

Definition 2.32. The representation of G whose character is a_G is called *Artin representation* of G.

The fact that a_G is a class function is clear. Write $a_G = \sum_{i=1}^{h} c_i \chi_i$ where $\chi_1, \ldots, \chi_h$ are the irreducible characters of G and $c_i \in \mathbb{C}$ for all i. Then we have

$$c_i = (a_G, \chi_i) = \frac{1}{g} \sum_{\sigma \in G} a_G(\sigma) \chi_i(\sigma)^{-1} = \frac{1}{g} \sum_{\sigma \in G} a_G(\sigma^{-1}) \chi_i(\sigma)$$

and as $a_G(\sigma) = a_G(\sigma^{-1})$ we have $c_i = (\chi_i, a_G)$. So for each class function φ on G define

$$f(\varphi) := (\varphi, a_G)$$

Such number is called *conductor* of φ. The fact that a_G is the character of a representation of G implies the fundamental

Theorem 2.33. $f(\chi)$ is a nonnegative integer for all characters χ.

Now recall that if $H \leq G$ and ψ is a class function on H then for all $\sigma \in G$ we have

$$\mathrm{Ind}(\psi)(\sigma) = \sum_{\tau \in G/H} \psi(\tau^{-1}\sigma\tau)$$

where by convention $\psi(\tau^{-1}\sigma\tau) = 0$ if $\tau^{-1}\sigma\tau \notin H$.

Proposition 2.34. The function a_G on G is equal to the function $\mathrm{Ind}(a_{G_0})$ induced by the corresponding function on the inertia subgroup.

[2]See the appendix for the inner product of class functions.

[3]A group G is said to be *p-elementary* for a prime number p if it is the direct product of a cyclic group of order prime to p and a p-group. G is said to be *elementary* if it is elementary for at least a prime p.

Proof. Since $G_0 \trianglelefteq G$, clearly $\mathrm{Ind}(a_{G_0})(\sigma) = 0 = a_G(\sigma)$ if $\sigma \notin G_0$. If $1 \neq \sigma \in G_0$, then

$$\mathrm{Ind}(a_{G_0})(\sigma) = \sum_{\tau \in G/G_0} a_G(\tau^{-1}\sigma\tau) = -\sum_{\tau \in G/G_0} i_{G_0}(\tau^{-1}\sigma\tau) = -f i_G(\sigma) = a_G(\sigma)$$

□

Proposition 2.35. Let G_i be the i-th ramification group of G, u_i the character of the augmentation representation of G_i and u_i^* the induced character of G. Then

$$a_G = \sum_{i=0}^{+\infty} \frac{1}{(G_0 \colon G_i)} u_i^*$$

Proof. Let $g_i := |G_i|$. Since $G_i \trianglelefteq G$, if R is a system of representatives of G_i in G and $\tau \in R$, one has that $\tau^{-1}\sigma\tau \in G_i$ iff $\sigma \in G_i$. This easily tells us that $u_i^*(\sigma) = 0$ for $\sigma \notin G_i$, while for $1 \neq \sigma \in G_i$ we have

$$u_i^*(\sigma) = \sum_{\tau \in R} u_i(\tau^{-1}\sigma\tau) = -\sum_{\tau \in R} 1 = -g/g_i = -f g_0/g_i$$

If $\sigma = 1_G$, then $u_i(1_G) = g_i - 1$ and so $u_i^*(1_G) = g/g_i(g_i - 1)$. This also tells us that $\sum_{\sigma \in G} u_i^*(\sigma) = 0$, i.e. the RHS is orthogonal with $\mathbb{1}_G$. Now, for every $\sigma \in G$ we can find $k \in \mathbb{N}$ s.t. $\sigma \in G_k \setminus G_{k+1}$. For such σ, it's clear that $a_G(\sigma) = -f(k+1)$ because $i_G(\sigma) = v_L(x^\sigma - x)$ and the latter is an integer $\geq k+1$ but not $\geq k+2$, namely it is exactly $k+1$. On the other hand,

$$\sum_{i=0}^{+\infty} \frac{1}{(G_0 \colon G_i)} u_i^*(\sigma) = -f g_0 \sum_{i=0}^{k} \frac{1}{(G_0 \colon G_i) g_i} = -f \sum_{i=0}^{k} 1 = -f(k+1)$$

For $\sigma = 1$ the claim follows from the orthogonality of both LHS and RHS with $\mathbb{1}_G$. □

Now for any class function φ on G we set

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

Corollary 2.36. If φ is a class function on G, then

$$f(\varphi) = \sum_{i=0}^{+\infty} \frac{g_i}{g_0} (\varphi(1) - \varphi(G_i))$$

Proof. Recall that $f(\varphi) = (\varphi, a_G)$. Now use proposition 2.35 and Frobenius reciprocity, namely the fact that

$$(\varphi, u_i^*) = (\varphi|_{G_i}, u_i) = \frac{1}{g_i} \sum_{\sigma \in G_i} \varphi(\sigma)\overline{u_i(\sigma)} = \varphi(1) - \varphi(G_i)$$

□

Corollary 2.37. If χ is the character of a representation of G in V then

$$f(\chi) = \sum_{i=0}^{+\infty} \frac{g_i}{g_0} \operatorname{codim} V^{G_i}$$

Proof. This follows from the fact that $\chi(G_i) = \dim V^{G_i}$. □

Corollary 2.38. $f(\chi)$ is a nonnegative rational number.

Proof. Since by proposition 2.35 $g_0 a_G$ is the character of a representation of G, the claim follows. □

Theorem 2.39. Let $H \leq G$ be a subgroup corresponding to the subextension K'/K, and let $d_{K'/K}$ be its the discriminant. Then

$$a_G|_H = \lambda r_H + f_{K'/K} \cdot a_H$$

where $\lambda = v_K(d_{K'/K})$.

Proof. See [Ser79]. □

Corollary 2.40. With the same notations of the theorem above, let ψ be a character of H and let ψ^* be the induced character on G. Then

$$f(\psi^*) = v_K(d_{K'/K})\psi(1) + f_{K'/K} f(\psi)$$

Proof. We have

$$f(\psi^*) = (\psi^*, a_G) = (\psi, a_G|_H)$$

by Frobenius reciprocity. By the previous theorem,

$$(\psi, a_G|_H) = \lambda(\psi, r_H) + f_{K'/K}(\psi, a_H) = \lambda\psi(1) + f_{K'/K} f(\psi)$$

□

To define the Artin conductor of a Galois representation, we proceed in the following way. Let $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{C})$ be a complex Galois representation, let $F := \overline{\mathbb{Q}}^{\ker\rho}$. We will continue to call ρ the corresponding faithful representation of $G = \mathrm{Gal}(F/\mathbb{Q})$ and χ its character. Now let $p \in \mathbb{Z}$ be a prime. For every prime $\mathfrak{p} \subseteq F$ lying over p, $F_{\mathfrak{p}}/\mathbb{Q}_p$ is a Galois extension of local fields whose Galois group is isomorphic to the decomposition group of $\mathfrak{p}$ over p. Therefore for each of such primes we can define a corresponding function $a_{\mathfrak{p}} := a_{\mathrm{Gal}(F_{\mathfrak{p}}/\mathbb{Q}_p)}$. Now extend this function to all G by setting $a_{\mathfrak{p}}(\sigma) = 0$ for all $\sigma \notin D_{\mathfrak{p}}$. Then define

$$a_p := \sum_{\mathfrak{p}|p} a_{\mathfrak{p}}$$

One checks that $a_p = \mathrm{Ind}(a_{\mathfrak{p}})$ for any choice of a prime $\mathfrak{p}$ lying over p. Therefore a_p is the character of a representation of G.

Definition 2.41. The representation whose character is a_p is called *Artin representation* of G attached to p.
For every rational prime p, set $f(\chi, p) := (\chi, a_p) = f(\chi|_{D_{\mathfrak{p}}})$ where the equality comes from Frobenius reciprocity. The (integral) ideal

$$f(\chi) = \prod_p p^{f(\chi,p)}$$

is called *Artin conductor* of ρ.

If p is unramified in F then $f(\chi, p) = 0$ (this follows easily by the definition of a_p). Conversely, if p ramifies in F then the definition of $f(\chi|_{D_\mathfrak{p}})$ implies that such an integer is ≥ 1. This fact, with remark 2.17, explains in which sense does the conductor "measure" the ramification of ρ.

Theorem 2.42. Let $H \leq G$ be a subgroup corresponding to the subextension K'/K.

i) If χ' is the character of another representation ρ' of G, then

$$f(\chi + \chi') = f(\chi) f(\chi')$$

ii) For every character ψ of H we have

$$f(\psi^*, L/K) = d_{K'/K}^{\psi(1)} \cdot N_{K'/K}(f(\psi, L/K'))$$

iii) If K'/K is Galois and ψ is a character of G/H we have

$$f(\psi, L/K) = f(\psi, K'/K)$$

Proof.
The proof immediate: i) follows from the linearity of the inner product of characters, ii) can be deduced easily by corollary 2.40 and iii) is just Frobenius reciprocity.

□

Now, if we apply ii) to the case $H = \{1\}$ we find that $\psi^* = r_G$, the character of the regular representation of G. So since obviously $f(\psi, L/L) = 1$ applying ii) of the previous theorem we get

$$f(r_G, L/K) = d_{L/K}$$

If we decompose r_G as $r_G = \sum_\chi \chi(1)\chi$ where χ runs over all irreducible characters of G, we find the "Fuhrerdiskriminantenproduktformel" of Artin and Hasse:

$$d_{L/K} = \prod_\chi f(\chi)^{\chi(1)}$$

which in particular tells us that the Artin conductor of any representation of G divides the discriminant of L/K.
To end the section, we define an "absolute" version of the ramification groups.

Definition 2.43. Let p be a finite prime of $\mathbb{Q}$ and $u \in \mathbb{R}$ s.t. $u \geq -1$. The *ramification groups* are given by

$$G_{p,u} = \mathrm{Gal}_u(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) := \{\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \colon v_p(x^\sigma - x) \geq u + 1 \ \forall x \in \overline{\mathbb{Z}}_p\}$$

It's clear that $G_{p,-1} = G_p$ while $G_{p,0}$ is the absolute inertia group over p.

Definition 2.44. The group $G_{p,1}$ is called *wild inertia group*. Let ρ be Galois representation ramified at p. If ρ is trivial on $G_{p,1}$ we say that it's *tamely ramified*, otherwise we say that it's *wildly ramified*. The group $G_{p,0}/G_{p,1}$ is called *tame inertia group*.

In terms of subextensions we have that $G_{p,0}$ is the Galois group of $\overline{\mathbb{Q}}_p/\mathbb{Q}_p^{ur}$, where $\mathbb{Q}_p^{ur}$ is the maximal unramified extension of $\mathbb{Q}_p$, while $G_{p,1}$ is the Galois group of $\overline{\mathbb{Q}}_p/\mathbb{Q}_p^t$ where $\mathbb{Q}_p^t$ is the maximal tamely ramified extension of $\mathbb{Q}_p$. It follows that $G_{p,0}/G_{p,1}$ is the Galois group of the extension $\mathbb{Q}_p^t/\mathbb{Q}_p^{ur}$. The wild inertia group is the pro-p Sylow subgroup of $G_{p,0}$ and there is an isomorphism

$$G_{p,0}/G_{p,1} \cong \prod_{l \neq p} \mathbb{Z}_l$$

Again one can see that $G_{p,i} = \varprojlim_K G_{p,i}^K$ where K runs over all finite extensions of $\mathbb{Q}_p$ and $G_{p,i}^K$ is the i-th ramification groups of the extension $K/\mathbb{Q}_p$. By remark 2.4, there are surjective maps $G_{p,i} \to G_{p,i}^K$ for each i, K. Now let $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{C})$ be a Galois representation with $K = \overline{\mathbb{Q}}^{\ker \rho}$. Fix a prime $p \in \mathbb{Z}$ and a prime $\mathfrak{p} \subseteq \mathcal{O}_K$ lying above p. One can show that the ramification group $G_{p,1}^K$ is the p-Sylow subgroup of $\mathrm{Gal}(K/\mathbb{Q}_p)$. Therefore we have that ρ is tamely ramified at p if and only if $(|\rho(I_p)|, p) = 1$.

Chapter 3

Correspondence between modular forms and Galois representations

We will construct a bijection between the set of normalized eigenforms in $M_k(N,\chi)$ and a certain class of Galois representations. This is done by looking at the Artin L-function associated to such representations. In fact we will see that there is a deep symmetry between those L-function and the ones associated to eigenforms. This symmetry is exactly what allows us to pass from modular forms to Galois representation and viceversa.

3.1 Artin L-functions

We start briefly recalling some basic facts about Dirichlet series and Euler product.
A *Dirichlet series* is a series of the form $\sum_{n\in\mathbb{N}} \frac{f(n)}{n^s}$, where $f\colon \mathbb{N} \to \mathbb{C}$ is any function and s is a complex variable.

Proposition 3.1. Let $g(s) = \sum_{n\in\mathbb{N}} \frac{f(n)}{n^s}$ be a Dirichlet series that doesn't diverge for all $s \in \mathbb{C}$ nor converge for all $s \in \mathbb{C}$. Then there exists two real numbers σ_c and σ_a, called respectively *abcissa of convergence* and *abcissa of absolute convergence* s.t.

i) $g(s)$ converges for all $s \in \mathbb{C}$ with $\Re(s) > \sigma_c$;

ii) $g(s)$ converges absolutely for all $s \in \mathbb{C}$ with $\Re(s) > \sigma_a$;

iii) $\sigma_c \leq \sigma_a$.

