Modular Forms of Weight one

Jef Laga

Contents

Introduction

In 1974 Pierre Deligne and Jean-Pierre Serre published the paper [DS74], "Formes modulaires de poids 1", revealing a connection between modular forms of weight one and Galois representations. Given a newform f of level N and type $(1, \chi)$ they construct a continuous two-dimensional Galois representation

$$\rho_f : \mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{C})$$

whose Artin L-function equals the L-function of f. The purpose of this essay is to explain this result and the necessary background surrounding it, as well as giving some explicit examples. The use of L-functions is emphasized throughout, since they seem to provide a natural framework for this connection.

The material is presented as follows. The first chapter provides some additional background on modular forms of arbitrary level and explicit constructions of modular forms of weight one. The content is largely taken from [Iwa97] and [Miy06]. In the interest of space we assume the basic theory of modular forms as described in the first five chapters of [DS05]. The second chapter is on Galois representations. The concepts of Artin conductor and Artin L-function are carefully explained. The third chapter explains the Deligne-Serre construction and is at the heart of the essay. The fourth and final chapter gives explicit examples of newforms of weight one classified according to their projective image, using the theory of binary quadratic forms (dihedral type) and databases recently made available by Kevin Buzzard and Alan Lauder [BL]. Most of the dihedral examples are self-constructed, some are taken from [Ser75].

The first two chapters are meant to provide the necessary background for understanding chapter 3. The reader mainly interested in the Deligne-Serre construction may go straight to chapter 3, going back to the first two chapters to fill in the details where necessary.

Before we continue I would like to thank my supervisor Dr. Jack Thorne for his helpful suggestions and the interesting conversations.

Disclaimer

This essay might contain mathematical inaccuracies which are entirely due to the author; corrections can be sent to `jcsl@cam.ac.uk`.

Notation

For a finite set X, we denote its cardinality by $|X|$.

If $K/\mathbf{Q}$ is a quadratic extension with discriminant Δ, there is a unique non-trivial homomorphism $\mathrm{Gal}(K/\mathbf{Q}) \to \mathbf{C}^\times$. The associated Dirichlet character (via class field theory) is written χ_Δ and has conductor $|\Delta|$. For a prime p not dividing Δ, it is given by

$$\chi_\Delta(p) = \left(\frac{\Delta}{p}\right)$$

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol.

1. Modular Forms

In this chapter we discuss some additional topics in the classical theory of modular forms which are relevant to modular forms of weight one and Galois representations. We will give some explicit constructions of modular forms in various ways. We will assume basic concepts of modular forms on congruence subgroups and the theory of newforms. Details of the definitions and proofs can be found in [DS05].

Let $\mathcal{H} = \{z \mid \Im(z) > 0\}$ be the upper half plane and $f : \mathcal{H} \to \mathbf{C}$ a holomorphic function. For each $k \in \mathbf{Z}_{\geq 1}$ and $\alpha \in \mathrm{GL}_2(\mathbf{R})$ we define a function $f|[\alpha]_k : \mathcal{H} \to \mathbf{C}$ by

$$(f|[\alpha]_k)(z) = \det(\alpha)^{k-1}(cz+d)^{-k} f(\alpha(z)).$$

If $\Gamma \leq \mathrm{SL}_2(\mathbf{Z})$ is a congruence subgroup we write $M_k(\Gamma)$ for the space of modular forms on Γ and $S_k(\Gamma)$ for the subspace of cusp forms. If $\chi : (\mathbf{Z}/N\mathbf{Z})^\times \to \mathbf{C}^\times$ is a Dirichlet character mod N we write $M_k(N,\chi)$ (resp. $S_k(N,\chi)$) for the space of modular forms (resp. cusp forms) on $\Gamma_0(N)$ with character χ. For such f we will say its level is N and its type is (k,χ). Such modular forms will be the main object of study of this essay.

For a fixed level N, let $\mathbf{T} \subset \mathrm{End}(M_k(\Gamma_1(N)))$ be the $\mathbf{C}$-algebra generated be the Hecke operators T_p for all primes p. Let $\mathbf{T}_{(N)}$ be the subalgebra of $\mathbf{T}$ generated by the Hecke operators T_p for p not dividing N ('away from N'). We will often consider $\mathbf{T}$ and $\mathbf{T}_{(N)}$ as subalgebras of $\mathrm{End}(S_k(\Gamma_1(N))$ or $\mathrm{End}(M_k(N,\chi))$ for a character χ since they are $\mathbf{T}$-invariant subspaces of $M_k(\Gamma_1(N))$. We say $f \in M_k(\Gamma_1(N))$ is a $\mathbf{T}$-eigenform (resp. $\mathbf{T}_{(N)}$-eigenform) if f is an eigenform for the Hecke operators T_n for all $n \geq 1$ (resp. all n coprime to N). Note that the Diamond operators $\langle d\rangle : M_k(\Gamma_1(N)) \to M_k(\Gamma_1(N))$ for $(d,N) = 1$ are in $\mathbf{T}_{(N)}$ and $\mathbf{T}$ so every $\mathbf{T}_{(N)}$-eigenform has a nebentype χ.

1.1. L-functions, twisting, converse theorems

Central to the study of modular forms are their associated L-functions. An L-function is a Dirichlet series with an Euler product and a functional equation. In this section we examine some properties of these L-functions and state so-called converse theorems. We mostly follow chapter 7 of [Iwa97] and section 4.3 of [Miy06].

1.1.1. Functional Equation

Let $f \in S_k(N,\chi)$ be a cusp form. We write $W_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$. Define

$$g = f|_{\omega_N} = N^{1-k/2} f|[W_N]_k = (\sqrt{N}z)^{-k} f(-1/Nz).$$

Since $W_N\Gamma_1(N) = \Gamma_1(N)W_N$ we know that $g \in S_k(\Gamma_1(N), \bar{\chi})$ and the normalization is chosen such that $g|_{\omega_N} = (-1)^k f$. We can associate to f and g the L-functions

$$L(f,s) = \sum_{n\geq 1} a_n n^{-s} \tag{1.1}$$

$$L(g,s) = \sum_{n\geq 1} b_n n^{-s} \tag{1.2}$$

where $f = \sum_{n\geq 1} a_n q^n$ and $g = \sum_{n\geq 1} b_n q^n$ are the q-expansions at infinity of f and g. Since $|a_n| = O(n^{k/2})$ we see that $L(f,s)$ converges absolutely for $\Re(s) > k/2 + 1$, and similarly for $L(g,s)$. We define the complete L-functions to be

$$\Lambda_f(s) = \left(\frac{\sqrt{N}}{2\pi}\right)^s \Gamma(s)L(f,s) \tag{1.3}$$

$$\Lambda_g(s) = \left(\frac{\sqrt{N}}{2\pi}\right)^s \Gamma(s)L(g,s). \tag{1.4}$$

The relation $g = f|_{\omega_N}$ translates into the functional equation

$$\Lambda_f(s) = i^k \Lambda_g(k-s).$$

So the complete L-functions are entire and have a holomorphic continuation to the whole complex plane, which shows that the $L(f,s)$ and $L(g,s)$ have a holomorphic continuation as well (since $1/\Gamma(s)$ is entire). An important observation is that the above arguments can be reversed, using the inverse Mellin transform. More precisely, we have the following result, due to Hecke, which applies to all modular forms (not only cusp forms):

Theorem 1.1.1 (Hecke)**.** Suppose f and g are holomorphic functions on $\mathcal{H}$ given by the Fourier series

$$f(z) = \sum_{n\geq 0} a_n e^{2\pi i n z},$$
$$g(z) = \sum_{n\geq 0} b_n e^{2\pi i n z},$$

such that $a_n, b_n = O(n^\alpha)$ as $n \to \infty$ for some positive constant α. Let N, k be positive integers and put

$$L(f,s) = \sum_{n\geq 1} a_n n^{-s}, \qquad L(g,s) = \sum_{n\geq 1} b_n n^{-s}, \tag{1.5}$$

$$\Lambda_f(s) = \left(\frac{\sqrt{N}}{2\pi}\right)^s \Gamma(s)L(f,s), \qquad \Lambda_g(s) = \left(\frac{\sqrt{N}}{2\pi}\right)^s \Gamma(s)L(g,s). \tag{1.6}$$

Then the following are equivalent:

1. The functions f and g satisfy
$$g(z) = (\sqrt{N}z)^{-k} f(-1/Nz).$$

2. Both $\Lambda(f,s)$ and $\Lambda(g,s)$ have a meromorphic continuation to the whole complex plane, the function
$$\Lambda(f,s) + \frac{a_0}{s} + \frac{b_0 i^k}{k-s} \tag{1.7}$$

is entire, bounded on vertical strips and satisfies

$$\Lambda_f(s) = i^k \Lambda_g(k-s)$$

.

Proof. See [Iwa97, Theorem 7.3]. □

We will apply this result to obtain a converse theorem for modular forms on $\mathrm{SL}_2(\mathbf{Z})$ (see theorem 1.1.3).

1.1.2. Twisting

We can get more functional equations by 'twisting' a modular form by a primitive Dirichlet character ψ.