Proof. See [Apo76]. □

Proposition 3.2. Let $g(s) = \sum_{n\in\mathbb{N}} \frac{f(n)}{n^s}$ be a Dirichlet series s.t. $f(n)$ is a multiplicative function. Suppose $g(s)$ converges absolutely for $\Re(s) > \sigma_a$. Then we can write

$$g(s) = \prod_p \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \dots\right) \quad \text{for } \Re(s) > \sigma_a$$

Moreover, if $f(n)$ is completely multiplicative we get

$$g(s) = \prod_p \left(\frac{1}{1 - f(p)p^{-s}}\right)$$

where p runs over all natural primes. Such products are called *Euler products.*

Now, theorem 1.47, tells us that we can associate to any $f(\tau) = \sum_{n=1}^{+\infty} a_n q^n \in M_k(N, \chi)$ which is a normalized eigenform a Dirichlet series

$$L(s, f) = \sum_{n=1}^{+\infty} \frac{a_n}{n^s}$$

that admits an Euler product at least in its region of absolute convergence. More precisely,

Theorem 3.3. Let $f(q) = \sum_{n=1}^{+\infty} a_n q^n \in M_k(N, \chi)$. Then:

i) If f is a cusp form, then $L(s, f)$ converges absolutely in the half plane $\Re(s) > k/2 + 1$. If f is not a cusp form, then $L(s, f)$ converges absolutely in the half plane $\Re(s) > k$.

ii) The following conditions are equivalent:

a) f is a normalized eigenform;

b) $L(s, f)$ admits the following Euler product

$$L(s, f) = \prod_p \left(\frac{1}{1 - a_p p^{-s} + \chi(p)p^{k-1-2s}}\right) =$$

$$= \prod_{p \mid N} \left(\frac{1}{1 - a_p p^{-s}}\right) \prod_{p \nmid N} \left(\frac{1}{1 - a_p p^{-s} + \chi(p)p^{k-1-2s}}\right)$$

iii) If $p \mid N$, then

$$|a_p| = \begin{cases} 0 & \text{if } p^2 \mid N \text{ and } \chi \text{ can be defined mod } N/p \\ p^{(k-1)/2} & \text{if } \chi \text{ cannot be defined mod } N/p \\ p^{k/2-1} & \text{if } p^2 \nmid N \text{ and } \chi \text{ can be defined mod } N/p \end{cases}$$

iv) Set $\Lambda(s, f) := N^{s/2}(2\pi)^{-s}\Gamma(s)L(s, f)$. Such a function admits a meromorphic continuation to the whole complex plane. Its only possible poles are at $s = 0, k$. Moreover, the following functional equation holds:

$$\Lambda(k - s, f) = ci^k \Lambda(s, \overline{f})$$

where $c \in \mathbb{C}$ is a constant.

Proof. See [Li75]. □

Now let $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{C})$ be a Galois representation. Our aim is to define an L-function attached to ρ as a product of "local" factors corresponding to primes (finite and infinite) of $\mathbb{Q}$.[1] Recall that we can think of ρ as giving a $\mathbb{C}[G_{\mathbb{Q}}]$-module structure to a vector space $V \cong \mathbb{C}^n$. For a prime $p \in \mathbb{Z}$, set

$$L_p(s,\rho) \coloneqq \det(I_n - p^{-s}\rho(\mathrm{Frob}_{\mathfrak{p}})|_{V^{I_{\mathfrak{p}}}})^{-1}$$

The terms involved have the following meanings:

- $\mathfrak{p} \subseteq \overline{\mathbb{Z}}$ is any maximal ideal lying over p;
- $D_{\mathfrak{p}}$ is the absolute decomposition group of the ideal $\mathfrak{p}$ and $I_{\mathfrak{p}}$ is the inertia group. $\mathrm{Frob}_{\mathfrak{p}}$ is any Frobenius element in $D_{\mathfrak{p}}$. If ρ is unramified at p, the action of $I_{\mathfrak{p}}$ on $\mathbb{C}^n$ is trivial. Therefore $\rho(\mathrm{Frob}_{\mathfrak{p}})$ is well defined and $\rho(\mathrm{Frob}_{\mathfrak{p}})|_{V^{I_{\mathfrak{p}}}}$ is just $\rho(\mathrm{Frob}_{\mathfrak{p}})$. Moreover, if we choose another $\mathfrak{p}'$ lying over p, then the Frobenius changes by conjugacy. So if $\sigma \in G_{\mathbb{Q}}$ is s.t. $\mathfrak{p}^{\sigma} = \mathfrak{p}'$, then $\mathrm{Frob}_{\mathfrak{p}'} = \sigma^{-1}\,\mathrm{Frob}_{\mathfrak{p}}\,\sigma$, so that

$$\rho(\mathrm{Frob}_{\mathfrak{p}'}) = \rho(\sigma)^{-1}\rho(\mathrm{Frob}_{\mathfrak{p}})\rho(\sigma)$$

and then clearly

$$\det(I_n - p^{-s}\rho(\mathrm{Frob}_{\mathfrak{p}})) = \det(I_n - p^{-s}\rho(\mathrm{Frob}_{\mathfrak{p}'}))$$

So the choice of $\mathfrak{p}$ and $\mathrm{Frob}_{\mathfrak{p}}$ does not matter for unramified primes. When ρ is ramified in p, by definition the action of $I_{\mathfrak{p}}$ is not trivial on $\mathbb{C}^n$. Therefore we have a pointwise fixed subspace

$$V^{I_{\mathfrak{p}}} = \{v \in \mathbb{C}^n \colon \rho(\sigma)v = v \ \forall\ \sigma \in I_{\mathfrak{p}}\}$$

If we choose any $\mathrm{Frob}_{\mathfrak{p}} \in D_{\mathfrak{p}}$, such an element is defined just up to some element in the inertia, but its action on $V^{I_{\mathfrak{p}}}$ is well-defined. Therefore it makes sense to consider the restriction of $\rho(\mathrm{Frob}_{\mathfrak{p}})$ to $V^{I_{\mathfrak{p}}}$. Now if we choose another $\mathfrak{p}'$ lying over p we have that $I_{\mathfrak{p}'} = \tau^{-1}I_{\mathfrak{p}}\tau$ for some $\tau \in G_{\mathbb{Q}}$. We claim that the effect on the (pointwise) fixed subspace is that

$$V^{I_{\mathfrak{p}'}} = \rho(\tau^{-1})V^{I_{\mathfrak{p}}}$$

In fact, if $\rho(\tau^{-1})v \in \rho(\tau^{-1})V^{I_{\mathfrak{p}}}$, then for all $\tau^{-1}\sigma\tau \in I_{\mathfrak{p}'}$ we have

$$(\rho(\tau^{-1})\rho(\sigma)\rho(\tau))(\rho(\tau^{-1})v) = \rho(\tau^{-1})v$$

an we have the $\supseteq$ inclusion. Conversely, if $v \in V^{I_{\mathfrak{p}'}}$ then by definition $\rho(\tau^{-1}\sigma\tau)v = v$, which means that $\rho(\sigma)\rho(\tau)v = \rho(\tau)v$, namely that $\rho(\tau)v \in V^{I_{\mathfrak{p}}}$ and we're done.
This tells us that $V^{I_{\mathfrak{p}}}$ and $V^{I_{\mathfrak{p}'}}$ have the same dimension and of course the matrices $\rho(\mathrm{Frob}_{\mathfrak{p}})|_{V^{I_{\mathfrak{p}}}}$ and $\rho(\mathrm{Frob}_{\mathfrak{p}'})|_{V^{I_{\mathfrak{p}'}}}$ have the same eigenvalues, so that our definition is again well-posed.

[1] We underline the distinction between finite and infinite primes because even if $\mathbb{Q}$ has only one infinite prime, this construction of the Artin L-function can be generalized in a pretty obvious way for any continuous representation $\rho\colon \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathrm{GL}_n(\mathbb{C})$ where K is a number field, so that in some case we shall be dealing with different infinite primes, the ones of K.

Definition 3.4. The *Artin L-function* of a Galois representation $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{C})$ is defined as

$$L(s,\rho) = \prod_p L_p(s,\rho)$$

where p runs over all finite primes of $\mathbb{Q}$.

Remarks 3.5.

1) The Euler product defining $L(s,\rho)$ converges for $\Re(s) > 1$. This is because $L(s,\rho)$ is bounded (in absolute value) up to a finite number of (holomorphic) factors by $\zeta(s)^n$.

2) There is a more explicit description of $L(s,\rho)$ using the logarithm. In fact, call $\lambda_1(p),\ldots,\lambda_n(p)$ the eigenvalues of $\rho(\mathrm{Frob}_{\mathfrak{p}})$ and notice that

$$\det(I_n - p^{-s}\rho(\mathrm{Frob}_{\mathfrak{p}})) = \prod_{1=1}^{n}(1-\lambda_i(p)p^{-s})$$

Thus,

$$\log(\det(I_n - p^{-s}\rho(\mathrm{Frob}_{\mathfrak{p}}))^{-1}) = \sum_{i=1}^{n}\log\left(\frac{1}{1-\lambda_i(p)p^{-s}}\right) = \sum_{i=1}^{n}\sum_{m=1}^{+\infty}\frac{\lambda_i(p)}{mp^{ms}} =$$

$$= \sum_{m=1}^{+\infty}\frac{\mathrm{Tr}(\mathrm{Frob}_{\mathfrak{p}}^m)}{mp^{ms}}$$

where if p is ramified with ramification index e in $F = \overline{\mathbb{Q}}^{\ker\rho}$, we set

$$\mathrm{Tr}(\mathrm{Frob}_{\mathfrak{p}}^m) \coloneqq \frac{1}{e}\sum_{\sigma\in\vartheta^{-1}(\mathrm{Frob}_{\mathfrak{p}}^m)}\chi(\sigma)$$

where $\vartheta\colon D_{\mathfrak{p}}/I_{\mathfrak{p}} \xrightarrow{\sim} \mathrm{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p)$ is the well-known isomorpshim.

3) It's easy to check that if $\rho'\colon G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{C})$ is another Galois representation, then

$$L(s,\rho\oplus\rho') = L(s,\rho)L(s,\rho')$$

4) If $\mathbb{1}\colon G_{\mathbb{Q}} \to \mathbb{C}^*$ denotes the trivial representation, it's clear that

$$L(s,\mathbb{1}) = \zeta(s)$$

The reason for introducing also factors for infinite primes is that the enlarged Artin L-function satisfies a certain functional equation. More precisely, we set

$$\Lambda(s,\rho) \coloneqq N^{s/2}(2\pi)^{-s}\Gamma(s)L(s,\rho)$$

where N is the Artin conductor of ρ. Recall that if $\rho\colon G \to \mathrm{GL}_n(\mathbb{C})$ is any representation of a group G, the *dual representation* or *contragradient representation* is the one given by

$$\begin{aligned}\rho^*\colon G &\to \mathrm{GL}_n(\mathbb{C})\\ \sigma &\mapsto \rho(\sigma^{-1})^T\end{aligned}$$

It's clear that if χ is the character of ρ, then $\overline{\chi}$ is the character of ρ^*. Also, $(\rho^*)^* = \rho$. The following fundamental result holds.

Theorem 3.6. If ρ is a Galois representation, then:

i) the enlarged L-function $\Lambda(s, \rho)$ possesses a meromorphic continuation to the entire complex plane;

ii) the following functional equation holds:

$$\Lambda(1-s, \rho) = W(\rho)\Lambda(s, \rho^*)$$

where $W(\rho)$ is a constant of absolute value 1 which is called *Artin root number*.

Proof. See [Mar77b]. □

One can show that the only possible poles of the meromorphic continuation of $\Lambda(s, \rho)$ are at $s = 0, 1$. Moreover, if ρ doesn't contain the unit representation then this analytic continuation is holomorphic at $s = 0$, so the only interesting possible lack of holomorphy is at $s = 1$.

Conjecture 3.7 (Artin conjecture)**.** If $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{C})$ is a (nontrivial) irreducible Galois representation, then the meromorphic continuation of $\Lambda(s, \rho)$ is holomorphic on the whole complex plane.

The case $n = 1$ is known to be true. It has been proved recently that if $n = 2$ and ρ is odd, then the Artin conjecture is true. The even case is still open.

3.2 The Deligne-Serre theorem

We are now ready to state and prove the main result, following [DS74].

Theorem 3.8. Let $N \in \mathbb{N}$, $\chi \in \widehat{G}_N$ an odd Dirichlet character and let $0 \neq f = \sum_{n=0}^{+\infty} a_n q^n \in M_1(N, \chi)$ be a normalized eigenform for the Hecke operators T_p such that $p \nmid N$. Then there exists a 2-dimensional complex Galois representation

$$\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$$

that is unramified at all primes that do not divide N and such that

$$\mathrm{Tr}(\mathrm{Frob}_p) = a_p \quad \text{and} \quad \det(\mathrm{Frob}_p) = \chi(p)$$

for all primes $p \nmid N$.
Such a representation is irreducible if and only if f is a cusp form.

Remarks 3.9.

1) Thanks to theorem 2.24, the representation ρ is unique up to isomorphism.

2) Clearly, $\det \rho = \chi$, identifying χ with the induced character on $\mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})$ (see example 2.18).

3) Let $c \in G_{\mathbb{Q}}$ be a complex conjugation. Previous point implies that $\det \rho(c) = -1$, namely ρ is odd.

Theorem 3.10. Let $f = \sum_{n=1}^{+\infty} a_n q^n \in S_1(N, \chi)$ be a normalized newform. Let ρ be the corresponding Galois representation given by theorem 3.8. Then

i) the Artin conductor of ρ is equal to N;

ii) the Artin L-function attached to ρ is $L(\rho, s) = \sum_{n=1}^{+\infty} a_n n^{-s}$.

Before proving this theorem, we need a preliminary lemma.

Lemma 3.11. Let

$$G(s) = A^s \prod_p G_p(s) \quad H(s) = A^s \prod_p H_p(s)$$

be two Euler products such that p runs over a finite set of primes, $A \in \mathbb{C}$ is a constant and $G_p(s), H_p(s) = \prod_{j \in J_p} (1 - \alpha_{p,j} p^{-s})^{\pm 1}$, for some $\alpha_{p,j} \in \mathbb{C}$ s.t. $|\alpha_{p,j}| < p^{1/2}$. Suppose also that

$$G(1-s) = \omega H(s) \quad \text{for some } \omega \in \mathbb{C}^*$$

Then $A = 1$ and $G_p(s) = H_p(s) = 1$ for all p.

Proof. If $H_p(s)$ were not 1 for all p, then the function H must have an infinite number of zeroes or poles of the form $(\log \alpha_{p,j} + 2\pi i n)/\log p$ with $n \in \mathbb{Z}$. By the functional equation, those should be zeroes or poles also for $G(1-s)$, but this is impossible since the hypothesis $|\alpha_{p,j}| < p^{1/2}$ ensures us that $\alpha_{p,j} \neq p/\alpha_{p,k}$ for all p, k. ☐

Proof of the theorem. Recall that the following functional equation holds

$$\Lambda(1-s, f) = c\Lambda(s, \overline{f})$$

where $\Lambda(s, f) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(s, f)$. Let M be the Artin conductor of ρ. Then we have

$$\Lambda(1-s, \rho) = W(\rho)\Lambda(s, \rho^*)$$

where $\Lambda(s, \rho) = M^{s/2}(2\pi)^{-s}\Gamma(s)L(s, \rho)$ and $W(\rho) \in \mathbb{C}^*$. Now set

$$F(s) := A^s \frac{L(s, f)}{L(s, \rho)} \quad \overline{F}(s) := A^s \frac{L(s, \overline{f})}{L(s, \rho^*)}$$

where $A = (N/M)^{1/2}$. Combining the two functional equations, one has that

$$F(1-s) = \frac{ic}{W(\rho)} \overline{F}(s)$$

By theorems 3.3 and 3.8, if p is a prime that does not divide N then the p-th terms in the Euler products of $\Lambda(s, f)$ and $\Lambda(s, \rho)$ coincide, so that $F(s) = A^s \prod_{p|N} F_p(s)$ where $F_p(s) = \frac{(1-b_p p^{-s})(1-c_p p^{-s})}{1-a_p p^{-s}}$. Here b_p and c_p are the eigenvalues of $\rho(\mathrm{Frob}_{\mathfrak{p}})$ suitably restricted to some subspace of $\mathbb{C}^2$ (as we already discussed) and $\mathfrak{p}$ lies over p; those numbers have absolute value 1 because $\rho(\mathrm{Frob}_{\mathfrak{p}})$ has finite order. The Fourier coefficients a_p respect the bounds stated in theorem 3.3 and therefore we're allowed to apply the previous lemma and get the claim. ☐

Corollary 3.12.

i) ρ is ramified at all primes dividing N.

ii) $L(\rho, s)$ has an analytic continuation to the entire complex plane (i.e. the Artin conjecture is true for ρ).

Proof. Part i) is immediate, part ii) is due to the fact that f is a normalized newform. □

If $f = \sum_{n=1}^{+\infty} a_n q^n \in S_1(N, \chi)$ is a normalized newform, then the Galois representation ρ attached to it by theorem 3.8 has the following properties:

a) ρ is irreducible;

b) $\chi = \det \rho$ is odd;

c) for all continuous characters $\chi\colon G_{\mathbb{Q}} \to \mathbb{C}^*$ the L-function $L(\rho \otimes \chi, s) = \sum_{n=1}^{+\infty} \chi(n) a_n n^{-s}$ has an analytic continuation to the entire complex plane. This follows from the fact that for any 1-dimensional Galois representation $\chi\colon G_{\mathbb{Q}} \to \mathbb{C}^*$, $f \otimes \chi := \sum_{n=1}^{+\infty} \chi(n) a_n q^n$ is again a newform (possibly of different level) whose corresponding Galois representation is $\rho \otimes \chi$.

Conversely, given a Galois representation satisfying those properties, we have the following

Theorem 3.13 (Weil-Langlands)**.** Given $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$ satisfying a),b),c) above with Artin conductor N and determinant χ, let $L(\rho, s) = \sum_{n=1}^{+\infty} a_n n^{-s}$ be its Artin L-function. Then $f = \sum_{n=1}^{+\infty} a_n q^n$ is a normalized newform lying in $S_1(N, \chi)$.

Such a theorem realize a bijection between the set of (isomorphism classes of) complex Galois representations of conductor N satisfying a),b) and c) above and the set of normalized newforms on $S_1(N, \chi)$. In fact, it's clear that the maps constructed by theorem 3.8 and by Weil-Langlands theorem are inverse one of each other, basically because the eigenspaces of $M_k(N, \chi)$ are at most 1-dimensional. Point c) is the Artin conjecture for the representation $\rho \otimes \chi$. Since ρ is 2-dimensional, $\det(\rho \otimes \chi) = \det(\rho)\chi^2$ and therefore if ρ is odd, so is $\rho \otimes \chi$. A recent work of Khare and Wintenberger on Serre's modularity conjecture has shown that the Artin conjecture for odd, 2-dimensional representations is true. This amounts to say that we have a bijection between the set of (isomorphism classes of) complex, 2-dimensional, irreducible, odd Galois representations of conductor N and the set of normalized newforms on $S_1(N, \chi)$.

3.3 The proof of the Deligne-Serre theorem

3.3.1 Step 1: Application of a result by Rankin to weight 1 modular forms

Proposition 3.14. Let $f \in S_k(N,\chi)$. Suppose f is an normalized eigenform for the T_p operator with $p \nmid N$. Then the series $\sum_{p \nmid N} |a_p|^2 p^{-s}$ converges for all $s \in \mathbb{R}$ such that $s > k$, and we have

$$\sum_{p \nmid N} |a_p|^2 p^{-s} \leq \log\left(\frac{1}{s-k}\right) + O(1) \text{ as } s \to k$$

Proof. Clearly we can assume that $f = \sum_{n=1}^{+\infty} a_n q^n$ is a newform. For all $p \nmid N$, let $\varphi_p \in \mathrm{GL}_2(\mathbb{C})$ be s.t. $\mathrm{Tr}(\varphi_p) = a_p$ and $\det(\varphi_p) = \chi(p)p^{k-1}$[2]. Then we know by theorem 3.3 that the Dirichlet series $L(s,f) = \sum_{n=1}^{+\infty} \frac{a_n}{n^s}$ admits the Euler product

$$L(s,f) = \prod_{p|N}(1 - a_p p^{-s})^{-1} \prod_{p \nmid N} \det(I_2 - \varphi_p p^{-s})^{-1}$$

Now let $F(s) = \prod_{p \nmid N} \det(I_2 - \varphi_p \otimes \overline{\varphi_p} p^{-s})^{-1}$. If we denote by λ_p, μ_p the eigenvalues of φ_p, it follows easily that

$$F(s) = \prod_{p \nmid N}(1 - \lambda_p\overline{\lambda_p}p^{-s})^{-1}(1 - \lambda_p\overline{\mu_p}p^{-s})^{-1}(1 - \mu_p\overline{\lambda_p}p^{-s})^{-1}(1 - \mu_p\overline{\mu_p}p^{-s})^{-1}$$

By the formula $\lambda_p\overline{\lambda_p}\mu_p\overline{\mu_p} = |\det(\varphi_p)|^2 = p^{2k-2}$ one can prove by a little calculation that

$$F(s) = H(s)\zeta(2s-2k+2)\left(\sum_{n=1}^{+\infty} |a_n| n^{-s}\right)$$

where $H(s) = \prod_{p|N}(1 - p^{-2s+2k-2})(1 - |a_p|^2 p^{-s})$. Rankin's proved in [Ran39] that the series $\sum_{n=1}^{+\infty} |a_n|^2 n^{-s}$ converges for $\Re(s) > k$ and its product with $\zeta(2s-2k+2)$ can be extended to a meromorphic function on the entire complex plane with a pole at $s = k$. Since by 3.3 we have that $|a_p| < p^{k/2}$ when $p \mid N$, the function $F(s)$ is clearly holomorphic on $\mathbb{C}$ and $\neq 0$ in $\Re(s) \geq k$. Therefore $F(s)$ is meromorphic on $\mathbb{C}$ and holomorphic for $\Re(s) \geq k$, except for a simple pole in $s = k$; moreover $F(s) \neq 0$ for $\Re(s) > k$ because none of its factors vanish. Now set

$$g_m(s) = \sum_{p \nmid N} \frac{|\mathrm{Tr}(\varphi_p^m)|^2}{m p^{ms}} \quad G(s) = \sum_{m=1}^{+\infty} g_m(s)$$

[2]This is always possible: it is enough to find $\lambda_p, \mu_p \in \mathbb{C}$ s.t. $\lambda_p + \mu_p = a_p$ and $\lambda_p\mu_p = \chi(p)p^{k-1}$.

We claim that for $|s|$ big enough, $G(s) = \log F(s)$. In fact,

$$\log F(s) = -\left(\sum_{p\nmid N} \log(I_2 - \lambda_p\overline{\lambda_p}p^{-s}) + \log(I_2 - \mu_p\overline{\lambda_p}p^{-s}) + \log(I_2 - \lambda_p\overline{\mu_p}p^{-s}) + \log(I_2 - \mu_p\overline{\mu_p}p^{-s})\right)$$

and using the expansion in power series of the logarithm one gets

$$\sum_{p\nmid N}\sum_{m=1}^{+\infty}((\lambda_p\overline{\lambda_p})^m + (\mu_p\overline{\lambda_p})^m + (\lambda_p\overline{\mu_p})^m + (\mu_p\overline{\mu_p})^m)\frac{1}{mp^{ms}} = \sum_{p\nmid N}\sum_{m=1}^{+\infty} g_m(s)$$

since $\mathrm{Tr}(\varphi_p^m) = \lambda_p^m + \mu_p^m$. Now, $F(s)$ is holomorphic and nonzero for $\Re(s) > k$. Recall the following

Lemma 3.15 (Landau)**.** Let $f(s) = \sum_{n=1}^{+\infty} a_n n^{-s}$ be a Dirichlet series with real coefficients $a_n \geq 0$. Suppose that for some $\sigma_0 \in \mathbb{R}$, $f(s)$ converges for all s such that $\Re(s) > \sigma_0$. If $f(s)$ extends to a holomorphic function in a neighborhood of $s = \sigma_0$, then $f(s)$ converges for $\Re(s) > \sigma_0 - \varepsilon$ for some $\varepsilon > 0$.

This lemma applied to $G(s)$ shows that $G(s)$ converges for $\Re(s) > k$. Since $L(s)$ has a simple pole in $s = k$, we get easily that

$$G(s) = \log\left(\frac{1}{s-k}\right) + O(1) \text{ for } s \to k$$

The claim easily follows from the fact that

$$\sum_{p\nmid N} |a_p|^2 p^{-s} = g_1(s) \leq G(s)$$

□

Before applying the above result to weight 1 modular forms, let's state the following

Definition 3.16. Let $\mathscr{P}$ the set of natural primes and $X \subseteq \mathscr{P}$. The *upper density* of X is given by

$$\text{dens sup}\, X = \limsup_{s\to 1,\, s>1} \frac{\sum_{p\in X} p^{-s}}{\log(1/(s-1))}$$

It's a well-known fact that this value lies in $[0, 1]$.

Proposition 3.17. Let $f \in S_1(N, \chi)$ be an eigenform for the Hecke operator T_p where $p \nmid N$. Then for every real $\eta > 0$, there exists $X_\eta \subseteq \mathscr{P}$, $Y_\eta \subseteq \mathbb{C}$ with Y_η finite such that

$$\text{dens}\sup X_\eta \leq \eta \text{ and } a_p \in Y_\eta \text{ for all } p \notin X_\eta$$

Proof. By theorem 1.51, $a_p \in K\ \forall p$, where K is a fixed number field. Now let $c \geq 0$ be a real constant. The set

$$Y(c) = \{\alpha \in \mathcal{O}_K : |\sigma(\alpha)|^2 \leq c \text{ for all embeddings } \sigma\colon K \to \mathbb{C}\}$$

is finite. This is because if $\sigma_1, \dots, \sigma_n$ are the embeddings of K in $\mathbb{C}$, then for any $\alpha \in Y(c)$ of degree $m \in \mathbb{N}$, the j-th coefficient of the minimal polynomial $x^m + a_{m-1}x^{m-1} + \cdots + a_0$ of α over $\mathbb{Q}$ is given by

$$a_j = \sum_{\substack{i_1, \dots, i_{m-j} \\ i_k \neq i_l \text{for } k \neq l}} \sigma_{i_1}(a) \dots \sigma_{i_{m-j}}(a)$$

and therefore one has by the triangle inequality

$$|a_j| = \sum_{\substack{i_1, \dots, i_{m-j} \\ i_k \neq i_l \text{for } k \neq l}} |\sigma_{i_1}(a)| \dots |\sigma_{i_{m-j}}(a)| \leq \binom{m}{m-j} \sqrt{c}$$

Since the a_j's are integers, this means that the minimal polynomials of the elements of $Y(c)$ are just a finite number, and hence $Y(c)$ must be finite. Now set

$$X(c) = \{p \in \mathscr{P} \colon a_p \notin Y(c)\}$$

It will be enough to prove that $\operatorname{dens\,sup} X(c) \leq \eta$ for sufficiently large c. Again by theorem 1.51, we know that $\sigma_i(a_p)$ is an eigenvalue for T_p for every embedding σ_i. Thanks to proposition 3.14 we have

$$\sum_{i=1}^{n} \sum_{p} |\sigma_i(a_p)|^2 p^{-s} \leq n \log\left(\frac{1}{s-1}\right) + O(1) \text{ for } s \to 1$$

Since $\displaystyle\sum_{i=1}^{n} |\sigma_i(a_p)|^2 \geq c$ for $p \in X(c)$, it's easy to conclude that

$$c \sum_{p \in X(c)} p^{-s} \leq n \log\left(\frac{1}{s-1}\right) + O(1) \text{ for } s \to 1$$

and so $\operatorname{dens\,sup} X(c) \leq n/c$, implying that it's enough to set $c \geq n/\eta$ to prove the claim. □

3.3.2 Step 2: l-adic and mod l representations

The key result we will use in our proof is the following, which is due to Deligne. For the proof and more details, see [Del71].

Theorem 3.18. Let $0 \neq f \in M_k(N, \chi)$, with $k \geq 2$. Suppose that f is a normalized eigenform for all T_p with $p \nmid N$. Let K be a number field which contains all the a_p and all the $\chi(p)$. Let λ be a finite place of K of residual characteristic l, and let K_λ be the completion of K with respect to it. Then there exists a semisimple Galois representation

$$\rho_\lambda \colon G_{\mathbb{Q}} \to \mathrm{GL}_2(K_\lambda)$$

which is unramified at all primes that don't divide Nl and s.t.

$$\mathrm{Tr}(\mathrm{Frob}_p) = a_p \text{ and } \det(\mathrm{Frob}_p) = \chi(p)p^{k-1} \text{ if } p \nmid Nl$$

By theorem 2.24, such a representation is unique up to isomorphism.
If f is an Eisenstein series, the attached representation is the direct sum of two 1-dimensional representations, and is therefore reducible. The construction of those Galois representations involves the étale cohomology of the modular curve of level N. It is interesting to note that the weight of the modular form we start with has to be ≥ 2, so for the weight 1 case we will need a different construction. First of all, we will show how it is possible, using theorem 3.18, to attach to an eigenform as above of any weight a continuous representation over a field of characteristic > 0. From here to the end of this section, $K \subseteq \mathbb{C}$ is a number field, λ is a finite place of K, $\mathcal{O}_\lambda$ is the valuation ring and m_λ its maximal ideal. Furthermore, $k_\lambda = \mathcal{O}_\lambda / m_\lambda$ is the residue field and l its characteristic.