Theorem 1.1.2. Let $f \in M_k(N, \chi)$ be a modular form of type (k, χ) where χ is a Dirichlet character mod N. Let ψ be a primitive Dirichlet character of conductor r coprime to N. If f has q-expansion

$$f = \sum_{n \geq 0} a_n q^n,$$

then the twisted form

$$f_\psi = \sum_{n \geq 0} \psi(n) a_n q^n$$

belongs to $M_k(Nr^2, \chi\psi^2)$. Moreover, if f is a cusp form then so is f_ψ.

Proof. See [Iwa97, Theorem 7.4]. □

Moreover, a computation [Iwa97, Theorem 7.5] shows that $f_\psi|_{\omega_N} = w(\psi) g|_{\bar{\psi}}$ where $g = f|_{\omega_N}$ and $w(\psi)$ is a constant. Now write $L_f(\psi, s)$ for the twisted L-function $L(f_\psi, s)$ and

$$\Lambda_f(\psi, s) = \Lambda_{f_\psi}(s) = \left(\frac{\sqrt{N}r}{2\pi}\right)^s \Gamma(s) L_f(\psi, s). \tag{1.8}$$

Then applying the previous results shows that $\Lambda_f(\psi, s)$ has a holomorphic continuation to the whole complex plane and satisfies the functional equation

$$\Lambda_f(\psi, s) = w(\psi) i^k \Lambda_g(\bar{\psi}, k-s) \tag{1.9}$$

with $g = f|_{\omega_N}$.

1.1.3. Converse theorems

We already observed that theorem 1.1.1 implies a converse theorem for modular forms on $\mathrm{SL}_2(\mathbf{Z})$. Let us state it here for clarity.

Theorem 1.1.3 (Hecke's converse theorem)**.** Let $k \geq 1$ be an integer and f a holomorphic function on $\mathcal{H}$ of the form

$$f(z) = \sum_{n \geq 0} a_n e^{2\pi i n z},$$

where $a_n = O(n^\alpha)$ for some constant $\alpha > 0$. Then $f(z)$ belongs to $M_k(\mathrm{SL}_2(\mathbf{Z}))$ if and only if $\Lambda(f,s) = (2\pi)^{-s}\Gamma(s)L(s,f)$ has a meromorphic continuation to the whole complex plane, the function

$$\Lambda(f,s) + \frac{a_0}{s} + \frac{i^k a_0}{k-s}$$

is entire, bounded on vertical strips and satisfies the functional equation

$$\Lambda(f,s) = i^k \Lambda(k-s, f).$$

The situation is more complicated for $\Gamma_0(N)$ since as a group it has much more generators in general. We need to require functional equations for sufficiently many twists of the L-function. To state the theorem, we need some notation. Fix a positive integer N. For a set $\mathcal{M} \subset \mathbf{Z}_{\geq 1}$, consider the following conditions:

(A) any element of $\mathcal{M}$ is prime to N,

(B) for any two coprime integers a, b there exists an element $m \in \mathcal{M}$ such that $m \equiv a \mod b$.

An example of a set $\mathcal{M}$ satisfying both conditions is the set of all primes not dividing N (by Dirichlet's theorem). We will need Gauss sums to describe the constants appearing the functional equations. If ψ is a primitive Dirichlet character mod m, then the Gauss sum of ψ is denoted by

$$W(\psi) = \sum_{a \geq 0}^{m-1} \psi(a) e^{2\pi a/m}.$$

for more on Gauss sums, see [Miy06, §3.1].

Theorem 1.1.4 (Weil's converse theorem)**.** Let k, N be positive integers, χ a Dirichlet character mod N with $\chi(-1) = (-1)^k$ and $\mathcal{M} \subset \mathbf{Z}_{\geq 1}$ a subset satisfying conditions (A) and (B). Let f, g be holomorphic functions on $\mathcal{H}$ given by the Fourier series

$$f(z) = \sum_{n \geq 0} a_n e^{2\pi i n z}, \tag{1.10}$$

$$g(z) = \sum_{n \geq 0} b_n e^{2\pi i n z}, \tag{1.11}$$

such that $a_n, b_n = O(n^\alpha)$ as $n \to \infty$ for some positive constant α. The following conditions are sufficient to conclude that $f \in M_k(N, \chi), g \in M_k(N, \overline{\chi})$ and $g = f|_{\omega_N}$:

1. The functions $\Lambda_f(s)$, $\Lambda_g(s)$ as defined in equation 1.6 have a meromorphic continuation to the whole s-plane, the function

$$\Lambda(f,s) + \frac{a_0}{s} + \frac{b_0 i^k}{k-s} \tag{1.12}$$

is entire and bounded on vertical strips and satisfies

$$\Lambda_f(s) = i^k \Lambda_g(k-s).$$

2. For any primitive Dirichlet character ψ with conductor $m_\psi \in \mathcal{M}$, the function $\Lambda_f(\psi, s)$ as defined in equation 1.8 has a holomorphic continuation to the whole complex plane, is bounded on vertical strips and satisfies the functional equation

$$\Lambda_f(\psi, s) = i^k C_\psi \Lambda_g(\psi, k-s),$$

with $C_\psi = \chi(m_\psi)\psi(-N)W(\psi)W(\bar{\psi})^{-1}$.

Moreover, if $L(f, s)$ is absolutely convergent on a half-plane $\Re(s) > k - \delta$ for some $\delta > 0$ then f is a cusp form.

Proof. See [Miy06, Theorem 4.3.15]. □

1.2. Eisenstein Series

Recall that if Γ is a congruence subgroup and $f, g \in M_k(\Gamma)$ are modular forms where either f or g (or both) is a cusp form, then the integral

$$\langle f, g \rangle = \int_{\Gamma\backslash\mathcal{H}} f(z)\overline{g(z)}y^k \frac{dxdy}{y^2}$$

is well-defined. It thus makes sense to ask whether a modular form $f \in M_k(\Gamma)$ is orthogonal to all cusp forms $g \in S_k(\Gamma)$. This defines the space of Eisenstein series, denoted $E_k(\Gamma)$, and we have the following decomposition:

$$M_k(\Gamma) = E_k(\Gamma) \oplus S_k(\Gamma).$$

The space $E_k(\Gamma_1(N))$ is well-understood and has a basis of $\mathbf{T}_{(N)}$-eigenforms for all Hecke operators called generalized Eisenstein series. They correspond naturally to Dirichlet L-functions of Dirichlet characters.

To illustrate the idea behind Eisenstein series on $\Gamma_1(N)$ it's worth looking at Eisentein series on $\mathrm{SL}_2(\mathbf{Z})$ from the viewpoint of L-functions. Suppose we start with the Riemann zeta function

$$\zeta(s) = \sum_{n\geq 1} n^{-s} = \prod_p (1 - p^{-s})^{-1}.$$

How can we associate a modular form to it? If we put $\xi(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$ then we have the classical functional equation $\xi(s) = \xi(1-s)$. Looking at the Euler product we see that $\zeta(s)$ couldn't be the L-function of a modular form, but we should consider the product of two zeta functions. Put

$$L(s) = \zeta(s)\zeta(s-k+1)$$

for $k \geq 2$ an even integer. We have

$$\begin{aligned}
\xi(s)\xi(s-k+1) &= \pi^{-s}\pi^{\frac{k-1}{2}}\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s-k+1}{2}\right)\zeta(s)\zeta(s-k+1) \\
&= \pi^{-s}\pi^{\frac{k-1}{2}}\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s+1}{2}\right)2^{k/2}w(s)^{-1}L(s) \\
&= \pi^{-s}\pi^{\frac{k-1}{2}}\pi^{1/2}2^{1-s}\Gamma(s)2^{k/2}w(s)^{-1}L(s) \\
&= 2(2\pi)^{k/2}(2\pi)^{-s}\Gamma(s)L(s)w(s)^{-1}
\end{aligned}$$

where we used the formulas

$$\Gamma(s+1) = s\Gamma(s) \tag{1.13}$$

$$\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s+1}{2}\right) = \pi^{1/2}2^{1-s}\Gamma(s) \tag{1.14}$$

and where we have set

$$w(s) = (s+1-k)(s+1-k-2)\dots(s-1).$$

Since $\xi(s)\xi(s-k+1)$ is invariant under $s \mapsto k-s$ and $w(k-s) = (-1)^{k/2}w(s)$ we conclude that the complete L-function

$$\Lambda(s) = (2\pi)^{-s}\Gamma(s)L(s)$$

satisfies the functional equation

$$\Lambda(s) = i^k\Lambda(k-s).$$

Since the product of two Dirichlet series has as coefficients the Dirichlet convolution of the coefficients of the factors we see that

$$L(s) = \sum_{n\geq 1}\sigma_{k-1}(n)n^{-s},$$

where $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$ is the $(k-1)$-th power sum of divisors function. If $k \geq 4$ we see that $\Lambda(s)$ is holomorphic except for a simple pole at $s = 0$ and k where the residue at $s = k$ is

$$\begin{aligned}(2\pi)^{-k}\Gamma(k)\zeta(k) &= (2\pi)^{-k}\Gamma(k)(-1)^{k/2+1}\frac{B_k(2\pi)^k}{2.k!}\\ &= -i^k\frac{B_k}{2k}\end{aligned}$$

So by the functional equation we conclude that

$$\Lambda(s) - \frac{B_k/2k}{s} - \frac{i^kB_k/2k}{k-s}$$

is entire and bounded on vertical strips. We conclude that

$$E_k = \frac{-B_k}{2k} + \sum_{n\geq 1}\sigma_{k-1}(n)q^n$$

is a modular form on $\mathrm{SL}_2(\mathbf{Z})$ of weight k by theorem 1.1.3. Notice that the constant $-B_k/2k$ came naturally out of our calculations.