Definition 3.19. Let $f \in M_k(N, \chi)$, where $k \geq 1$. We say that f is λ-*integral* (resp. that $f \equiv 0 \bmod m_\lambda$) if every coefficient of the Fourier expansion of f lies in $\mathcal{O}_\lambda$ (resp. in m_λ).
if f is λ-integral, we say that f is an *eigenform* $\bmod\, m_\lambda$ of the Hecke operator T_p, with eigenvalue $a_p \in k_\lambda$ if

$$T_p f - a_p f \equiv 0 \bmod m_\lambda$$

Theorem 3.20. Let $f \in M_k(N, \chi)$, $k \geq 1$, with coefficients in K. Suppose that f is λ-integral but $f \not\equiv 0 \bmod m_\lambda$ and that f is an eigenform of T_p modulo m_λ, for $p \nmid Nl$, with eigenvalues $a_p \in k_\lambda$. Let k_f be the subextension of k_λ generated by the a_p and the $\chi(p) \mod m_\lambda$. Then there exists a semisimple representation

$$\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(k_f)$$

unramified outside of Nl and s.t. for all primes $p \nmid Nl$ one has

$$\mathrm{Tr}(\mathrm{Frob}_p) = a_p \text{ and } \det(\mathrm{Frob}_p) \equiv \chi(p) p^{k-1} \bmod m_\lambda \qquad (**)$$

Before starting with the proof of this theorem, we state two preliminary lemmas.

Lemma 3.21. Let M be a free module of finite rank over a discrete valuation ring $\mathcal{O}$. Let $m \subseteq \mathcal{O}$ be the maximal ideal, k the residue field and K the field of fractions of $\mathcal{O}$. Let $\mathcal{T} \subseteq \mathrm{End}_{\mathcal{O}}(M)$ be a set of endomorphisms which commute two by two. Let $f \in M/mM$ be a nonzero common eigenvector for all the $T \in \mathcal{T}$, with eigenvalues a_T. Then there exist:

a) a discrete valuation ring $\mathcal{O}' \supseteq \mathcal{O}$ with maximal ideal m' s.t. $m' \cap \mathcal{O} = m$ and with field of fractions K' s.t. $[K' \colon K] < \infty$;

b) an element $0 \neq f' \in M' = \mathcal{O}' \otimes_{\mathcal{O}} M$ which is an eigenvector for all the $T \in \mathcal{T}$ with eigenvalues $a'_T \equiv a_T \mod m'$.

Proof. See [DS74]. □

Lemma 3.22. Let $\varphi\colon G \to \mathrm{GL}_n(k)$ be a semisimple representation of a group G over a finite field k. Let $k' \subseteq k$ be a subfield s.t. the coefficients of the polynomials $\det(I_n - \varphi(\sigma)T)$, $\sigma \in G$ all lie in k'. Then φ is *realizable* over k', namely φ is isomorphic to a representation $\varphi'\colon G \to \mathrm{GL}_n(k')$.

Proof. See [DS74]. □

Proof of theorem 3.20. We are going to do three preliminary reductions.
a) Suppose that $(K', \lambda', f', k', \chi', (a'_p))$ is as in the hypothesis of the theorem with $K \subseteq K'$ and $\lambda' \mid \lambda$. Then if $a_p \equiv a'_p \mod m_{\lambda'}$ and $\chi(p)p^{k-1} \equiv \chi'(p)p^{k'-1} \mod m_{\lambda'}$ for all $p \nmid Nl$, it's immediate to see that the theorem holds for f if and only if it holds for f'. In particular, if $f \equiv f' \mod \lambda'$, $\chi = \chi'$ and $k \equiv k' \mod (l-1)$, then the theorem for f and the theorem for f' are equivalent.
b) If $n > 2$ is an even integer, let E_n be the Eisenstein series of weight n over Γ (see definition 1.12). If $l - 1 \mid n$ then one can show (see [SD73]) that E_n is l-integral and that $E_n \equiv 1 \mod l$. This shows that $fE_n \equiv f \mod \lambda$, and of course fE_n is a modular form of type $(k + n, \chi)$ on $\Gamma_0(N)$. By our choice of n, $k + n \equiv k \mod (l - 1)$ and so by reduction a) the theorem for f is equivalent to the theorem for fE_n which has weight > 2.
c) It's enough to show the theorem for f eigenform for the T_p, $p \nmid Nl$. In fact, pick any f as in the hypothesis of the theorem. Now apply lemma 3.21 with $M = \{f \in M_k(N, \chi) \colon f \text{ has coefficient in } \mathcal{O}_\lambda\}$ and $\mathcal{T} = \{T_p\}_{p \nmid Nl}$. Then we can find some $f' \in M$ which is equivalent to f modulo λ because of the lemma and such that $(k, \chi) = (k', \chi')$. Therefore we can apply again reduction a).
So from now on, let $k \geq 2$ and f be an eigenform for the T_p, $p \nmid Nl$. If $l \nmid N$, since T_p and T_l commute we may as well suppose that f is an eigenvector for T_l. Now apply theorem 3.18 and construct a representation

$$\rho_\lambda \colon G_\mathbb{Q} \to \mathrm{GL}_2(K_\lambda)$$

By lemma 2.19, we can assume that the image of ρ_λ is contained in $\mathrm{GL}_2(\widehat{\mathcal{O}_\lambda})$, where $\widehat{\mathcal{O}_\lambda}$ is the valuation ring of K_λ. Now reduce such a representation modulo λ to get another representation

$$\widetilde{\rho_\lambda} \colon G_\mathbb{Q} \to \mathrm{GL}_2(k_\lambda)$$

To conclude the proof, let φ be the semisimplification of $\widetilde{\rho_\lambda}$: this is a semisimple represetation, unramified outside Nl and satisfying (**). The group $\varphi(G_\mathbb{Q})$ is isomorphic to $\mathrm{Gal}(\overline{\mathbb{Q}}^{\ker \varphi}/\mathbb{Q})$ and is finite: by Chebotarev density theorem we deduce that every element in $\varphi(G_\mathbb{Q})$ is of the form $\varphi(\mathrm{Frob}_\mathfrak{p})$, with $\mathfrak{p} \cap \mathbb{Q} = p$ and $p \nmid Nl$. By the definition of k_f, it follows directly that the polynomials $\det(I_2 - \varphi(\sigma)T)$, $\sigma \in G_\mathbb{Q}$ all lie in k_f and by applying lemma 3.22 we are done.
□

3.3.3 Step 3: A bound on the order of certain subgroups of $GL_2(\mathbb{F}_l)$

In this section, $l \in \mathbb{Z}$ will denote a prime and $\mathbb{F}_l = \mathbb{Z}/l\mathbb{Z}$. Let η, M be two positive real numbers, let G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_l)$.

Definition 3.23. We say that G has the property $C(\eta, M)$ if there exists a subset $H \subseteq G$ s.t.

i) $|H| \geq (1 - \eta)|G|$;

ii) $|\{\det(1 - hT),\, h \in H\}| \leq M$.

We say that G is *semisimple* if the identical representation $G \to \mathrm{GL}_2(\mathbb{F}_l)$ is semisimple.

Proposition 3.24. Let $\eta < 1/2$ and $M \geq 0$. Then there exists a constant $A = A(\eta, M)$ s.t. for all primes l and all semisimple subgroups $G \leq \mathrm{GL}_2(\mathbb{F}_l)$ satisfying the $C(\eta, M)$ property, we have $|G| \leq A$.

Proof. Let $G \leq \mathrm{GL}_2(\mathbb{F}_l)$ be a semisimple subgroup. Then one of the following is true (cfr. [Ser72]):

a) $\mathrm{SL}_2(\mathbb{F}_l) \leq G$;

b) G is contained in some Cartan subgroup T;

c) G is contained in the normalizator of some Cartan subgroup T and is not contained in T;

d) the image of G in $\mathrm{PGL}_2(\mathbb{F}_l)$ is isomorphic to S_4, A_4 or A_5.

We will show that in each case we have an upper bound on $|G|$. Recall that $|\mathrm{GL}_2(\mathbb{F}_l)| = (l^2-1)(l^2-l)$. This implies, by the fact that the determinant induces an exact sequence $0 \to \mathrm{SL}_2(\mathbb{F}_l) \to \mathrm{GL}_2(\mathbb{F}_l) \overset{\det}{\to} \mathbb{F}_l^* \to 0$, that $|\mathrm{SL}_2(\mathbb{F}_l)| = l^3 - l$. Now we can start to analize the different cases.
a) Let $r = (G\colon \mathrm{SL}_2(\mathbb{F}_l))$. Then $|G| = r(l^3 - l)$. If we fix any characteristic polynomial, the number of elements of $\mathrm{GL}_2(\mathbb{F}_l)$ having that characteristic polynomial is $l^2 + l, l^2$ or $l^2 - l$ depending if the polynomial has respectively 2,1 or 0 roots in $\mathbb{F}_l$. Therefore if G satisfies $C(\eta, M)$ in any case we have

$$(1-\eta)rl(l^2-l) = (1-\eta)|G| \leq |H| \leq M(l^2+l)$$

implying

$$(1-\eta)r(l-1) \leq M \Longrightarrow l \leq 1 + \frac{M}{(1-\eta)r} \leq 1 + \frac{M}{1-\eta}$$

Since we have a bound on l, we have automatically a bound on $|\mathrm{GL}_2(\mathbb{F}_l)|$ and so also on $|G|$.
b) Fixed a characteristic polynomial, no more than 2 elements of T can have it as characteristic polynomial. The fact that $\eta < 1/2$ implies easily that

$$(1-\eta)|G| \leq 2M \Longrightarrow |G| \leq \frac{2M}{1-\eta}$$

c) The group $G' = G \cap T$ has index 2 in G. Therefore if G satisfy $C(\eta, M)$ then we have

$$(1-\eta)|G| = (1-\eta)2|G'| = (1-2\eta)|G'| + |G'| \leq |H|$$

namely $(1-2\eta)|G'| \leq |H| - |G'|$. On the other hand, $|H| - |G'| \leq |H \cap T|$, because the condition $\eta < 1/2$ ensures us that $|H| \geq |G|/2 = |G'|$ so once we set $H' := H \cap T$ using point b) for G' we finally have

$$|G| \leq \frac{4M}{1-2\eta}$$

d) The image of G in $\mathrm{PGL}_2(\mathbb{F}_l)$ has order at most $60 = |A_5|$. Therefore $G \cap \mathrm{SL}_2(\mathbb{F}_l)$ has order at most 120, because for every element $M \in \mathrm{SL}_2(\mathbb{F}_l)$ the only multiple of M lying again in $\mathrm{SL}_2(\mathbb{F}_l)$ is $-M$. Now, by the exactness of the sequence $\mathrm{SL}_2(\mathbb{F}_l) \hookrightarrow \mathrm{GL}_2(\mathbb{F}_l) \twoheadrightarrow \mathbb{F}_l^*$ it follows that for any fixed determinant $\beta \in \mathbb{F}_l^*$ there exist at most 120 matrices in G with determinant β: in fact fixed such a matrix in G then only all its multiple by elements of $\mathrm{SL}_2(\mathbb{F}_l) \cap G$ have determinant β. So in G there are also at most 120 elements with fixed characteristic polynomial. Then if G satisfies $C(\eta, M)$ we have $(1-\eta)|G| \leq 120M$, namely

$$|G| \leq \frac{120M}{1-\eta}$$

The theorem is clearly proved choosing A as the maximum among the constants found in each case. □

3.3.4 Step 4: Conclusion of the proof

Let f be as in the hypothesis of theorem 3.8. If f is an Eisenstein series, theorem 1.50 shows us immediately how to construct the desired rappresentation: f is uniquely associated to two Dirichlet characters that ψ, φ that (raised to modulo N) have product χ. Hence the map

$$\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$$

$$\sigma \mapsto \begin{pmatrix} \psi(\sigma) & 0 \\ 0 & \varphi(\sigma) \end{pmatrix}$$

is a reducible representation with the desired properties, after having identified ψ and φ with characters of $G_{\mathbb{Q}}$ as in example 2.18.

So from now on we suppose that $f = \sum_{n=1}^{+\infty} a_n q^n$ is a cusp form. Let $K \subseteq \mathbb{C}$ be a Galois number field containing the a_p and the $\chi(p)$, for all primes p. Let L be the set of rational primes that split completely in K. For all $l \in L$, fix a place λ_l of K extending l. The residue field is of course isomorphic to $\mathbb{F}_l$. By theorem 3.20, there exists a semisimple continuous representation

$$\rho_l\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_l)$$

unramified outside of Nl and s.t. $\det(1 - \mathrm{Frob}_p T) \equiv 1 - a_p T + \chi(p) T^2 \bmod \lambda_l$ for all primes $p \nmid Nl$. Now let $G_l = \rho_l(G_{\mathbb{Q}}) \subseteq \mathrm{GL}_2(\mathbb{F}_l)$.

Lemma 3.25. For all $\eta > 0$, there exists a constant M s.t. G_l satisfies $C(\eta, M)$ for all $l \in L$.

Proof. By proposition 3.17, there exists a subset $X_\eta \subseteq \mathscr{P}$ s.t. $\operatorname{dens\,sup} X_\eta \leq \eta$ and s.t. the set $\{a_p \colon p \notin X_\eta\}$ is finite. Now let $\mathscr{M} = \{1 - a_p T + \chi(p) T^2 \colon p \notin X_\eta\}$ which is a finite set, and let $M = |\mathscr{M}|$. We claim that G_l satisfies $C(\eta, M)$ for all $l \in L$. In fact, $G_l \cong \overline{\mathbb{Q}}^{\ker \rho} = \mathrm{Gal}(F/\mathbb{Q}) = G$ for some Galois number field F because of the continuity of ρ_l. Now let $H = \{\sigma^{-1} \mathrm{Frob}_{\mathfrak{p}} \sigma \colon \sigma \in G,\ \mathfrak{p} \mid p\} \subseteq G$ and $H_l \subseteq G_l$ be its image under the isomorphism $G \to G_l$. By Chebotarev density theorem, $|H| \geq (1-\eta)|G|$, so that $|H_l| \geq (1-\eta)|G_l|$. On the other hand, if $h \in H_l$ then by construction the polynomial $\det(1 - hT)$ is the reduction modulo λ_l of an element in $\mathscr{M}$ and therefore it lies in a set that contains at most M elements. Hence G_l satisfies $C(\eta, M)$. □

Corollary 3.26. If $\eta < 1/2$, there exists an absolute constant $A = A(\eta, M)$ s.t. $|G_l| \leq A$ for all $l \in L$.

Proof. This follows directly from proposition 3.24 together with the fact that obviously G_l is semisimple being ρ_l a semisimple representation. □

So now fix a constant A as in the above corollary. Up to replacing K with a bigger number field (reducing L consequently), we may well suppose that K contains all n-th roots of unity for all $n \leq A$. Let

$$Y = \{(1-\alpha T)(1-\beta T) \colon \alpha, \beta \text{ are roots of unity of order } \leq A\}$$

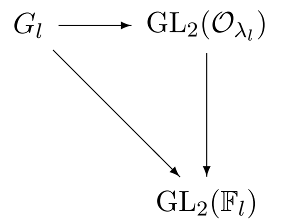
It's clear that by construction if $p \nmid N$, then for all $l \in L$ with $l \neq p$ there exists $R(T) \in Y$ s.t.

$$1 - a_p T + \chi(p)T^2 \equiv R(T) \bmod \lambda_l$$

Since Y is finite and L is infinite, there must exist some $R(T)$ s.t. the above congruence is satisfied for an infinite number of l's. This implies that such a congruence has to be an equality, namely that the polynomials $1 - a_p T + \chi T^2$ all lie in Y. Now let

$$L' = \{l \in L \colon l > A,\ R, S \in Y,\ R \neq S \Longrightarrow R \not\equiv S \bmod \lambda_l\}$$

Since $L \setminus L'$ is finite, L' is infinite. Choose $l \in L'$. Since $|G_l| < A$ and $A < l$, it follows that $(|G_l|, l) = 1$ and therefore the identical representation $G_l \to \mathrm{GL}_2(\mathbb{F}_l)$ is the reduction modulo λ_l of a representation $G_l \to \mathrm{GL}_2(\mathcal{O}_{\lambda_l})$, where $\mathcal{O}_{\lambda_l}$ is the valuation ring of λ_l in K, namely we have a commutative diagram



Composing the representation $G_l \to \mathrm{GL}_2(\mathcal{O}_{\lambda_l})$ with the projection $G_{\mathbb{Q}} \to G_l$ we get a representation $\rho \colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O}_{\lambda_l})$ which by construction is unramified outside Nl. If $p \nmid Nl$, the eigenvalues of $\rho(\mathrm{Frob}_p)$ are roots of unity of order $\leq A$, because $\rho(G_{\mathbb{Q}}) \cong G_l$ and $|G_l| \leq A$. Therefore $\det(I_2 - \rho(\mathrm{Frob}_p)T) \in Y$. On the other hand, again by construction one has that

$$\det(I_2 - \rho(\mathrm{Frob}_p)T) \equiv 1 - a_p T + \chi(p)T^2 \bmod \lambda_l$$

But we have seen above that $1 - a_p T + \chi(p)T^2 \in Y$ and since $l \in L'$ the last congruence is an equality. Now repeat the same construction by choosing another $l' \in L'$. What we find is a second representation $\rho' \colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O}_{\lambda_{l'}})$ which has the same properties as ρ but for $p \nmid Nl'$. This implies that

$$\det(I_2 - \rho(\mathrm{Frob}_p)T) = \det(I_2 - \rho'(\mathrm{Frob}_p)T) \quad \forall\, p \nmid Nll'$$

By theorem 2.24 it follows easily that ρ and ρ' are isomorphic as representation over $\mathrm{GL}_2(K)$ and so they are isomorphic also as complex representations. Moreover, since ρ is unramified at l' and symmetrically ρ' is unramified at l, then both ρ and ρ' are unramified outside N. Finally, by construction we clearly have that

$$\det(I_2 - \rho(\mathrm{Frob}_p)T) = 1 - a_p T + \chi(p)T^2 \quad \forall\, p \nmid N$$

The last thing we have to show is that ρ is irreducible. Suppose it is not. Then there exist two 1-dimensional representations $\chi_1, \chi_2 \colon G_{\mathbb{Q}} \to \mathbb{C}^*$ s.t. $\rho \cong \chi_1 \oplus \chi_2$, so that $\chi = \chi_1\chi_2$, $a_p = \chi_1(p) + \chi_2(p)$ for $p \nmid N$ and both χ_i's are unramified outside N. Then we have

$$\sum |a_p|^2 p^{-s} = 2\sum p^{-s} + \sum \chi_1(p)\overline{\chi_2(p)}p^{-s} + \sum \overline{\chi_1(p)}\chi_2(p)p^{-s}$$

It's a well-known fact that as $s \to 1^+$, $\sum p^{-s} = \log\left(\frac{1}{s-1}\right) + O(1)$. On the other hand, $\chi_1\overline{\chi_2} \neq \mathbb{1}$ because otherwise we would have $\chi = \chi_1^2$ and so $\chi(-1) = 1$. Hence,

$$\sum \chi_1(p)\overline{\chi_2(p)}p^{-s} = O(1) = \sum \overline{\chi_1(p)}\chi_2(p)p^{-s}$$

and so

$$\sum |a_p|^2 p^{-s} = 2\log\left(\frac{1}{s-1}\right) + O(1)$$

which is in contradiction with proposition 3.14.

Chapter 4

The dimension of $S_1^+(N, \chi)$

One of the applications of the Deligne-Serre theorem is a way to compute the dimension of the space $S_1^+(N, \chi)$. In fact, this can be done by counting isomorphism classes of irreducible 2-dimensional complex Galois representations with conductor N and determinant χ. The aim of this chapter is to illustrate this technique in a particular case, namely the case where N is prime. The method starts from a characterization of the projective images of linear representations.

4.1 Projective Galois representations

Definition 4.1. A *projective Galois representation* is a continuous homomorphism $\overline{\rho}\colon G_{\mathbb{Q}} \to \mathrm{PGL}_n(\mathbb{C})$.

Such an homomorphism must have finite image. In fact, if there would exist an open neighborhood of the identity of $\mathrm{PGL}_n(\mathbb{C})$ containing a nontrivial subgroup, then the preimage in $\mathrm{GL}_n(\mathbb{C})$ of such a neighborhood would be an open neighborhood of the identity in $\mathrm{GL}_n(\mathbb{C})$ containing a nontrivial subgroup, too and this is impossible by theorem 2.15.
It is clear that every complex Galois representation gives rise to a projective representation just by composing with the projection $\pi\colon \mathrm{GL}_n(\mathbb{C}) \twoheadrightarrow \mathrm{PGL}_n(\mathbb{C})$. Conversely, one could ask wether given a projective Galois representation $\overline{\rho}$, there exist a Galois representation ρ such that $\overline{\rho} = \pi \circ \rho$.

Definition 4.2. Let $\overline{\rho}\colon G_{\mathbb{Q}} \to \mathrm{PGL}_n(\mathbb{C})$ be a projective Galois representation. A *lifting* of $\overline{\rho}$ is a Galois representation $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{C})$ such that the following diagram

$$\begin{array}{ccc} G_{\mathbb{Q}} & \xrightarrow{\rho} & \mathrm{GL}_n(\mathbb{C}) \\ & \overline{\rho}\searrow & \downarrow \pi \\ & & \mathrm{PGL}_n(\mathbb{C}) \end{array}$$

commutes.

Remark 4.3. Let ρ be a lifting of $\overline{\rho}$. Then for any 1-dimensional Galois representation $\chi\colon G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{C})$, the representation $\rho \otimes \chi$ is a lifting of ρ, too. Indeed, for any $\sigma \in G_{\mathbb{Q}}$, $\rho(\sigma)$ and $(\rho \otimes \chi)(\sigma)$ differ for a nonzero constant, and so they

map to the same element of the quotient $\mathrm{PGL}_n(\mathbb{C})$.
Conversely, let ρ and ρ' be two liftings of $\overline{\rho}$. Then it is clear that $\rho' = \rho \otimes \chi$ for some 1-dimensional representation χ.

The reason why is useful to look at projectivizations of 2-dimensional Galois representation is that $\mathrm{PGL}_2(\mathbb{C})$ contains up to isomorphism just a few number of finite subgroups, which are classified by the following

Theorem 4.4. Let $G \subseteq \mathrm{PGL}_2(\mathbb{C})$ be a finite subgroup. Then G is either

- cyclic;
- isomorphic to the dihedral group D_{2n};
- isomorphic to S_4 or A_4;
- isomorphic to A_5.

Proof. See [Ser72]. □

Corollary 4.5. Let $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$ be a Galois representation and $\overline{\rho}\colon G_{\mathbb{Q}} \to \mathrm{PGL}_2(\mathbb{C})$ its projectivization. Then ρ is reducible if and only if $\overline{\rho}(G_{\mathbb{Q}})$ is cyclic.

Proof. If ρ is reducible then $\rho(\sigma) = \begin{pmatrix} \rho_1(\sigma) & 0 \\ 0 & \rho_2(\sigma) \end{pmatrix}$ for some 1-dimensional representations ρ_1 and ρ_2. So for every $\sigma \in G_{\mathbb{Q}}$ we have that

$$\overline{\rho}(\sigma) \equiv \begin{pmatrix} \rho_1(\sigma)\rho_2^{-1}(\sigma) & 0 \\ 0 & 1 \end{pmatrix} \bmod \mathbb{C}^*$$

By theorem 4.4 the group $\overline{\rho}(G_{\mathbb{Q}})$ is either cyclic or isomorphic to D_4. The latter case is however impossible, since clearly $\overline{\rho}(G_{\mathbb{Q}})$ can contain at most 1 element of period 2.
Conversely, if $\overline{\rho}(G_{\mathbb{Q}})$ is cyclic, in particular it is abelian. Then also $\rho(G_{\mathbb{Q}})$ is abelian because $\mathbb{C}^* \cap \rho(G_{\mathbb{Q}})$ is contained in the center of $\rho(G_{\mathbb{Q}})$. Now let $F = \overline{\mathbb{Q}}^{\ker \rho}$ and consider ρ as a faithful representation of the finite group $G = \mathrm{Gal}(F/\mathbb{Q})$. This implies that G is abelian, but the irreducible representations of an abelian group can be just 1-dimensional, and therefore ρ must be reducible as a representation of G, and so also as a representation of $G_{\mathbb{Q}}$. □

Of course the first natural problem is understanding when a projective representation admits a lifting. The answer is provided by the following theorem, which uses concepts from Galois cohomology. So note that with $H^n(G, A) = Z^n(G, A)/B^n(G, A)$ we will denote the n-th Galois cohomology group of the G-module A, where G is a group, A is an abelian group and the action of G on A is continuous with respect to the discrete topology on A.

Theorem 4.6. Let $\overline{\rho}\colon G_K \to \mathrm{PGL}_n(\mathbb{C})$ be a continuous representation of the Galois group $G_K = \mathrm{Gal}(\overline{K}/K)$, where K is a local or a global field. Then $\overline{\rho}$ admits a lifting to a continuous representation $\rho\colon G_K \to \mathrm{GL}_n(\mathbb{C})$.

Proof. For each $\sigma \in G_K$ choose an element $\alpha(\sigma) \in \mathrm{GL}_n(\mathbb{C})$ such that $\alpha(\sigma) \equiv \overline{\rho}(\sigma) \bmod \mathbb{C}^*$. Of course this is not necessarily an homomorphism of G_K to $\mathrm{GL}_n(\mathbb{C})$. However,

$$\alpha(\sigma_1\sigma_2) \equiv \overline{\rho}(\sigma_1)\overline{\rho}(\sigma_2) \equiv \alpha(\sigma_1)\alpha(\sigma_2) \bmod \mathbb{C}^*$$

and this implies that $\alpha(\sigma_1)\alpha(\sigma_2)\alpha(\sigma_1\sigma_2)^{-1} \in \mathbb{C}^*$. So we have defined a map

$$\xi\colon G_K \times G_K \to \mathbb{C}^*$$
$$(\sigma_1, \sigma_2) \mapsto \alpha(\sigma_1)\alpha(\sigma_2)\alpha(\sigma_1\sigma_2)^{-1}$$

which is continuous. One checks directly that ξ is a also a 2-cocycle, namely that

$$d_2(\xi)(\sigma_1, \sigma_2, \sigma_3) = \xi(\sigma_2, \sigma_3)\xi(\sigma_1\sigma_2, \sigma_3)^{-1}\xi(\sigma_1, \sigma_2\sigma_3)\xi(\sigma_1, \sigma_2)^{-1} = 1$$

where the action of G_K on $\mathbb{C}^*$ is trivial. So $\xi \in Z^2(G_K, \mathbb{C}^*)$. Now, by the theorem of Tate proved by Serre in [Ser77b], the group $H^2(G_K, \mathbb{C}^*)$ is trivial. Hence $Z^2(G_K, \mathbb{C}^*) = B^2(G_K, \mathbb{C}^*)$ and ξ is a coboundary. This means that there exists a continuous map

$$\beta\colon G_K \to \mathbb{C}^*$$

such that $\xi = d_1(\beta)$, i.e. such that $\xi(\sigma_1, \sigma_2) = \beta(\sigma_1)\beta(\sigma_2)\beta(\sigma_1\sigma_2)^{-1}$. Now define

$$\rho\colon G_K \to \mathrm{GL}_n(\mathbb{C})$$
$$\sigma \mapsto \beta(\sigma)^{-1}\alpha(\sigma)$$

By construction, ρ is continuous and $\rho(\sigma) \equiv \overline{\rho}(\sigma) \bmod \mathbb{C}^*$, so we only need to show that it is a homomorphism. For all $\sigma_1, \sigma_2 \in G_K$, we have

$$\rho(\sigma_1)\rho(\sigma_2) = \rho(\sigma_1)\rho(\sigma_2)\rho(\sigma_1\sigma_2)^{-1}\rho(\sigma_1\sigma_2) =$$
$$= \beta(\sigma_1)^{-1}\alpha(\sigma_1)\beta(\sigma_2)^{-1}\alpha(\sigma_2)\beta(\sigma_1\sigma_2)\alpha(\sigma_1\sigma_2)^{-1}\rho(\sigma_1\sigma_2) =$$
$$= [\beta(\sigma_1)\beta(\sigma_2)\beta(\sigma_1\sigma_2)^{-1}]^{-1}[\alpha(\sigma_1)\alpha(\sigma_2)\alpha(\sigma_1\sigma_2)^{-1}]\rho(\sigma_1\sigma_2) = \rho(\sigma_1\sigma_2)$$

and we are done. □

The following theorem shows how one can recover a global lifting starting from local ones.

Theorem 4.7 (Tate)**.** Let $\overline{\rho}\colon G_{\mathbb{Q}} \to \mathrm{PGL}_n(\mathbb{C})$ be a projective Galois representation. For each prime $p \in \mathbb{Z}$, let ρ'_p be a lifting of $\overline{\rho}|_{D_p}$. Suppose that ρ'_p is unramified at p for almost all p. Then there exists a unique lifting ρ of $\overline{\rho}$ s.t.

$$\rho|_{I_p} = \rho'_p|_{I_p}$$

for all p.

Proof. Let ρ_1 be any lifting of $\overline{\rho}$. For each p, let χ_p be a 1-dimensional representation of D_p s.t.

$$\rho'_p = \chi_p \otimes \rho_1|_{D_p}$$

Clearly χ_p is unramified for almost all p, because so is ρ'_p. By (local) class field theory we can consider χ_p as a character of $\mathbb{Q}_p^*$. Doing that for all p we can find an idele class character χ of $\mathbb{Q}$ s.t. $\chi|_{\mathbb{Z}_p^*} = \chi_p|_{\mathbb{Z}_p^*}$ for all p. Now again by class field theory we can view such a character as a character of $G_{\mathbb{Q}}$. Then $\rho = \chi \otimes \rho_1$ is the required lifting. □

Definition 4.8. Let $\overline{\rho}\colon G_{\mathbb{Q}} \to \mathrm{PGL}_n(\mathbb{C})$ be a projective Galois representation. The *conductor* of $\overline{\rho}$ is the integer

$$N = \prod_p p^{m(p)}$$

where $m(p)$ is the least integer s.t. $\overline{\rho}|_{D_p}$ has a lifting with conductor $p^{m(p)}$.