We can do something similar for the L-functions of two Dirichlet characters. Let χ be a primitive Dirichlet character mod M with associated Dirichlet series

$$L(\chi, s) = \sum_{n\geq 1}\chi(n)n^{-s} = \prod_p \left(1-\chi(p)p^{-s}\right)^{-1}.$$

If

$$\Lambda(\chi, s) = \left(\frac{M}{\pi}\right)^{s/2}\Gamma\left(\frac{s+u}{2}\right)L(\chi, s),$$

where $u \in \{0, 1\}$ is chosen such that $\chi(-1) = (-1)^u$, then

$$\Lambda(\chi, s) = \epsilon_\chi\Lambda(\bar{\chi}, 1-s) \tag{1.15}$$

where $\epsilon_\chi = i^{-u}W(\chi)M^{-1/2}$ and $W(\chi) = \sum_{a=0}^{M-1}\chi(a)e^{2\pi ia/M}$ is the Gauss sum of χ. We can exploit this functional equation to get modular forms on $\Gamma_0(N)$. Suppose χ_1, χ_2 are primitive Dirichlet characters mod M_1 and M_2. Set $M = M_1M_2$ and $\chi = \chi_1\chi_2$ which is a Dirichlet character mod M. Let k be a positive integer that we assume to be different from 2 for simplicity. Then similarly as above we form the L-function

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

The coefficients of $L(s)$ are given by 'generalized divisor functions':

$$\sigma_{k-1}^{\chi_1,\chi_2}(n) = \sum_{d|n}\chi_1(d)\chi_2(n/d)(n/d)^{k-1}.$$

We set

$$\Lambda(s) = \left(\frac{\sqrt{M}}{2\pi}\right)^s \Gamma(s)L(s).$$

A similar calculation as above and using Weil's converse theorem shows the following.

Theorem 1.2.1. Let χ_1, χ_2 be primitive Dirichlet characters mod M_1 and mod M_2 respectively. Put $M = M_1M_2$ and $\chi = \chi_1\chi_2$. Let $k \neq 2$ be a positive integer satisfying $\chi(-1) = (-1)^k$. Then there exists an $a_0 \in \mathbf{C}$ such that

$$E_k^{\chi_1,\chi_2}(z) := a_0 + \sum_{n\geq 1}\sigma_{k-1}^{\chi_1,\chi_2}(n)q^n \in M_k(M,\chi).$$

It is given by

1. $a_0 = 0$, if $k \neq 1$ and χ_1 is non-trivial, or if both χ_1 and χ_2 are non-trivial.
2. $a_0 = L(1-k,\chi)/2$, otherwise.

Moreover, since the associated L-function has an Euler product, $E_k^{\chi_1,\chi_2}$ is an eigenform for all the Hecke operators T_n, $n \geq 1$.

Proof. See [Miy06, Theorem 4.7.1]. □

In fact, one can prove that $E_k^{\chi_1,\chi_2}$ are all in the Eisenstein space of $\Gamma_1(N)$. If $\chi = \chi_1\chi_2$ is a character mod M with M dividing N then $E_k^{\chi_1,\chi_2}(dz)$ is in the Eisenstein space $E_k(N,\chi)$ if $dM \mid N$ and is a $\mathbf{T}_{(N)}$-eigenform. By counting dimensions [Miy06, Theorem 4.7.2] we can fully describe the space $E_k(N,\chi)$.

Theorem 1.2.2. Let $k \neq 2$ be a positive integer and and χ a Dirichlet character mod N satisfying $\chi(-1) = (-1)^k$. The Eisenstein space $E_k(N,\chi)$ is spanned by the forms $E_k^{\chi_1,\chi_2}(dz)$ where χ_1, χ_2 are primitive Dirichlet characters mod M_1, M_2 with $\chi_1\chi_2 = \chi$ and $dM_1M_2 \mid N$. Moreover, they form a basis for $k > 2$ if one considers ordered pairs (χ_1, χ_2) satisfying the above conditions and for $k = 1$ if one considers unordered pairs $\{\chi_1, \chi_2\}$ satisfying the above conditions.

1.3. Hecke characters and L-functions

Let K be a number field of degree n over $\mathbf{Q}$ with r_1 real and $2r_2$ complex embeddings. Write $\tau_1, \ldots, \tau_{r_1}$ for the real embeddings and $\tau_{r_1+1}, \bar{\tau}_{r_1+1}, \ldots, \tau_{r_1+r_2}, \bar{\tau}_{r_1+r_2}$ for the pairs of complex conjugate embeddings.

We will define a Hecke character of a number field K, which is a generalization of a Dirichlet character, and see how they provide examples of modular forms in certain cases. Let $\mathcal{O}_K$ be the ring of integers of K, I the group of nonzero fractional ideals and P the subgroup of principal ideals of I. We know $Cl_K = I/P$ is a finite group, the class group. More generally, if $\mathfrak{m}$ is an integral ideal of K, set

$$I(\mathfrak{m}) = \{\mathfrak{a} \in I \mid (\mathfrak{a}, \mathfrak{m}) = 1\}$$
$$P(\mathfrak{m}) = \{(a) \in P \mid a \equiv 1 \bmod^* \mathfrak{m}\}$$

where $a \equiv 1 \bmod^* \mathfrak{m}$ means that $v_\mathfrak{p}(a-1) \geq v_\mathfrak{p}(\mathfrak{m})$ for each prime $\mathfrak{p}$ dividing $\mathfrak{m}$. It is a fact that $I(\mathfrak{m})/P(\mathfrak{m})$ is a finite group, called the ray class group mod $\mathfrak{m}$. Class field theory more or less says that there is a unique abelian extension of K, the ray class field mod $\mathfrak{m}$, denoted $K_\mathfrak{m}$ which is unramified outside $\mathfrak{m}$ and for which the homomorphism

$$I(\mathfrak{m})/P(\mathfrak{m}) \to \mathrm{Gal}(K_\mathfrak{m}/K),$$

that sends a prime ideal $\mathfrak{p} \in I(\mathfrak{m})$ to the Frobenius at $\mathfrak{p}$ in $\mathrm{Gal}(K_\mathfrak{m}/K)$, is an isomorphism. Note that this morphism is well-defined since $\mathrm{Gal}(K_\mathfrak{m}/K)$ is abelian.

Definition 1.3.1. Let $\xi : I(\mathfrak{m}) \to S^1$ be a homomorphism. We say ξ is a Hecke character mod $\mathfrak{m}$ if

$$\xi((a)) = \prod_{\nu=1}^{r_1+r_2} \left(\frac{\tau_\nu(a)}{|\tau_\nu(a)|}\right)^{u_\nu} |\tau_\nu(a)|^{iv_\nu} \quad \text{for } a \equiv 1 \bmod^* \mathfrak{m}$$

where u_ν, v_ν $(1 \leq \nu \leq r_1 + r_2)$ are real numbers such that

- $u_\nu \in \begin{cases} \{0,1\} & (\tau_\nu \text{ real}), \\ \mathbf{Z} & (\tau_\nu \text{ complex }), \end{cases}$
- $\sum_{\nu=1}^{r_1+r_2} v_\nu = 0$.

Remark 1.3.2. There is another definition of Hecke characters in terms of ideles. If $\mathbf{J}_K$ denotes the ideles of K then a Hecke character is a continuous morphism $\mathbf{J}_K/K^\times \to S^1$. Since we are interested in explicit examples the classical definition of Hecke will suffice for our purposes.

Clearly if $\mathfrak{m}$ divides $\mathfrak{n}$ then every Hecke character mod $\mathfrak{m}$ is a Hecke character mod $\mathfrak{n}$. The smallest ideal $\mathfrak{m}$ (in the obvious sense) such that a Hecke character ξ is defined mod $\mathfrak{m}$ is called the conductor of ξ. If the conductor of ξ mod $\mathfrak{m}$ equals $\mathfrak{m}$ we say ξ is primitive (this is the exact analogue of Dirichlet characters). Furthermore, if ξ satisfies the additional conditions that $v_\nu = 0$ for all ν and $u_\nu = 0$ for τ_ν complex then we say ξ is a class character. This implies that ξ defines a homomorphism on some ray class group of K (of modulus $\mathfrak{m} \cup \{\text{real places of } K\}$). Note that class characters of conductor $(1) = \mathcal{O}_K$ are precisely the characters on the narrow ideal class group of K. We can always extend a Hecke character ξ to be a function on I by setting $\xi(\mathfrak{a}) = 0$ if $(\mathfrak{a}, \mathfrak{m}) = 1$.