By theorem 4.7 it is clear that if $\overline{\rho}$ has conductor N then it has a lifting with conductor N. Moreover, since any two liftings differ by a character, any lifting of $\overline{\rho}$ has conductor a multiple of N.
From now on, we will set $n = 2$.

Remarks 4.9. Let $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$ be a Galois representation and $\overline{\rho}\colon G_{\mathbb{Q}} \to \mathrm{PGL}_2(\mathbb{C})$ be its projectivization. Let $\rho_p = \rho|_{D_p}$ and $F_p = \overline{\mathbb{Q}}_p^{\ker \rho_p}$

1) If ρ is unramified at p, then $I_p \cap F_p = \{1\}$, so $D_p \cap F_p$ is cyclic and therefore $\overline{\rho}(D_p)$ is cyclic, too. Obviously, $m(p) = 0$.

2) If ρ is ramified at p, but only tamely ramified, then $\overline{\rho}(D_p)$ is either cyclic or dihedral. This is because $\overline{\rho}|_{I_p}$ factors through the wild inertia group $G_{p,1}$ and so $\overline{\rho}(I_p) = \overline{\rho}(I_p/G_{p,1})$ is cyclic. Consequently, $\overline{\rho}(D_p)$ has a normal cyclic subgroup, namely $\overline{\rho}(I_p)$. Since there exists a surjection $D_p/I_p \to \overline{\rho}(D_p)/\overline{\rho}(I_p)$, this last group is abelian. By theorem 4.4 this implies that $\overline{\rho}(D_p)$ is cyclic or dihedral. In the first case, as noted in corollary 4.5, any lifting of $\overline{\rho}|_{D_p}$ is cyclic. Moreover, have $m(p) = 1$ because if D_p is cyclic, so is I_p and so it's clear that the subspace of $\mathbb{C}^2$ pointwise fixed by I_p is exactly the one fixed by a generator of I_p and so it must be 1-dimensional.

4.2 Representations with prime conductor

In this section, we will describe a classification of the irreducible representations with prime conductor.

4.2.1 Dihedral representations

Recall that the dihedral group of order $2n$ can be presented as

$$D_{2n} = \langle r, s\colon r^n = s^2 = 1 \;\; srs = r^{-1}\rangle$$

Every element of $x \in D_{2n}$ can be written uniquely as $x = s^i r^k$ where $i \in \{0, 1\}$ and $k \in \{0, \dots, n-1\}$. If $i = 0$, then $x \in C_n$, a cyclic subgroup of order n. If $n \geq 3$, C_n is unique, while D_4 contains three distinct subgroups of order 2. Observe that the relation $srs = r^{-1}$ implies that $sr^k s = r^{-k}$ for all $k \in \{0, \dots, n-1\}$.
If n is even, there are precisely 4 nonisomorphic 1-dimensional representations of D_{2n}. One can define them setting $\rho(r) = \pm 1$ and $\rho(s) = \pm 1$ in all possible ways.
Now let $w = e^{2\pi i/n}$ and for $h \in \mathbb{N}$ set

$$\rho^h(r^k) = \begin{pmatrix} w^{hk} & 0 \\ 0 & w^{-hk} \end{pmatrix} \qquad \rho^h(sr^k) = \begin{pmatrix} 0 & w^{-hk} \\ w^{hk} & 0 \end{pmatrix}$$

It can be checked that this defines a 2-dimensional representation. If $h = 0, n/2$, the representation ρ^h is reducible, since by conjugating by the matrix $\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$

it becomes diagonal. The representation ρ^h depends only on h mod n, so ρ^h and ρ^{n-h} are isomorphic for every $0 < h < n$. On the other hand, if $0 < h < n/2$ then ρ^h is irreducible, because the only 1-dimensional subspaces of $\mathbb{C}^2$ stable under the action of $\rho^h(r)$ are the coordinate axes, since $w^h \neq w^{-h}$, but those lines are not stable under $\rho^h(s)$. Now it is enough to note that the character χ_h of ρ^h is given by

$$\chi_h(r^k) = w^k + w^{-k} = 2\cos\left(\frac{2\pi hk}{n}\right)$$

$$\chi_h(sr^k) = 0$$

to see that if $0 < h, l < n/2$ then ρ^h and ρ^l are not isomorphic. We have thus found all irreducible representations (up to isomorphism) of D_{2n} for n even, because the sum of the squares of their degrees is $4 \cdot 1 + (n/2 - 1) \cdot 4 = 2n$.
If n is odd, there are just 2 irreducible representations of D_{2n} of degree 1. The nontrivial one is defined by mapping $r^k \mapsto 1$ and $sr^k \mapsto -1$ for all k. The representations ρ^h defined above remain valid in the case n odd; note just that $h < n/2$ can be written as $h < (n-1)/2$. Therefore the sum of the squares of the degrees of all these representations is $2 \cdot 1 + \frac{1}{2}(n-1) \cdot 4 = 2n$, and this means that we have found again all irreducible representations up to isomorphism.
Now suppose we have a dihedral representation of $G_{\mathbb{Q}}$, i.e. a Galois representation $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$ such that $\overline{\rho}(G_{\mathbb{Q}}) \cong D_{2n}$ for some $n \in \mathbb{N}$, $n \geq 2$. Set $E := \overline{\mathbb{Q}}^{\ker \overline{\rho}}$ and write C_n for the unique cyclic subgroup of D_{2n} of order n. The composition

$$\omega\colon G_{\mathbb{Q}} \xrightarrow{\overline{\rho}} \overline{\rho}(G_{\mathbb{Q}}) \to D_{2n}/C_n \cong \{\pm 1\} \leq \mathbb{C}^*$$

is a 1-dimensional representation of $G_{\mathbb{Q}}$ and it corresponds to some quadratic extension $K/\mathbb{Q}$. Now set $G_K := \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ and $G_E := \mathrm{Gal}(\overline{\mathbb{Q}}/E)$, so that $D_{2n} \cong \mathrm{Gal}(E/\mathbb{Q})$. By construction $\overline{\rho}(G_K) \cong C_n$ and so $\rho|_{G_K}$ is reducible, thus up to isomorphism we can write

$$\overline{\rho}|_{G_K}\colon G_K \to \mathrm{GL}_2(\mathbb{C})$$

$$\gamma \mapsto \begin{pmatrix} \chi(\gamma) & 0 \\ 0 & \chi'(\gamma) \end{pmatrix}$$

for some 1-dimensional representations χ, χ' of G_K. Now take $\gamma \in G_K$ and suppose, using the same notation as above, that $[\gamma] = r^k$ in the quotient group $G_K/G_E \cong C_n$. Then we must have $\chi(\gamma) \cdot \chi'(\gamma) = 1$, namely $\chi'(\gamma) = \chi(\gamma^{-1})$. Noting that for every $m \in \{0, \ldots, n\}$ one has $(sr^m)r^k(sr^m)^{-1} = r^{-k}$, it follows that $\chi'(\gamma) = \chi_\sigma(\gamma)$, where $\sigma \in G_{\mathbb{Q}} \setminus G_K$ and $\chi_\sigma(\gamma) := \chi(\sigma\gamma\sigma^{-1})$. Moreover, if we look at χ as a character of $\mathrm{Gal}(E/K)$ and we construct the induced representation, we find immediately that the representation of $\mathrm{Gal}(E/\mathbb{Q})$ induced by $\overline{\rho}$ by the quotient over $\ker\overline{\rho}$ is isomorphic to $\mathrm{Ind}_{C_n}^{D_{2n}} \chi$.
We want now show that the converse of this fact holds too. In order to do this, we have to introduce the transfer homomorphism. Let G be any group, let $H \leq G$ be a subgroup of finite index. Let $\vartheta\colon G/H \to G$ be a system of representatives for the left cosets of H in G. Given $s \in G$ and $t \in G/H$, we define an element $a_{s,t} \in H$ via the formula

$$s\vartheta(t) = \vartheta(st)a_{s,t}$$

where we write st for $\pi(s)t$, with $\pi\colon G \to G/H$ the projection onto the quotient. The element $a_{s,t}$ exists because clearly $s\vartheta(t)$ and $\vartheta(st)$ lie in the same coset.

Definition 4.10. Let $\overline{s} \in G^{ab}$ and $s \in G$ be any lifting of $\overline{s}$. The image in H^{ab} of the element $\prod_{t \in G/H} a_{s,t}$ is called the *transfer* of $\overline{s}$.

One can show that the definition is well-posed and that this correspondence is an homomorphism $\mathrm{Ver}\colon G^{ab} \to H^{ab}$.

Proposition 4.11. Let G be a finite group and $H \leq G$ a subgroup. Let χ be a character of H and χ^* the induced character on G. For $s \in G$, let $\varepsilon_{G/H}(s)$ be the signature of the permutation of G/H induced by multiplication by s. Then

$$\det_{\chi^*}(s) = \varepsilon_{G/H}(s)^{\chi(1)} \det_{\chi}(\mathrm{Ver}(s))$$

Proof. Let V be the complex vector space that corresponds to the representation χ^* and $W \subseteq V$ be the subspace invariant by H that corresponds to χ. If $\vartheta\colon G/H \to G$ is a a set of representatives for the left cosets of H in G and $W_\sigma \coloneqq \vartheta(\sigma)W$ for any $\sigma \in G/H$, then we have a decomposition of vector spaces $V = \bigoplus_{\sigma \in G/H} W_\sigma$. We have to find the determinant of the endomorphism $x \mapsto sx$ of V for every $s \in G$. Write $x = \sum_{\sigma \in G/H} \vartheta(\sigma)x_\sigma$ with $x_\sigma \in W_\sigma$. Then

$$sx = \sum_{\sigma \in G/H} s\vartheta(\sigma)x_\sigma = \sum_{\sigma \in G/H} \vartheta(s\sigma)a_{s,\sigma}x_\sigma$$

This shows that the map $x \mapsto sx$ is the composition of the maps v and u, where

$$\begin{aligned} u\colon V &\to V \\ \sum \vartheta(\sigma)x_\sigma &\mapsto \sum \vartheta(\sigma)a_{s,\sigma}x_\sigma \end{aligned}$$

and

$$\begin{aligned} v\colon V &\to V \\ \sum \vartheta(\sigma)x_\sigma &\mapsto \sum \vartheta(s\sigma)\vartheta(\sigma)^{-1}x_\sigma \end{aligned}$$

Since u maps W_σ to itself, we have

$$\det_V(u) = \prod_{\sigma \in G/H} \det_{W_\sigma}(u|_{W_\sigma}) = \prod_{\sigma \in G/H} \det_W(x \mapsto a_{s,\sigma}x) = \det_W(x \mapsto \prod_\sigma a_{s,\sigma}x) = \det_\chi(\mathrm{Ver}(s))$$

Now let $\{e_i\}_{i=1,\ldots,\chi(1)}$ be a basis of W. Then $\{\vartheta(\sigma)e_i\}$ for $\sigma \in G/H$, $i = 1, \ldots, \chi(1)$ is a basis of V. By constuction, for each i the map v maps $\vartheta(\sigma)W$ onto $\vartheta(s\sigma)W$ and so it permutes the $\vartheta(\sigma)e_i$. The signature of such a permutation is $\varepsilon_{G/H}(s)$. Since there are $\chi(1)$ indices i, the claim follows. □

Proposition 4.12. The following diagram commutes

$$\begin{array}{ccc} \mathrm{Gal}(\overline{\mathbb{Q}}/K)^{ab} & \xrightarrow{\mathrm{Ver}} & \mathrm{Gal}(\overline{\mathbb{Q}}/E)^{ab} \\ \uparrow & & \uparrow \\ I_K & \xrightarrow{\quad i \quad} & I_E \end{array}$$

where E/K is an extension of number fields, I_K and I_E are the idèle class groups, the vertical maps are the Artin maps and i is the inclusion.

Proof. See [Ser79]. □

Now suppose that we have a quadratic number field K which corresponds to a character ω of $G_{\mathbb{Q}}$ and a 1-dimensional linear representation $\chi\colon G_K \to \mathbb{C}^*$. Let ρ be the representation of $G_{\mathbb{Q}}$ induced by χ and let $\sigma \in G_{\mathbb{Q}}$ such that its image in $\mathrm{Gal}(K/\mathbb{Q})$ generates that group. Let χ_σ be as above. Finally, let $\mathfrak{m}$ be the conductor of χ and d_K be the discriminant of K.

Proposition 4.13.

a) The following are equivalent:

  i) ρ is irreducible;
  ii) ρ is dihedral;
  iii) $\chi \neq \chi_\sigma$.

b) The conductor of ρ is $|d_K| \cdot N_{K/\mathbb{Q}}(\mathfrak{m})$.

c) ρ is odd if and only if one of the following holds:

  i) K is imaginary;
  ii) K is real and χ has signature $(+,-)$ at infinity, namely if $c, c' \in G_K$ are Frobenius elements at the two real places of K then $\chi(c) \neq \chi(c')$.

d) If $\overline{\rho}(G_{\mathbb{Q}}) = D_{2n}$, then n is the order of $\chi^{-1}\chi_\sigma$.