For each Hecke character $\xi : I((m)) \to S^1$ we define the Hecke L-function by $(s \in \mathbf{C})$

$$L(\xi, s) = \sum_\mathfrak{a} \xi(\mathfrak{a}) N(\mathfrak{a})^{-s}.$$

where the sum if taken over all non-zero integral ideals of K and $N(\mathfrak{a}) = |(\mathcal{O}_K/\mathfrak{a})|$ is the absolute norm. This converges absolutely for $\Re(s) > 1$ and has an Euler product

$$L(\xi, s) = \prod_\mathfrak{p} \left(1 - \xi(\mathfrak{p}) N(\mathfrak{p})^{-s}\right)^{-1},$$

where the product runs over all primes of K. Note that if ξ is the trivial character mod (1) then $L(\xi, s)$ is the Dedekind zeta function of K. By generalizing the proof for the Riemann zeta-function, Hecke obtained a functional equation for every Hecke L-function:

Theorem 1.3.3. Let ξ be a primitive Hecke character of conductor $\mathfrak{m}$. Put

$$\Lambda(\xi, s) = \left(\frac{2^{r_1}|\Delta_F|N(\mathfrak{m})}{(2\pi)^n}\right)^{s/2} \prod_{\nu=1}^{r_1+r_2} \Gamma\left(\frac{n_\nu(s+iv_\nu)+|u_\nu|}{2}\right) L(\xi, s)$$

where n_ν is 1 if τ_ν is real and 2 if τ_ν is complex. Then $\Lambda(\xi, s)$ has an analytic continuation to a meromorphic function on the whole s-plane, and satisfies the functional equation

$$\Lambda(\xi, 1-s) = T(\xi)\Lambda(\bar{\xi}, s),$$

where $\bar{\xi}$ is the conjugate Hecke character and $T(\xi)$ a constant only depending on ξ. Moreover, $\Lambda(\xi, s)$ is entire if ξ is nontrivial.

Proof. See [Miy06, Theorem 3.3.1]. □

The Gamma factors appearing in $\Lambda(\xi, s)$ can be interpreted as the Euler factors corresponding to the infinite places.

It might be worth seeing theorem 1.3.3 for a simple example. If ξ is a class character mod m of $\mathbf{Q}$, then $\xi((a)) = \mathrm{sgn}(a)^u$ for all $a \equiv 1 \bmod^* m$. Defining $\chi(a) = \xi((a))$ for positive integers a coprime to m and extending periodically mod m, we see that χ is a Dirichlet character mod m satisfying $\chi(-1) = \chi(m-1) = (-1)^u$. The functional equation for ξ is just the functional equation for χ as in equation 1.15. If ξ is a class character of an imaginary quadratic number field F, then

$$\Lambda(\xi, s) = (|\Delta_F|N(\mathfrak{m}))^{s/2}(2\pi)^{-s}\Gamma(s)L(\xi, s) \tag{1.16}$$

which looks like the complete L-function of a modular form. Using Weil's converse theorem we can make this connection precise.

Say that a Hecke character ξ mod $\mathfrak{m}$ on a number field K is induced from a Dirichlet character ψ through the norm if it is of the form $\psi \circ N$ i.e. if

$$\xi(\mathfrak{a}) = \psi(N(\mathfrak{a}))$$

for all $\mathfrak{a} \in I(\mathfrak{m})$.

Theorem 1.3.4. Let K be an imaginary quadratic field with discriminant Δ and ξ a Hecke character mod $\mathfrak{m}$ such that

$$\xi((a)) = \left(\frac{a}{|a|}\right)^u \quad (a \equiv 1 \mod \mathfrak{m})$$

with $u \in \mathbf{Z}$. Let

$$f(z) = \sum_{\mathfrak{a}} \xi(a)N(\mathfrak{a})^{u/2} q^{N(\mathfrak{a})},$$

where $\mathfrak{a}$ runs over all integral ideals of K. Then $f(z) \in M_{u+1}(N, \chi)$ with $N = |\Delta|N(\mathfrak{m})$ and f is a cusp form unless $u = 0$ and ξ is induced from a Dirichlet character through the norm. The character χ is defined by

$$\chi(m) = \chi_\Delta(m)\xi((m))$$

where

$$\chi_\Delta(m) = \left(\frac{\Delta}{\cdot}\right)$$

is the quadratic character associated to K. Moreover, f is a $\mathbf{T}$-eigenform and if ξ is primitive then f is a newform.

Proof. See [Miy06, Theorem 4.8.2]. □

The fact that f is a $\mathbf{T}$-eigenform follows from the fact that $L(\xi, s)$ has an Euler product. If we choose $u = 0$, we get modular forms of weight one. The modular forms constructed this way have a close connection to theta series. We will explore this in more detail in the section on dihedral representations in chapter 4. There exists a similar theorem for real quadratic fields:

Theorem 1.3.5. Let K be a real quadratic field with discriminant Δ and ξ a Hecke character mod $\mathfrak{m}$ such that

$$\xi((a)) = \operatorname{sgn}(a^\tau) \quad (a \equiv 1 \mod \mathfrak{m})$$

for some embedding $\tau : K \to \mathbf{R}$. Let

$$f(z) = \sum_{\mathfrak{a}} \xi(\mathfrak{a}) q^{N\mathfrak{a}},$$

where $\mathfrak{a}$ runs over all integral ideals of K. Then $f(z) \in S_1(N, \chi)$ with $N = \Delta N(\mathfrak{m})$ and χ is defined by

$$\chi(m) = \chi_\Delta(m)\xi((m)).$$

Moreover, f is an eigenform and if ξ is primitive then f is a newform.

Proof. See [Miy06, Theorem 4.8.3]. □

1.4. Properties of eigenvalues

1.4.1. Rationality

There are certain results for which the algebro-geometric theory of modular forms is indispensable. This aspect is not explained in this essay but we will need the result nevertheless:

Theorem 1.4.1. Let $f = \sum_{n\geq 1} a_n q^n \in S_k(N, \chi)$ be a cusp form and $\sigma : \mathbf{C} \to \mathbf{C}$ an automorphism.

1. The function $f^\sigma(z) = \sum_{n\geq 1} a_n^\sigma q^n$ is an element of $S_k(N, \chi^\sigma)$,
2. if the coefficients a_n are algebraic, they have bounded denominators,
3. the eigenvalues of the Hecke operators T_n for $n \geq 1$ lie in the ring of integers of a number field K.

Proof. See [DS74, §2.7] and [DI94, §12.3]. □

It is possible to give a more elementary proof of this result for weight $k \geq 2$, see [Shi94, Theorem 3.52]. There are tricks to derive the theorem for weight $k = 1$ via this approach, as explained in [Ser75, §2.5].

Lemma 1.4.2. Let L be the set of cusp form in $S_k(\Gamma_1(N))$ with rational integer q-expansion. Then L is a free $\mathbf{Z}$-module of finite type. Moreover, let R be a subring of $\mathbf{C}$ and let S_R be the set of cusp forms in $S_k(N,\chi)$ with q-expansion in $R[[q]]$. Then $S_R \cong L \otimes_{\mathbf{Z}} R$.

Proof. There exists an integer $B \geq 1$ such that the map

$$\begin{aligned} S_k(N,\chi) &\to \mathbf{C}^B \\ f = \sum_{n\geq 0} a_n q^n &\mapsto (a_1, \ldots, a_n) \end{aligned}$$

is injective. One can take $B = 1 + k[\mathrm{SL}_2(\mathbf{Z}) : \Gamma_0(N)]/12$. The image of L under this map will be a submodule of $\mathbf{Z}^B$, hence free of finite type. So L is free of finite type. The remaining part of the corollary follows from [DI94, §12.3].

□

1.4.2. Eigenvalues at the bad primes

Let $f \in S_k(N,\chi)$ be a newform with L-function

$$L(f,s) = \sum_{n\geq 1} a_n n^{-s} = \prod_{p|N} (1 - a_p p^{-s})^{-1} \prod_{p\nmid N} (1 - app^{-s} + \chi(p)p^{k-1-2s})^{-1}.$$

Growth conditions on the coefficients of f are of great interest for the study of modular forms (the Ramanujan-Petersson conjecture is an example, see corollary 3.6.1). The eigenvalues of T_p at the bad primes are easy to describe.

Proposition 1.4.3. Let $f = \sum_{n\geq 1} a_n q^n \in S_k(N,\chi)$ be a newform and p a prime dividing N. Then

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

Proof. See [Li74, Theorem 3]. □

2. Galois Representations

This chapter gives a short introduction to Galois representations. We begin with some general considerations where we include mod p and l-adic representations. We define the Artin conductor and Artin L-function for Artin representations. We end with a few results needed in the proof of the Deligne-Serre construction in chapter three.

2.1. Definitions

2.1.1. Representations

Let G be a topological group and F a topological field. For each $d \geq 1$, we give $\mathrm{GL}_d(F)$ the subspace topology coming from $\mathrm{Mat}_d(F) \simeq F^{d\times d}$.

Definition 2.1.1. A representation of G is a continuous homomorphism

$$G \to \mathrm{GL}_d(F).$$

We call d the degree of the representation and F the field of definition.

The most important case for us will be if G is a profinite group. Recall that a profinite group is the inverse limit of an inverse system $((A_i)_{i\in I}, (f_{ij})_{i\leq j\in I})$ of finite groups:

$$G = \varprojlim A_i = \left\{ (a_i) \in \prod_{i\in I} A_i \mid f_{ij}(a_j) = a_i,\ \forall i \leq j \right\} \subseteq \prod_{i\in I} A_i.$$

We equip G with the subspace topology coming from the topology on $\prod_{i\in I} A_i$ where every finite group A_i is given the discrete topology. It is the weakest topology which makes the natural projection maps $G \to A_i$ continuous. Under this topology, profinite groups are always Hausdorff, compact and totally disconnected. Moreover, note that every open subgroup is of finite index: the quotient is compact and discrete, hence finite. The open normal subgroups of G form a neighbourhood basis of the identity.

Example 2.1.2. If L/K is a (possibly infinite) Galois extension, then $\mathrm{Gal}(L/K)$ is a profinite group and we have an isomorphism

$$\mathrm{Gal}(L/K) \cong \varprojlim_{\substack{E/K\subset L/K \\ \text{finite Galois}}} \mathrm{Gal}(E/K)$$

Where the inverse limit runs over all the finite Galois subextensions of E/K. The topology on $\mathrm{Gal}(L/K)$ that arises in this way is called the *Krull topology.*

The above discussion specializes to the Galois extension $\bar{K}/K$ where $\bar{K}$ is a separable closure of K. We will write its Galois group as $G_K = \mathrm{Gal}(\bar{K}/K)$. We say G_K is the *absolute Galois group* of K. In this case, a representation

$$\rho : G_K \to \mathrm{GL}_d(F)$$

is called a *Galois representation.* According to the field of definition F we say ρ is

- an Artin representation if $F = \mathbf{C}$ (with the Euclidean topology),
- a mod p representation if $F = \overline{\mathbf{F}}_p$ (with the discrete topology),
- an l-adic representation if $F = \overline{\mathbf{Q}}_l$ (with the l-adic topology).

We will be interested in the case where K is a number field or local field of characteristic zero (where separability is automatic).

Lemma 2.1.3. If G is profinite, then every complex representation $\rho : G \to \mathrm{GL}_d(\mathbf{C})$ (where $\mathbf{C}$ is equipped with the Euclidean topology) has open kernel.

Proof. We claim that there is an open neighbourhood U of the identity I_d in $\mathrm{GL}_d(\mathbf{C})$ which contains no nontrivial subgroups. Indeed, take the norm $||\cdot||$ on $\mathrm{Mat}_d(\mathbf{C})$ induced from the norm on $\mathbf{C}^d$ given by $||(z_i)||= \sqrt{|z_1|^2+\cdots+|z_d|^2}$. Set

$$U = \{A \in \mathrm{GL}_d(\mathbf{C}) \mid ||A - I_d||< 1/2\}.$$

Suppose $A \in U, A \neq I_d$ lies in a nontrivial subgroup contained in U. Since $||P^{-1}AP - I_d||= ||A - I_d||$ we may suppose that A is in its Jordan canonical form. If one of the eigenvalues of A has absolute value different from 1 the norms $||A^n||$ for $n \in \mathbf{Z}$ are clearly unbounded so $A^n \notin U$ for some $n \in \mathbf{Z}$. If A has an eigenvalue $\alpha \neq 1$ with $|\alpha|= 1$ then $|\alpha^n - 1|> 1/2$ for some $n \in \mathbf{Z}$ so $A^n \notin U$ for some $n \in \mathbf{Z}$. The only case left is when all the eigenvalues of A are equal to 1. But in that case A has at least one non-trivial Jordan block since $A \neq I_d$ so again $||A^n||$ is unbounded for $n \in \mathbf{Z}$ so $A^n \notin U$ for some $n \in \mathbf{Z}$. This covers all cases and shows that U does not contain any non-trivial subgroup.

Now given such an open set U and a representation ρ, look at its inverse image $\rho^{-1}(U)$ in G. Since G is profinite and $\rho^{-1}(U)$ is open, there is a subgroup H of finite index contained in $\rho^{-1}(U)$. But then $\rho(H)$ is a subgroup of $GL_d(\mathbf{C})$ contained in U, hence trivial. So H is in the kernel of ρ, which implies it is a finite index closed subgroup of G, hence open. □

So for every field K, a representation $\rho : G_K \to \mathrm{GL}_d(\mathbf{C})$ factors through a finite extension of K, so we might as well equip $\mathrm{GL}_d(\mathbf{C})$ with the discrete topology (some authors do this by default). It is important to remark that if K is a number field, not every Galois representation $G_K \to \mathrm{GL}_d(F)$ has finite image. Indeed, if $F = \overline{\mathbf{Q}}_l$ we will see examples where the image is infinite (see theorem 3.2.1 of the next chapter).

Lemma 2.1.4. Let G be a profinite group and $\rho : G \to \mathrm{GL}_d(\mathbf{Q}_l)$ a continuous representation. Then ρ can be conjugated to a representation with values in $\mathrm{GL}_d(\mathbf{Z}_l)$.

Proof. It is enough to show that G stabilizes some lattice in $\mathbf{Q}_l^d$, i.e. a free $\mathbf{Z}_l$-module which contains a basis for $\mathbf{Q}_l^d$. Take the standard lattic $L = \mathbf{Z}_l^d \subset \mathbf{Q}_l^d$. The set of all $A \in \mathrm{GL}_d(\mathbf{Q}_l)$ such that $A \cdot L = L$ is precisely $\mathrm{GL}_d(\mathbf{Z}_l)$, an open subgroup of $\mathrm{GL}_d(\mathbf{Q}_l)$. So the set of all $g \in G$ such that $\rho(g)L = L$ is an open subgroup H of G. So G/H is finite and G stabilizes the lattice

$$\sum_{g \in G/H} g \cdot L.$$

□

2.1.2. Ramification

Let's define the notion of ramification for a Galois representation. Let K a number field with absolute Galois group G_K. For each prime $\mathfrak{p}$ in K, choose an embedding $\overline{K} \to \overline{K_\mathfrak{p}}$. The restriction map $\mathrm{Gal}(\overline{K}_\mathfrak{p}/K_\mathfrak{p}) \to \mathrm{Gal}(\overline{K}/K)$ is injective, its image is the decomposition group $D_\mathfrak{p} \subset G_K$. The ring of integers of $\overline{K}_\mathfrak{p}$ is stable under the action of $\mathrm{Gal}(\overline{K}_\mathfrak{p}/K_\mathfrak{p})$, as is its unique maximal ideal. The residue field may be identified with the algebraic closure $\bar{k}$ of k, where k is the residue field of K. Let $I_\mathfrak{p}$ be the kernel of the reduction map

$$D_\mathfrak{p} \to \mathrm{Gal}(\bar{k}/k).$$

Since $k = \mathbf{F}_q$ is a finite field, the group $\mathrm{Gal}(\bar{k}/k) = \mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q)$ is topologically cyclic, generated by the Frobenius $x \mapsto x^q$. Since the reduction map $D_\mathfrak{p} \to \mathrm{Gal}(\bar{k}/k)$ is surjective, there exists an element $\mathrm{Frob}_p \in D_\mathfrak{p}$ which reduces to the Frobenius on $\bar{k}$. We call such elements Frobenius elements.

Definition 2.1.5. Let L be a finite extension of $\mathbf{Q}_p$ and K a number field.

- We say a representation $\sigma : G_L \to \mathrm{GL}_d(F)$ is unramified if the inertia group of G_L is in the kernel of σ. Otherwise, we say σ is ramified.
- We say a representation $\rho : G_K \to \mathrm{GL}_d(F)$ is unramified at a prime $\mathfrak{p}$ of K if $\rho|_{I_\mathfrak{p}}$ is trivial or equivalently, if the associated local representation $\rho|_{D_\mathfrak{p}} \colon G_{K_\mathfrak{p}} \to \mathrm{GL}_d(F)$ is unramified.

For an ideal $\mathfrak{m}$ of K, say ρ is unramified outside $\mathfrak{m}$ if ρ is unramified for every prime $\mathfrak{p}$ not dividing $\mathfrak{m}$.

This definition doesn't depend on the choice of the embedding $\overline{K} \to \overline{K}_\mathfrak{p}$. If $\rho : G_K \to \mathrm{GL}_d(F)$ is unramified at $\mathfrak{p}$ and $\mathrm{Frob}_\mathfrak{p}$ is a Frobenius at $\mathfrak{p}$ then $\rho(\mathrm{Frob}_\mathfrak{p})$ is well-defined up to conjugation. It thus makes sense to speak of the trace, determinant and characteristic polynomial of $\rho(\mathrm{Frob}_\mathfrak{p})$. If ρ factors through a finite extension L/K then it is ramified at only finitely many primes.

2.2. Artin conductor

In this section we will define for each representation $\rho : G_K \to \mathrm{GL}_d(\mathbf{C})$ an ideal in K which measures the ramification behaviour of ρ in a precise way, called the Artin conductor. To do this, we will first look at the local case. We refer to [Ser95, chapter VI] for the proofs.

Suppose L/K is a finite Galois extension of local fields, which we will assume to be finite extensions of $\mathbf{Q}_p$. Recall that $G = \mathrm{Gal}(L/K)$ comes with a filtration

$$G \supset G_0 \supset G_1 \supset G_2 \supset \cdots$$

called the ramification groups in the lower numbering. If L, K have residue fields k_L, k_K then G_0 is the kernel of the reduction map $G \to \mathrm{Gal}(k_L/k_K)$ and G_1 is the unique sylow-p-subgroup of G_0. By setting $G_t = G_{\lceil t \rceil}$ for every real number $t > -1$ (set $G_{-1} = G$) and

$$\phi_{L/K}(u) = \int_0^u \frac{dt}{[G_0 : G_t]}$$

We define the upper ramification groups to be $G^u = G_{\phi^{-1}_{L/K}(u)}$ for $u > -1$.