Proof.
a) Since $\rho|_{G_K}$ is reducible, $\overline{\rho}(G_K)$ is cyclic. This means that $\overline{\rho}(G_{\mathbb{Q}})$ has a cyclic subgroup of index ≥ 2, and by theorem 4.4 it follows that $\overline{\rho}(G_{\mathbb{Q}})$ is either cyclic or dihedral, so the equivalence of i) and ii) is clear by corollary 4.5. The equivalence of i) and iii) follows from theorem A.23.
b) This follows immediately from theorem 2.42
c) By proposition 4.11, the determinant of ρ is given by

$$\det(\rho) = \omega\chi_{\mathbb{Q}}$$

where $\chi_{\mathbb{Q}} = \chi \circ \mathrm{Ver}_{K/\mathbb{Q}}$ and $\mathrm{Ver}_{K/\mathbb{Q}}\colon G_{\mathbb{Q}}^{ab} \to \mathrm{Gal}(\overline{\mathbb{Q}}/K)^{ab}$ is the transfer map. By proposition 4.12, $\chi_{\mathbb{Q}}$ as an idèle class character is just the restriction of χ to the idèle class group of $\mathbb{Q}$. Now, ω is odd if and only if K is imaginary. If v is the archimedean place of K, then $K_v \cong \mathbb{C}$ and so necessarily $\chi|_{K_v^*}$ is trivial because $\mathbb{C}^*$ is connected. Thus that $\chi_{\mathbb{Q}}$ is even. If K is real, ω is even. Let v_1, v_2 be the two real places of K, so that $K_{v_1} \cong K_{v_2} \cong \mathbb{R}$. Since $\mathbb{R}^*$ has two connected components $\det(\rho)$ is odd if and only if the signature of χ is $(+,-)$.
d) We have that $C_n = \overline{\rho}(G_K)$ and $\overline{\rho}|_{G_K}$ is given by

$$\gamma \mapsto \begin{pmatrix} \chi(\gamma) & 0 \\ 0 & \chi_\sigma(\gamma) \end{pmatrix} \equiv \begin{pmatrix} \chi(\gamma)\chi_\sigma^{-1}(\gamma) & 0 \\ 0 & 1 \end{pmatrix} \bmod \mathbb{C}^*$$

so the claim is clear. □

One can prove (see [Ser77b]) that representations induced from characters of real quadratic fields cannot have prime conductor.
The first consequence of the theorem is that to have a dihedral representation

of prime conductor we must have $p \equiv 3 \bmod 4$ because otherwise d_K cannot be prime. In such case, dihedral Galois representations with prime conductor p are exactly the ones induced from unramified characters of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ where $K = \mathbb{Q}(\sqrt{-p})$. Unramified characters can be viewed as characters of the ideal class group of K, so we can count dihedral representations by counting characters of the ideal class group. Let Cl_K be the ideal class group of K and h be its class number. Recall that if $p \equiv 3 \bmod 4$ then h is odd. Let H be the Hilbert class field of K, so that $\mathrm{Gal}(H/K) \cong \mathrm{Cl}_K$. Now note that since $[K\colon \mathbb{Q}] = 2$, for every ideal $I \subseteq \mathcal{O}_K$, the ideal $I \cdot I^\sigma$ is principal in $\mathcal{O}_K$. So if we look at χ as a character of Cl_K, we have that $\chi(I \cdot I^\sigma) = 1$, so $\chi(I^\sigma) = \chi(I)^{-1}$. On the other hand, let φ be the isomorphism between Cl_K and $\mathrm{Gal}(H/K)$. Then φ takes I^σ to $\sigma\varphi(I)\sigma^{-1}$ and hence $\chi(I)^{-1} = \chi_\sigma(I)$. This tells us that $\chi(I)\chi_\sigma(I) = 1$ and we can conclude that $\chi = \chi_\sigma$ if and only if $\chi^2 = 1$. As h is odd this cannot happen if χ is nontrivial. So we have showed that for any nontrivial character of $\mathrm{Gal}(H/K)$ the induced representation of $\mathrm{Gal}(H/\mathbb{Q})$ is dihedral and irreducible. Now let χ, χ' two characters of $\mathrm{Gal}(H/\mathbb{Q})$. Then the representations induced by χ and χ' are isomorphic if and only if $\chi' = \chi^{-1}$. Therefore, there are $\frac{1}{2}(h-1)$ nonisomorphic dihedral representations with conductor p.
To sum up, we have found that any dihedral representation of prime conductor p must be such that:

a) $p \equiv 3 \bmod 4$;

b) $\rho = \mathrm{Ind}_{K/\mathbb{Q}}(\chi)$ where $K = \mathbb{Q}(\sqrt{-p})$ and χ is an unramified character of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$;

c) $\det(\rho)$ is the Legendre symbol modulo p.

So starting from such a representation, the associated Artin L-function is defined as

$$L(s,\chi) = L(s,\rho) = \prod_{\mathfrak{p} \subseteq \mathcal{O}_K} (1 - \chi(\mathrm{Frob}_\mathfrak{p}) N(\mathfrak{p})^{-s})^{-1}$$

where $\mathfrak{p}$ runs over all prime ideals of $\mathcal{O}_K$ and the first equality comes from the fact that the L-functions attached to χ and to $\mathrm{Ind}\,\chi$ are equal for every representation χ. Regarding χ as a character of $\mathcal{O}_K$ we can write

$$L(s,\rho) = \prod_{\mathfrak{p} \subseteq \mathcal{O}_K} (1 - \chi(\mathfrak{p}) N(\mathfrak{p})^{-s})^{-1} = \sum_{I \subseteq \mathcal{O}_K} \chi(I) N(I)^{-s}$$

where I runs over all ideals of $\mathcal{O}_K$. Such Dirichlet series must correspond, by theorem 3.13, to the newform

$$f = \sum_{I \subseteq \mathcal{O}_K} \chi(I) q^{N(I)}$$

Looking at tables of quadratic fields, it turns out that the first nontrivial example is $p = 23$. In this case, $h = 3$, so there is exactly 1 normalized cuspform of dihedral type. The Hilbert class field H of $\mathbb{Q}(\sqrt{-23})$ is generated by the roots of $x^3 - x - 1 = 0$ and $\mathrm{Gal}(H/\mathbb{Q}) \cong D_6$. The corresponding newform is given by $f = \dfrac{1}{2}(\theta_1 - \theta_2)$ where

$$\theta_1 = \sum_{m,n \in \mathbb{Z}} q^{m^2+mn+6n^2} \quad \theta_2 = \sum_{m,n \in \mathbb{Z}} q^{2m^2+mn+3n^2}$$

or

$$f = q \cdot \prod_{n=1}^{+\infty} (1 - q^n)(1 - q^{23n}) = \eta(z)\eta(23z)$$

4.2.2 Non-dihedral representations

Theorem 4.14. Let $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$ an irreducible Galois representation with prime conductor p such that $\varepsilon = \det(\rho)$ is odd. Suppose ρ is not dihedral. then

a) $p \neq 1 \bmod 8$;

b) if $p \equiv 5 \bmod 8$ then ρ of type S_4 and ε has order 4 and conductor p;

c) if $p \equiv 3 \bmod 4$ then ρ is of type S_4 or A_5 and ε is the Legendre symbol modulo p;

Proof. The conductor of ε divides p and since ε is odd, it is not trivial and therefore its conductor is exactly p. Let $I_p \subseteq G_{\mathbb{Q}}$ be the inertia group above p. Since the conductor of ρ is exactly p, ρ is tamely ramified at p and therefore $\rho(I_p)$ is cyclic. So up to isomorphism we can write $\rho|_{I_p} = \psi \oplus \mathbb{1}$ for some 1-dimensional representation of I_p. Hence the natural homomorphisms

$$\rho(I_p) \to \varepsilon(I_p) \quad \text{and} \quad \rho(I_p) \to \overline{\rho}(I_p)$$

are isomorphisms. Since ε is ramified only at p, we have that $\varepsilon(I_p) = \varepsilon(G_{\mathbb{Q}})$ and this group is cyclic of even order since p is odd. Since it is a subgroup of A_4, S_4 or A_5, this order has to be 2 or 4. On the other hand, ε has conductor p and so it can be viewed as a character of $(\mathbb{Z}/p\mathbb{Z})^*$. The fact that $\varepsilon(-1) = -1$ implies that ε is faithful on the 2-primary component of $(\mathbb{Z}/p\mathbb{Z})^*$. Therefore we cannot have $p \equiv 1$ mod 8 because in this case the order of ε would be ≥ 8. If $p \equiv 5$ mod 8 ε has order 4 and since A_4 and A_5 have no elements of order 4, ρ is of type S_4. Now suppose $p \equiv 3$ mod 4. Then ε has order 2 and so it is the Legendre symbol. If ρ were of type A_4, then the image of I_p under the map

$$I_p \xrightarrow{\overline{\rho}} A_4 \to C_3$$

would be trivial (recall that A_4 has a normal subgroup isomorphic to D_4). So the kernel of the Galois representation

$$G_{\mathbb{Q}} \xrightarrow{\rho} A_4 \to C_3$$

would correspond to an everywhere unramified cubic field, impossible. Hence ρ is of type S_4 or A_5. □

One can show that the converse of this theorem holds, in the following sense. Start with a Galois extension $E/\mathbb{Q}$, a prime number p and consider the following cases

a) $\mathrm{Gal}(E/\mathbb{Q}) \cong S_4$ and $p \equiv 5$ mod 8;

b) $\mathrm{Gal}(E/\mathbb{Q}) \cong S_4$ and $p \equiv 3$ mod 4;

c) $\mathrm{Gal}(E/\mathbb{Q}) \cong A_5$ and $p \equiv 3$ mod 4;

Any embedding of $\mathrm{Gal}(E/\mathbb{Q})$ into $\mathrm{PGL}_2(\mathbb{C})$ defines, via composition with the projection onto the quotient, a projective Galois representation $\overline{\rho}_E$ of $G_{\mathbb{Q}}$. In cases a) and b) $\overline{\rho}_E$ is essentially unique because any two embeddings of S_4 into $\mathrm{PGL}_2(\mathbb{C})$ are conjugate, while in case c) there are two conjugacy classes of embeddings of A_5 in $\mathrm{PGL}_2(\mathbb{C})$.

Theorem 4.15. The projective representation $\overline{\rho}_E$ defined as above has a lifting with conductor p and odd determinant if and only if:

a) E is the normal closure of a nonreal quartic number field E_4 with discriminant p^3;

b) E is the normal closure of a quartic number field E_4 with discriminant $-p$;

c) E is the normal closure of a nonreal quintic field E_5 with discriminant p^2.

In each of those cases, $\overline{\rho}_E$ has precisely two nonisomorphic liftings with odd determinant and conductor p. If one of these is ρ, the other one is $\rho \otimes \det(\rho)$.

Proof. See [Ser77b]. □

To conclude, we have that in the case where $p \equiv 3 \bmod 4$ and χ is the Legendre symbol mod p, the space $S_1^+(N, \chi)$ has dimension $\frac{1}{2}(h-1) + 2s + 4a$, where h is the class number of $\mathbb{Q}(\sqrt{-p})$, s is the number of nonisomorphic quartic fields with discriminant $-p$ and a is the number of nonisomorphic quintic fields with discriminant p^2.

Appendix A

Representations of finite groups

We will state here some of the basic results about (linear) representations of finite groups. From now on, G will denote a finite group of order g.

Definition A.1. Let $n \in \mathbb{N}$ and K be any field. A *linear representation of degree* n *of* G is a homomorphism

$$\rho\colon G \to \mathrm{GL}_n(K)$$

or equivalently a $K[G]$-module which is also an n-dimensional K-vector space.
Two representations $\rho, \rho'\colon G \to \mathrm{GL}_n(K)$ are *isomorphic* if there exists $M \in \mathrm{GL}_n(K)$ s.t. $M^{-1}\rho(\sigma)M = \rho'(\sigma)$ for all $\sigma \in G$, or equivalently V, V' are two isomorphic representations if there exists a K-linear isomorphism $f\colon V \to V'$ s.t. $f(v^\sigma) = f(v)^\sigma$ for all $v \in V$, $\sigma \in G$.

In what follows, we will always assume $K = \mathbb{C}$, even if most of the result are still valid over any field of characteristic 0.
Let V be a complex vector space of dimension g with a basis $\{e_\tau\}_{\tau \in G}$. The *regular representation* of G is defined as follows: for every $\sigma \in G$, we set $e_\tau^\sigma \coloneqq e_{\sigma\tau}$.
Note that for every $\sigma \in G$, one has $e_\sigma = e_{1_G}^\sigma$. Hence the images of e_{1_G} under the action of the elements of G form a basis of V. Conversely, suppose that W is a complex representation of G such that there exists a vector $w \in W$ such that $\{w^\sigma\}_{\sigma \in G}$ is a basis of W. Then W is isomorphic to the regular representation, via the isomorphism

$$V \to W$$

$$e_\sigma \mapsto w^\sigma$$

Let $\rho\colon G \to \mathrm{Aut}(V)$ be a representation. A linear subspace $W \subseteq V$ is said to be *stable* under G if for all $x \in W$, $\rho(\sigma)x \in W$ for all $\sigma \in G$. In this case we have a representation

$$\rho^W\colon G \to \mathrm{Aut}(W)$$

which is called *subrepresentation* of G.

Definition A.2. A representation $\rho\colon G \to \mathrm{Aut}(V)$ is said to be *irreducible* if $V \neq 0$ and $0, V$ are the only stable subspaces.

This definition remains valid also for representations of infinite groups.

Theorem A.3. Let V be a vector space over a field of characteristic zero. Let $\rho\colon G \to \mathrm{Aut}(V)$ be a representation of a finite group G and let $W \subseteq V$ be a subspace stable under the action of G. Then there exist a complement W^0 of W that is stable under the action of G.

Proof. See [Ser77a] □

As a consequence of this theorem, we have the following fundamental

Theorem A.4. Every representation of a finite group G into $\mathrm{GL}_n(K)$ with $\operatorname{char} K = 0$ is isomorphic to a direct sum of irreducible representations.

Proof. Induction on $\dim V$. □

Definition A.5. A representation $\rho\colon G \to \mathrm{Aut}(V)$ is said to be *semisimple* if it is isomorphic to a direct sum of irreducible representations.

A.1 Character theory

Definition A.6. Let $\rho\colon G \to \mathrm{GL}_n(\mathbb{C})$ a complex representation of G. The *character* of ρ is the map given by

$$\chi\colon G \to \mathbb{C}$$

$$\sigma \mapsto \mathrm{Tr}(\rho(\sigma))$$

The *determinant* of ρ is the 1-dimensional representation given by

$$\det\colon G \to \mathbb{C}^*$$

$$\sigma \mapsto \det(\rho(\sigma))$$

Remarks A.7.

1) Obviously, both character and determinant are invariant under isomorphism since they are two of the coefficients of the characteristic polynomial of $\rho(\sigma)$ for any $\sigma \in G$. When we deal with 2-dimensional representations, they are all the coefficients of the characteristic polynomial.

2) Suppose χ is the character of a complex representation $\rho\colon G \to \mathrm{GL}_n(\mathbb{C})$. Then

   a) $\chi(1) = n$;
   b) $\chi(\sigma^{-1}) = \overline{\chi(\sigma)}$ for all $\sigma \in G$;
   c) $\chi(\tau\sigma\tau^{-1}) = \chi(\sigma)$ for all $\sigma, \tau \in G$.

   In fact, a) is obvious. For b), since any $\sigma \in G$ has finite order, the same is true for the eigenvalues $\lambda_1, \ldots, \lambda_n$ of $\rho(\sigma)$ and therefore they all have absolute value 1. Hence

$$\overline{\chi(\sigma)} = \overline{\mathrm{Tr}(\rho(\sigma))} = \overline{\sum_i \lambda_i} = \sum_i \lambda_i^{-1} = \mathrm{Tr}(\rho(\sigma)^{-1}) = \mathrm{Tr}(\rho(\sigma^{-1})) = \chi(\sigma^{-1})$$

   Point c), setting $u = \tau\sigma$ and $v = \tau^{-1}$ can be restated as $\chi(vu) = \chi(uv)$, which is true by the well-known fact that $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$ for all $A, B \in \mathrm{GL}_n(\mathbb{C})$.