Definition 2.2.1. The Artin conductor of a representation $\rho : G \to \mathrm{GL}(V)$ is defined as

$$\mathfrak{f}(\rho) = \sum_{i=0}^{\infty} \frac{|G_i|}{|G_0|} \dim(V/V^{G_i})$$

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

It is a non-trivial fact that the Artin conductor of a representation is always an integer. We can rewrite it as follows:

$$\begin{aligned}\mathfrak{f}(\rho) &= \int_{-1}^{\infty} \frac{|G_t|}{|G_0|} \dim(V/V^{G_i})\, dt \\ &= \int_{-1}^{\infty} \frac{|G_t|}{|G_0|} \dim(V/V^{G^{\phi_{L/K}(t)}})\, dt.\end{aligned}$$

Making the substitution $u = \phi_{L/K}(t)$ and noting that $\phi'_{L/K}(t) = \frac{|G_t|}{|G_0|}$ almost everywhere, we obtain the expression

$$\mathfrak{f}(\rho) = \int_{-1}^{\infty} \dim(V/V^{G^u})\, du. \tag{2.1}$$

Clearly, the representation ρ is unramified if and only if $\mathfrak{f}(\rho) = 0$. Equation 2.1 shows that we have the following more precise statement:

Proposition 2.2.2. Let $\rho : G \to \mathrm{GL}_d(\mathbf{C})$ be an irreducible representation of G and r the largest integer such that $\rho|_{G^r}$ is non-trivial (if $\rho|_{G^0}$ is trivial, set $r = -1$). Then

$$\mathfrak{f}(\rho) = \deg(\rho)(r+1).$$

Proof. Since G^u is a normal subgroup of G, then subspace V^{G^u} is G-invariant, hence equal to V or trivial because ρ is irreducible. The result follows from equation 2.1.

□

Remark 2.2.3. This result is particularly useful for one-dimensional representations, which are always irreducible.

Let's move on to the global picture. Let L/K be a finite Galois extension of number fields with $G = \mathrm{Gal}(L/K)$. For each prime $\mathfrak{p}$ in K and prime $\mathfrak{P}$ in L above $\mathfrak{p}$ we have subgroups

$$D_{\mathfrak{P}|\mathfrak{p}} \subseteq G$$

which are isomorphic to $\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ where $L_{\mathfrak{P}}$ and $K_{\mathfrak{p}}$ are the $\mathfrak{P}$-adic and $\mathfrak{p}$-adic completions of L and K respectively. If $\rho : G \to \mathrm{GL}_d(\mathbf{C})$ is a representation we can restrict it to $D_{\mathfrak{P}|\mathfrak{p}}$ and get a local representation

$$\rho_{\mathfrak{p}} : \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \to \mathrm{GL}_d(\mathbf{C}).$$

Set $\mathfrak{f}(\rho, \mathfrak{p}) = \mathfrak{f}(\rho_{\mathfrak{p}})$, which doesn't depend on the choice of the prime $\mathfrak{P}$ above $\mathfrak{p}$. Since ρ is ramified at only finitely many primes, the product

$$\mathfrak{f}(\rho) = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathfrak{f}(\rho,\mathfrak{p})}$$

is a well-defined integral ideal of K, and is called the *Artin conductor* of ρ. It satisfies the following properties:

Proposition 2.2.4. Let ρ, ρ' be two complex representations of $G = \mathrm{Gal}(L/K)$. Then we have

1. $\mathfrak{f}(\rho \oplus \rho') = \mathfrak{f}(\rho)\mathfrak{f}(\rho')$ and $\mathfrak{f}(\mathbf{1}_G) = 1$ where $\mathbf{1}_G$ is the trivial representation
2. If $K'/K \subset L/K$ is a subextension with $H = \mathrm{Gal}(L/K') \leq G$ and ψ a representation of H then
$$\mathfrak{f}\left(\mathrm{Ind}_H^G \psi\right) = \mathfrak{d}_{K'/K}^{\deg(\psi)} N_{K'/K}(\mathfrak{f}(\psi)),$$
where $\mathrm{Ind}_H^G \psi$ is the induced representation on G and $\mathfrak{d}_{K'/K}$ the discriminant of the extension K'/K.
3. If $K'/K \subset L/K$ is a Galois subextension with $H = \mathrm{Gal}(L/K')$ and $\sigma : G/H \to \mathrm{GL}(V)$ a representation of $G/H = \mathrm{Gal}(K'/K)$ with inflation $\tilde{\sigma} : G \to \mathrm{GL}(V)$ then
$$\mathfrak{f}(\widetilde{\rho}) = \mathfrak{f}(\rho).$$

As an application of the previous proposition, take $H = \{1\}$ in property 2 and let ψ be the trivial representation on H. The induction of ψ to G is the regular representation, and so decomposing this we get that
$$\mathfrak{d}_{L/K} = \prod_{\rho} \mathfrak{f}(\rho)^{\deg(\rho)}$$
where the product runs over all irreducible representations of $\mathrm{Gal}(L/K)$. This is known as the 'Führerdiskriminantenproduktformel'.

The definition of the Artin conductor for representations $\rho : G_K \to \mathrm{GL}_d(\mathbf{C})$ of the absolute Galois group of a number field K is straightforward: by lemma 2.1.3, ρ factors through some $\mathrm{Gal}(L/K)$ where L/K is a finite Galois extension as in the following diagram:

$$\begin{array}{ccc} G_K & \xrightarrow{\rho} & \mathrm{GL}_d(\mathbf{C}) \\ \downarrow & \nearrow_{\tilde{\rho}} & \\ \mathrm{Gal}(L/K) & & \end{array}$$

hence we define the Artin conductor of ρ to be the one attached to the representation $\tilde{\rho} : \mathrm{Gal}(L/K) \to \mathrm{GL}_d(\mathbf{C})$, that is $\mathfrak{f}(\rho) = \mathfrak{f}(\tilde{\rho})$. Property 3 of proposition 2.2.4 shows that this doesn't depend on L.

Example 2.2.5. To illustrate why the Artin conductor is a suitable invariant, let's describe all one-dimensional representations $G_{\mathbf{Q}} \to \mathbf{C}^\times$ of the absolute Galois group of $\mathbf{Q}$ of conductor N. If ψ is such a representation then by Kronecker-Weber ψ factors through some $\mathrm{Gal}(\mathbf{Q}(\zeta_M)/\mathbf{Q})$ for some $M \geq 1$. For a prime p let $M = tp^e$ with $p \nmid t$. The i-th ramification group at p in the upper numbering is given by $\mathrm{Gal}(\mathbf{Q}(\zeta_M)/\mathbf{Q}(\zeta_{tp^i}))$ for $i = 0, 1, \ldots, e-1$ and is trivial for $i \geq e$. By proposition 2.2.2, this shows that N divides M and ψ is trivial on $\mathrm{Gal}(\mathbf{Q}_{\zeta_M}/\mathbf{Q}_{\zeta_{tp^{v_p(N)}}})$. In other words, ψ factors through $\mathrm{Gal}(\mathbf{Q}(\zeta_N)/\mathbf{Q})$ but not through any smaller cyclotomic extension. Using the isomorphism $\mathrm{Gal}(\mathbf{Q}(\zeta_N)/\mathbf{Q}) \simeq (\mathbf{Z}/N\mathbf{Z})^\times$, we can identify ψ with a Dirichlet character mod N and the above considerations show that it is primitive. In conclusion, we showed that there is a natural correspondence
$$\left\{\begin{array}{c}\text{Representations } \psi : G_{\mathbf{Q}} \to \mathbf{C}^\times \\ \text{of conductor } N\end{array}\right\} \leftrightarrow \left\{\begin{array}{c}\text{Dirichlet characters } \chi : (\mathbf{Z}/N\mathbf{Z})^\times \to \mathbf{C}^\times \\ \text{of conductor } N\end{array}\right\}.$$

More generally, a one-dimensional representation $\rho : G_K \to \mathbf{C}^\times$ of conductor $\mathfrak{m}$ will correspond to a primitive Hecke character mod $\mathfrak{m}$ by class field theory.

2.3. Artin L-functions

Recall that a Dirichlet character $\chi : (\mathbf{Z}/N\mathbf{Z})^\times \to \mathbf{C}^\times$ has an associated L-function

$$L(\chi, s) = \sum_{n \geq 1} \chi(n) n^{-s} = \prod_p \left(1 - \chi(p)p^{-s}\right)^{-1}$$

with an appropriate functional equation. Dirichlet characters are just one-dimensional representations $G_{\mathbf{Q}} \to \mathbf{C}^\times$: in this section we will define an L-function for every Artin representation of G_K for a number field K. Rather than defining the coefficients directly we will prescribe the Euler factors and look at one prime at a time.