3) If $\rho_1 \colon G \to \mathrm{Aut}(V_1)$ and $\rho_2 \colon G \to \mathrm{Aut}(V_2)$ are complex representations with characters χ_1, χ_2, then

   a) the character of the representation $\rho_1 \oplus \rho_2$ is given by $\chi_1 + \chi_2$;

   b) the character of the representation $\rho_1 \otimes \rho_2$ is given by $\chi_1\chi_2$.

One of the crucial results which we are going to prove is that the character of a complex representation of a finite group completely determines the representation itself.[1]

Definition A.8. Let $\phi, \psi \colon G \to \mathbb{C}$ be any two complex-valued functions. Set

$$(\phi, \psi) \coloneqq \frac{1}{g} \sum_{\sigma \in G} \phi(\sigma)\overline{\psi(\sigma)}$$

This is an Hermitian scalar product: it is linear in ϕ, antilinear in ψ and $(\phi, \phi) > 0$ for all $\phi \neq 0$.

Theorem A.9. Let χ be the character of an irreducible representation ρ of G. Then

i) $(\chi, \chi) = 1$;

ii) if χ' is the character of an irreducible representation nonisomorphic to ρ, then

$$(\chi, \chi') = 0$$

i.e. χ, χ' are orthogonal.

Proof. See [Ser77a]. □

Recall that a *class function* on G is a function $f \colon G \to \mathbb{C}$ s.t. $f(\sigma) = f(\tau^{-1}\sigma\tau)$ for all $\sigma, \tau \in G$, i.e. f is defined on the set of conjugacy classes of G.
The set of class functions on G has a structure of complex vector space in an obvious way. By remark A.7, we see that the character of a representation is a class function. Moreover, we have the following fundamental

Theorem A.10. The set of characters of the irreducible representations of G is an orthonormal basis for the vector space of class functions. Such a space has dimension equal to the number of conjugacy classes in G. Moreover, a linear combination of irreducible characters is the character of a representation of G if and only if the coefficients are all nonnegative integers.

Proof. See [Ser77a]. □

Corollary A.11. Every finite group has a finite number of nonisomorphic irreducible representations.

Theorem A.12. Let $\rho \colon G \to \mathrm{Aut}(V)$ be a complex representation. Suppose that V decomposes into a direct sum of irreducible representations

$$V = W_1 \oplus W_2 \oplus \cdots \oplus W_k$$

Then if $W \subseteq V$ is an irreducible representation of G with character χ, the number of W_i isomorphic to W is equal to the scalar product (ϕ, χ).

[1] This result remains true for representations over any field of characteristic 0. In characteristic p, we need the whole characteristic polynomial to recover the representation.

Proof. By remark A.7, $\phi = \chi_1 + \chi_2 + \cdots + \chi_k$ where χ_i is the character of W_i. Therefore by theorem A.12, using the fact that

$$(\phi, \chi) = \sum_{i=1}^{k} (\phi, \chi_i)$$

the result follows. □

Corollary A.13. Two representations with the same character are isomorphic.

Proof. By the previous theorem they contain each given irreducible representation the same number of times, and so the claim is clear. □

Now suppose we have a representation V with character ϕ of G. Call $W_1, \dots, W_h$ the nonisomorphic irreducible representations of G with characters $\chi_1, \dots, \chi_h$. Then we can write

$$V = m_1 W_1 \oplus \cdots \oplus m_h W_h$$

where the m_i are nonnegative integers. Now we know that $m_i = (\phi, \chi_i)$ by the orthogonality relations and for the same reason $(\phi, \phi) = \sum_{i=1}^{h} m_i^2$. These observations imply very easily the following

Theorem A.14. For every character χ, (χ, χ) is a nonnegative integer and $(\phi, \phi) = 1$ iff ϕ is an irreducible character.

Let V be the regular representation of G. Recall that for a basis $\{e_\tau\}_{\tau \in G}$ of V we have $e_\tau^\sigma = e_{\sigma\tau}$. If $\rho \colon G \to \mathrm{GL}_g(\mathbb{C})$ is the homomorphism that describes the representation in the basis $\{e_\tau\}$, the fact that for every $\sigma \neq 1_G$ we have $\sigma\tau \neq \tau$ implies that $\mathrm{Tr}(\rho(\sigma)) = 0$ if $\sigma \neq 1_G$. On the other hand, as we already said $\mathrm{Tr}(\rho(1_G)) = g$. Thus we have determined the character of ρ, namely

$$\chi(\sigma) = \begin{cases} 0 & \text{if } \sigma \neq 1_G \\ g & \text{if } \sigma = 1_G \end{cases}$$

Therefore we have the following

Lemma A.15.

i) Every irreducible representation of G is contained in the regular representation with multiplicity equal to its degree.

ii) If $n_1, \dots, n_h$ are the degrees of the irreducible representations of G, we have $\sum_{i=1}^{h} n_i^2 = g$.

iii) For $1_G \neq \sigma \in G$ we have $\sum_{i=1}^{h} n_i \chi_i(\sigma) = 0$.

Proof.
i) Let r_G be the character of the regular representation. If W_i is an irreducible representation of G with character χ_i and degree n_i, by theorem A.12 its multiplicity is the scalar product (r_G, χ_i), namely

$$(r_G, \chi_i) = \frac{1}{g} \sum_{\sigma \in G} r_G(\sigma^{-1})\chi_i(\sigma) = \frac{1}{g} \cdot g\chi_i(1_G) = n_i$$

ii),iii) By i) we have $r_G(\sigma) = \sum_{i=1}^{h} n_i \chi_i(\sigma)$. For $\sigma = 1_G$ we get ii) and for $\sigma \neq 1_G$ we get iii). □

Corollary A.16. G is abelian if and only if it has exactly g nonisomorphic irreducible representations, each of them of degree 1.

Proof. Since G is abelian, its order is equal to the number of conjugacy classes, namely $g = h$. Now apply the previous theorem and get the claim. □

Definition A.17. The *unit representation* of G is given by $V = \mathbb{C}$ and $v^\sigma = v$ for all $\sigma \in G$, $v \in V$. Its character is denoted by $\mathbb{1}_G$. This representation is clearly irreducible, and therefore it embeds in the regular representation. The quotient is called the *augmentation representation* and its character u_G is s.t. $r_G = u_G + \mathbb{1}_G$.

A.2 Induced representations

Let $H \leq G$ be any subgroup. It's clear that any representation of G gives rise by restriction to a representation of H. The other way round is more complicated. We now describe a particular construction of a representation of G starting from representations of H. Suppose that V is a representation of G and that $W \subseteq V$ is an H-stable subspace of V. For any $\sigma \in G$, the subspace W^σ depends only on the left coset of H in G, since for any $\delta \in H$ one has

$$W^\sigma = (W^\delta)^\sigma = W^{\sigma\delta}$$

Therefore if $H = H_1, \ldots, H_m$ are the left cosets of H in G it makes sense to define for each H_i a subspace $W_i := W^\tau$ where $\tau \in H_i$. The elements of G permute those subspaces, namely for any $\sigma \in G$ one has $W_i^\sigma = W_j$ for some $j \in \{1, \ldots, m\}$. Moreover, $W_i \cap W_j = \{0\}$ if $i \neq j$ because if $\sigma w = \tau w$ for some $\sigma, \tau \in G$ and $w \in W$, then $w = \sigma^{-1}\tau w$ and so $\sigma^{-1}\tau \in H_1 = H$, namely $\sigma H = \tau H$. Thus we can define a representation of G by setting

$$\operatorname{Ind}_H^G(W) := \bigoplus_{i=1}^{m} W_i$$

Definition A.18. We say that the representation ρ of G in V is *induced* by the representation θ of H in $W \subseteq V$ if $V = \operatorname{Ind}_H^G(W)$.

In such a case we have that $\dim V = \sum_{i=1}^{m} \dim(W_i) = (G\colon H) \dim W$ and so $\dim W \mid \dim V$.

Recall that giving a representation ρ of G is the same as giving a $\mathbb{C}[G]$-module V. It's not hard to show that V is induced from a $\mathbb{C}[H]$-module W if and only if the natural map $\mathbb{C}[G] \otimes_{\mathbb{C}[H]} W \to V$ is an isomorphism. Moreover, with this fact one can easily check that induction is transitive, i.e. if $H \leq K \leq G$, then $\mathrm{Ind}_H^G(W) \cong \mathrm{Ind}_K^G(\mathrm{Ind}_H^K(W))$.

Example A.19. The regular representation V of G is induced by the regular representation of any of its subgroups. Indeed, if $\{e_\tau\}_{\tau \in G}$ is a basis of V s.t. $e_\tau^\sigma = e_{\sigma\tau}$ and $H \leq G$, then $\{e_\delta\}_{\delta \in H}$ generates a subrepresentation $W \subseteq V$, which is the regular representation of H. It's then straightforward to check that V is induced by W.

Starting from a representation of a subgroup H of G, we can recover a unique representation of G:

Theorem A.20. Let $H \leq G$ be a subgroup and let $\vartheta\colon H \to \mathrm{Aut}(W)$ be a representation of H. Then there exists a unique (up to isomorphism) representation $\rho\colon G \to \mathrm{Aut}(V)$ s.t. ρ is induced by ϑ.

Proof. See [Ser77a]. □

Such a theorem suggests us the possibility to calculate the character of a representation of G which is induced by a representation of H just by the character of H. In fact, this is possible.

Theorem A.21. Let $H \leq G$ be a subgroup of order h and R a system of representatives of H in G. For every $\sigma \in G$ we have

$$\chi_\rho(\sigma) = \sum_{\substack{r \in R \\ r^{-1}\sigma r \in H}} \chi_\vartheta(r^{-1}\sigma r) = \frac{1}{h} \sum_{\substack{\tau \in G \\ \tau^{-1}\sigma\tau \in H}} \chi_\vartheta(\tau^{-1}\sigma\tau)$$

Proof. See [Ser77a]. □

Now, as we mentioned before, the set of irreducible characters on G is a basis for the complex vector space of class functions and a linear combination of irreducible characters is the character of a representation iff the coefficients are integers. Therefore if $\{\chi_1, \ldots, \chi_h\}$ are the irreducible characters of G it makes sense to introduce the following object:

$$R(G) := \mathbb{Z}\chi_1 \oplus \mathbb{Z}\chi_2 \oplus \cdots \oplus \mathbb{Z}\chi_h$$

which is a free finitely generated $\mathbb{Z}$-module but also a ring since a product of characters is again a character. Now if $H \leq G$, one has two homomorphism

$$\mathrm{Res}\colon R(G) \to R(H)$$

which sends a character of G to the character that corresponds to the representation of H obtained by restriction and

$$\mathrm{Ind}\colon R(H) \to R(G)$$

which sends the character of a representation of H to the character of the induced representation of G. Those two homomorphisms are adjoints, in the following sense

Theorem A.22 (Frobenius reciprocity)**.** For every characters ϕ of H and ψ of G we have

$$(\phi, \operatorname{Res} \psi)_H = (\operatorname{Ind} \phi, \psi)_G$$

This extends in an obvious way to any pair of class functions on G and H.

Moreover, one can check that

$$\operatorname{Ind}(\phi) \cdot \psi = \operatorname{Ind}(\phi \cdot \operatorname{Res}(\psi))$$

which implies that the image of $R(H)$ under Ind is an ideal of $R(G)$. The last important result concerning induced representations is the following one.

Theorem A.23 (Mackey's irreducibility criterion)**.** Let $H \leq G$, let $S \subseteq G$ be a system of representatives for the double cosets of H in G. Let $\rho\colon H \to \operatorname{Aut}(W)$ be a representation of H. For each $s \in S$, let $H_s := sHs^{-1}$ and define

$$\rho^s\colon H_s \to W$$

$$x \mapsto \rho(s^{-1}xs)$$

Then the representation $\operatorname{Ind}_H^G \rho$ is irreducible if and only if

i) ρ is irreducible;

ii) for every $s \in G \setminus H$ the representations ρ^s and $\operatorname{Res}_{H_s} \rho$ are disjoint, i.e. they have no irreducible components in common.

Proof. See [Ser77a]. □

Bibliography

[AM69] M.F. Atiyah and I.G. MacDonald. *Introduction to commutative algebra*. Westview Press, 1969.

[Apo76] T.M. Apostol. *Introduction to analytic number theory*. Springer-Verlag, 1976.

[CA67] J.W.S. Cassels and A.Frohlic. *Algebraic number theory*. Academic Press, 1967.

[Chi09] N. Childress. *Class field theory*. Springer, 2009.

[Del71] P. Deligne. Formes modulaires et représentations l-adiques. *Séminaire Bourbaki*, vol. 1968/69:139–172, 1971.

[DJ05] F. Diamond and J.Shurman. *A first course in modular forms*. Springer, 2005.

[DS74] P. Deligne and J.-P. Serre. Formes modulaires de poids 1. *Annales scientifiques de l'E.N.S.* 4^e *série*, 7:507–530, 1974.

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

[Mar77a] D. Marcus. *Number Fields*. Springer-Verlag, 1977.

[Mar77b] J. Martinet. Character theory and artin l-functions. *Algebraic Number Fields, ed A. Fröhlich, Proc. Symp. Durham 1975*, pages 1–87, 1977.

[Ran39] R.A. Rankin. Contributions to the theory of ramanujan's function $\tau(n)$ and similar arithmetical functions. *Proc. Cambridge Phil. Soc*, vol. 35:351–372, 1939.

[SD73] H.P.F. Swinnerton-Dyer. On l-adic reoresentations and congruences for coefficients of modular forms. *Springer Lecture Notes*, vol. 350:149–156, 1973.

[Ser72] J.-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math*, vol. 15:259–331, 1972.

[Ser77a] J.-P. Serre. *Linear representations of finite groups*. Springer, 1977.

[Ser77b] J.-P. Serre. Modular forms of weight one and galois representations. *Algebraic Number Fields, ed A. Fröhlich, Proc. Symp. Durham 1975*, pages 193–268, 1977.

[Ser79] J.-P. Serre. *Local Fields.* Springer-Verlag, 1979.

[Sha72] S. Shatz. *Profinite groups, arithmetic, and geometry.* Princeton University Press, 1972.

[Sil94] J.H. Silverman. *Advanced topics in the arithmetic of elliptic curves.* Springer-Verlag, 1994.

[Ste] W. Stein. A brief introduction to classical and adelic algebraic number theory. **http://modular.math.washington.edu/papers/**.