Let $\rho : G_K \to \mathrm{GL}(V)$ be a complex representation with K a number field. For a prime $\mathfrak{p}$ in K, let $\rho_\mathfrak{p}$ be the restriction of ρ at the decomposition group $D_\mathfrak{p}$ of $\mathfrak{p}$ (after a choice of an embedding $\overline{K} \hookrightarrow \overline{K}_\mathfrak{p}$). Define the local factor at $\mathfrak{p}$ to be

$$L_\mathfrak{p}(\rho, s) = \det\left(1 - N(\mathfrak{p})^{-s}\left(\rho|_{V^{I_\mathfrak{p}}}\right)(\mathrm{Frob}_\mathfrak{p})\right)^{-1}, \tag{2.2}$$

where $N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$ is the absolute norm, $V^{I_\mathfrak{p}}$ is the subspace of V fixed by the inertia subgroup $I_\mathfrak{p}$ at $\mathfrak{p}$ and $\mathrm{Frob}_\mathfrak{p}$ a choice of Frobenius at $\mathfrak{p}$. Since $\mathrm{Frob}_\mathfrak{p}$ is a well-defined element of $D_\mathfrak{p}/I_\mathfrak{p}$ up to conjugacy the above expression is independent of the choice of prime above $\mathfrak{p}$ and choice of Frobenius.

Definition 2.3.1. The Artin L-function of an Artin representation $\rho : G_K \to GL(V)$ is defined by

$$L(\rho, s) = \prod_\mathfrak{p} L_\mathfrak{p}(\rho, s),$$

where the product is over all prime ideals of K and the local factors $L_\mathfrak{p}(\rho, s)$ are given by equation 2.2.

Example 2.3.2. Suppose $\rho : G_K \to \mathbf{C}^\times$ is one-dimensional. Then the local factors for a prime $\mathfrak{p}$ of K are as follows:

$$L(\rho_\mathfrak{p}, s) = \begin{cases} (1 - N(\mathfrak{p})^{-s}\rho(\mathrm{Frob}_\mathfrak{p}))^{-1} & \text{if } \mathfrak{p} \text{ is unramified,} \\ 1 & \text{otherwise.} \end{cases} \tag{2.3}$$

In particular if $K = \mathbf{Q}$ we obtain the L-function of the associated Dirichlet character.

Proposition 2.3.3. The Artin L-function of a representation converges on some half-plane $\Re(s) > a$ $(a > 0)$ and satisfies the following properties:

1. (Additivity) If

   $$0 \longrightarrow (\rho', V') \longrightarrow (\rho, V) \longrightarrow (\rho'', V'') \longrightarrow 0$$

   is a short exact sequence of Artin representations then

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

2. (Induction) If L/K is a finite extension, $\rho : G_L \to GL(V)$ a repersentation and σ the induced representation on G_K then $L(\rho, s) = L(\sigma, s)$.

Proof. See [Del73, §3] or [Mar77, §1]. □

Example 2.3.4. If $\rho : G_L \to \mathbf{C}^\times$ is the trivial representation then

$$L(\rho, s) = \zeta_L(s)$$

is the Dedekind zeta function of L. Now suppose that L/K is a finite Galois extension and $r_{L/K}$ the regular representation of $\mathrm{Gal}(L/K)$. On the one hand $r_{L/K}$ is induced from the trivial representation, on the other hand it decomposes as a direct sum of irreducible representations of $\mathrm{Gal}(L/K)$ which can be seen as representations of G_K. By proposition 2.3.3 we obtain

$$\zeta_L(s) = \prod_{i=1}^{n} L(\rho_i, s)^{d_i} \tag{2.4}$$

where $\rho_1, \ldots, \rho_n$ are the irreducible representations of $\mathrm{Gal}(L/K)$ of degree $d_1, \ldots, d_n$ respectively.

If $\chi : G_K \to \mathbf{C}^\times$ is a one-dimensional representation then χ corresponds to a class character and we know (theorem 1.3.3) that the complete L-function is entire (if χ is nontrivial) and satisfies a functional equation. To state the functional equation for general $\rho : G_K \to \mathrm{GL}(V)$ we need to define the Gamma factors at infinity. It is convenient to define

$$\Gamma_{\mathbf{C}}(s) = 2(2\pi)^{-s}\Gamma(s),$$
$$\Gamma_{\mathbf{R}}(s) = \pi^{-s/2}\Gamma(s/2).$$

This allows us to restate the duplication formula in an elegant way: $\Gamma_{\mathbf{C}}(s) = \Gamma_{\mathbf{R}}(s)\Gamma_{\mathbf{R}}(s+1)$.

Now suppose that v is an infinite place. Recall that this is an equivalence class of archimedean absolute values on K or which amounts to the same thing, a real embedding $K \to \mathbf{R}$ or a pair of complex conjugate embeddings $K \to \mathbf{C}$. Note that each real place defines an element $c \in G_K$ of order two, the restriction of complex conjugation under an embedding $\bar{K} \to \mathbf{C}$ extending the given embedding $K \to \mathbf{R}$. This c is a well-defined element of G_K up to conjugation and we say c is a complex conjugation associated to v. For each infinite place v, define the local factor at v to be

$$L_v(\rho, s) = \begin{cases} \Gamma_{\mathbf{C}}(s)^{\deg(\rho)} & \text{if } v \text{ is complex,} \\ \Gamma_{\mathbf{R}}(s)^a \Gamma_{\mathbf{R}}(s+1)^b & \text{if } v \text{ is real.} \end{cases} \tag{2.5}$$

where a, b are the dimensions of the $+1$ and -1 eigenspace of $\rho(c)$ where c is a complex conjugation associated to v. We set

$$L_\infty(\rho, s) = \prod_{v \text{ infinite}} L_v(\rho, s)$$

Now if $\mathfrak{f}(\rho)$ is the Artin conductor of ρ, set

$$A(\rho) = |\Delta_K|^{\deg(\rho)} N_{K/\mathbf{Q}}(\mathfrak{f}(\rho)), \tag{2.6}$$

which is the Artin conductor of the induced representation on $G_{\mathbf{Q}}$.

Definition 2.3.5. The complete L-function of an Artin representation $\rho : G_K \to GL(V)$ is defined as

$$\Lambda(\rho, s) = A(\rho)^{s/2} L_\infty(\rho, s) L(\rho, s). \tag{2.7}$$

Theorem 2.3.6. The complete Artin L-function satisfies properties 1 and 2 of proposition 2.3.3 i.e. it is additive and inductive. Moreover, $\Lambda(\rho, s)$ has a meromorphic continuation to the whole complex plane and satisfies the functional equation

$$\Lambda(\rho, 1-s) = W(\rho)\Lambda(\rho^*, s), \tag{2.8}$$

where ρ^* is the contragradient representation and $W(\rho) \in \mathbf{C}$ is a constant of absolute value 1.

Remark 2.3.7. The constant $W(\rho)$ is called the Artin root number.

Details of the proof can be found in [Mar77, §1.4]. Let's indicate how one could prove this result. The fact that $\Lambda(\rho, s)$ is well behaved under short exact sequences and induced representations follows from the corresponding properties of the Artin conductor, the duplication formula and proposition 2.3.3. By Brauer's induction theorem [Ser77, §10.5] the character of ρ is an integer linear combination of induced characters of one-dimensional representations on finite index subgroups of G_K. So we can write

$$L(\rho, s) = \prod_j L(\chi_j, s)^{m_j}$$

with χ_j one-dimensional representations and $m_j \in \mathbf{Z}$ (not necessarily positive). This reduces to the case of one-dimensional representations, which has already been established (see theorem 1.3.3).

Example 2.3.8. Suppose $K = \mathbf{Q}$ and $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{C})$ is two-dimensional. Suppose furthermore that ρ is odd: this means that $\det(\rho(c)) = -1$ for any complex conjugation $c \in G_Q$. Since c has order two we can conjugate c to the matrix $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. If M is the conductor of ρ, we see that the complete L-function is

$$\Lambda(\rho, s) = M^{s/2}\Gamma_{\mathbf{R}}(s)\Gamma_{\mathbf{R}}(s+1)L(\rho, s) \tag{2.9}$$

$$= M^{s/2}\Gamma_{\mathbf{C}}(s)L(\rho, s). \tag{2.10}$$

It is important to remark that the above theorem does not assert that $\Lambda(\rho, s)$ is entire, since the $m_j \in \mathbf{Z}$ obtained from Brauer's induction theorem could be negative. It seems appropriate to mention the following conjecture:

Conjecture 2.3.9 (Artin)**.** If ρ doesn't contain the trivial representation then $L(\rho, s)$ is entire.

The most common ways of proving that a representation $L(\rho, s)$ satisfies the Artin conjecture is by proving that it is induced from a one-dimensional representation or that it comes from a modular (or more generally, automorphic) form, as we will explain in the next chapter (corollary 3.5.2).

2.4. Chebotarev density theorem

It is often useful to know that primes are uniformly spread in different ways. For example if $a, n \in \mathbf{Z}_{\geq 1}$ are coprime natural numbers then the density of primes congruent to $a \mod n$ is roughly $\frac{1}{\phi(n)}$ by a theorem of Dirichlet. More precisely, if $\mathcal{P}$ denotes the set of prime ideals in a number field K, we define the *natural density* of a subset $X \subset \mathcal{P}$ as

$$d(X) = \lim_{x \to \infty} \frac{|\{\mathfrak{p} \in X \mid N_{K/\mathbf{Q}}(\mathfrak{p}) \leq x\}|}{|\{\mathfrak{p} \in \mathcal{P} \mid N_{K/\mathbf{Q}}(\mathfrak{p}) \leq x\}|}$$

provided that the limit exists. We define the *Dirichlet density* of $X \subset \mathcal{P}$ as

$$\delta(X) = \lim_{s \xrightarrow{+} 1} \frac{\sum_{\mathfrak{p} \in \mathcal{P}} N_{K/\mathbf{Q}}(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p} \in \mathcal{P}} N_{K/\mathbf{Q}}(\mathfrak{p})^{-s}}$$

provided that the limit exists. The precise statement of Dirichlet's theorem says that for a, n coprime we have

$$\delta\left(\left\{p \in \mathcal{P} \mid p \equiv a \mod n\right\}\right) = \frac{1}{\phi(n)}$$

In fact a similar result for natural density holds but this is harder to prove. Roughly speaking, proving a result on Dirichlet density requires proving that a certain L-function doesn't vanish at $s = 1$, while proving a result on natural density requires proving that an L-function doesn't vanish on the line $\Re(s) = 1$ (this is exactly what happens in the proof of Dirichlet's theorem).

Chebotarev density theorem is a generalization of Dirichlet's theorem for finite Galois extensions of number fields L/K. The starting point is that the extension $\mathbf{Q}(\zeta_n)/\mathbf{Q}$ has Galois group $(\mathbf{Z}/n\mathbf{Z})^\times$ where a prime $p \in (\mathbf{Z}/n\mathbf{Z})^\times$ corresponds to the element $(\zeta_n \mapsto \zeta_n^p) \in \mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$. So a distribution of prime numbers mod n is the same as studying Frobenii in $\mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$. Recall that if $\mathfrak{p}$ is a prime of K which is unramified in L then for every prime $\mathfrak{P}$ above $\mathfrak{p}$ in L there exists an element $\mathrm{Frob}_{\mathfrak{P}|\mathfrak{p}} \in \mathrm{Gal}(L/K)$, a Frobenius at $\mathfrak{p}$, such that for all $x \in \mathcal{O}_L$ we have

$$x^{\mathrm{Frob}_{\mathfrak{P}|\mathfrak{p}}} \equiv x^{N(\mathfrak{p})} \mod \mathfrak{P}$$

where $N(\mathfrak{p})$. Different choices of $\mathfrak{P}$ above $\mathfrak{p}$ give conjugate elements of the Galois group, so we will think of $\mathrm{Frob}_\mathfrak{p}$ as being well-defined up to conjugacy.

Theorem 2.4.1 (Chebotarev density theorem)**.** Let L/K be a finite Galois extension of number fields and let $\mathcal{P}$ denote the set of nonzero prime ideals in $\mathcal{O}_K$. Let C be a conjugacy class of $\mathrm{Gal}(L/K)$. Then

$$\delta\left(\left\{\mathfrak{p} \in \mathcal{P} \mid \mathfrak{p} \text{ is unramified and } \mathrm{Frob}_\mathfrak{p} \in C\right\}\right) = \frac{|C|}{|G|}$$

Proof. See [Neu99, §13.4]. □

Remark 2.4.2. The corresponding statement for natural density holds as well but is less relevant for our purposes.

2.5. The Brauer-Nesbitt theorem and representations mod p

We will need the following facts from representation theory in the next chapter.

Theorem 2.5.1 (Brauer-Nesbitt)**.** Let k be a field and A a unital associative k-algebra. Let M, N be A-modules which are of finite dimension over k. Then the following are equivalent:

1. M and N have the same composition factors (as A-modules)
2. for all $a \in A$ the characteristic polynomials of the k-linear maps $M \xrightarrow{m \mapsto a \cdot m} M$ and $N \xrightarrow{n \mapsto a \cdot n} N$ are equal.

Proof. See [CR62, Proposition 30.16]. □

The theorem of Brauer-Nesbitt, together with Chebotarev density theorem implies that Galois representations are determined by Frobenii:

Corollary 2.5.2. Let K be a number field and F a topological field. Let $\rho, \rho' : G_K \to \mathrm{GL}_d(F)$ be (continuous) semisimple representations. Let X be a set of primes of K of density one such that for all $\mathfrak{p} \in X$, ρ and ρ' are unramified at $\mathfrak{p}$ and such that the characteristic polynomials of $\rho(\mathrm{Frob}_\mathfrak{p})$ and $\rho'(\mathrm{Frob}_\mathfrak{p})$ agree. Then ρ and ρ' are isomorphic.

Proof. By Chebotarev density theorem, the set of all Frobenii coming from X is dense in G_K. Since ρ and ρ' are continuous and the map $\mathrm{GL}_d(F) \to F[x]$ sending a matrix to its characteristic polynomial is continuous, we see that the characteristic polynomials of $\rho(g)$ and $\rho'(g)$ are the same for all $g \in G_K$ hence by Brauer-Nesbitt ρ and ρ' are isomorphic. □

Remark 2.5.3. If F has characteristic zero, the characteristic polynomial of a matrix $A \in \mathrm{GL}_d(F)$ is determined by the elements $Tr(A^k)$ $(k = 1 \dots d)$ so we only have to assume the traces agree (a well-known fact in classical representation theory of finite groups over $\mathbf{C}$).

2.5.1. Splitting fields and reducing representations mod p

Let G be a finite group and let K be a number field which is a splitting field for G (i.e. every representation $G \to \mathrm{GL}_d(K)$ is irreducible over K if and only if it is irreducible over $\bar{K}$). Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime above $p \in \mathbf{Q}$. Write $\mathcal{O}_\mathfrak{p}$ for the localization of $\mathcal{O}_K$ at $\mathfrak{p}$. Let $k_\mathfrak{p} = \mathcal{O}_\mathfrak{p}/\mathfrak{p}$ be the residue field.

Lemma 2.5.4. Suppose $p \nmid |G|$ and let ρ, τ be irreducible $\mathcal{O}_\mathfrak{p}$-representations of G (i.e. morphisms $G \to \mathrm{GL}_d(\mathcal{O}_\mathfrak{p})$). Then composing ρ, τ with the projection $\mathrm{GL}_d(\mathcal{O}_\mathfrak{p}) \to \mathrm{GL}_d(k_\mathfrak{p})$ yields absolutely irreducible representations $\tilde{\rho}, \tilde{\tau}$. Moreover, we have

$$\rho \simeq \tau \Leftrightarrow \tilde{\rho} \simeq \tilde{\tau}$$

Proof. See [Fei67, §4.3]. □

We will need the following theorem in the proof of theorem 3.1.1.

Theorem 2.5.5. Assume $p \nmid |G|$. Then the reduction mod $\mathfrak{p}$-map $\rho \mapsto \tilde{\rho}$ induces a bijection between isomorphism classes of $\mathcal{O}_\mathfrak{p}$-representations of G and $k_\mathfrak{p}$-representations of G. Moreover, ρ is abolutely irreducible if and only $\tilde{\rho}$ is.

Proof. By lemma 2.5.4, we know the map is injective. Since $p \nmid |G|$ the number of p-regular conjugacy classes of G equals the number of conjugacy classes so reduction mod $\mathfrak{p}$ induces a bijection on the isomorphism classes of irreducible representations of G, so on all representations by complete reducibility. □

We conclude this section with a reassuring result on splitting fields of finite groups.

Theorem 2.5.6. If $|G| = n$ then $\mathbf{Q}(\zeta_n)$ is a splitting field for G.

Proof. See [Ser77, §13.1]. □

3. The Deligne-Serre construction

3.1. Main Result

The similarity between the L-functions of a newform of type $(1, \chi)$ and a two-dimensional odd Artin representation (theorem 1.1.3 and example 2.3.8) gives us a reason to believe that these two seemingly different objects are related. In 1974, Deligne and Serre [DS74] showed that for every newform f on $\Gamma_0(N)$ of type $(1, \chi)$ there exists an irreducible two-dimensional $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{C})$ such that $L(f, s) = L(\rho, s)$. This chapter will be devoted to the precise statement and proof of this result.

For each prime p of $\mathbf{Q}$, choose a Frobenius $\mathrm{Frob}_p \in G_{\mathbf{Q}}$. Recall that if a representation $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(F)$ is unramified at p, then $\rho(\mathrm{Frob}_p)$ is a well-defined element of $\mathrm{GL}_2(F)$ up to conjugacy.

Theorem 3.1.1. Let χ be a Dirichlet character mod N with $\chi(-1) = -1$. Let $f \in M_1(N, \chi)$ be a nonzero modular form satisfying $T_p f = a_p f$ for all primes p not dividing N. Then there exists a representation

$$\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{C})$$

which is unramified outside N such that for all $p \nmid N$ we have

$$\det(1 - \rho(\mathrm{Frob}_p)T) = 1 - a_p T + \chi(p)T^2. \tag{3.1}$$

Moreover, ρ is irreducible if and only if f is a cusp form.

Remark 3.1.2. If such a representation exists, it is unique up to conjugacy in $\mathrm{GL}_2(\mathbf{C})$ by corollary 2.5.2.

The proof will be presented as follows: first we will give an outline of the proof combining several claims which will be assumed at first. The next sections will be devoted to explaining these intermediate steps.

Proof of theorem 3.1.1. If f is an Eisenstein series, the result is clear since we have an explicit description of the eigenforms by theorem 1.2.2. Indeed, the $\mathbf{T}_{(N)}$-eigenspace containing f contains some $E_1^{\chi_1,\chi_2}(z)$ where $\chi = \chi_1\chi_2$ is a Dirichlet character mod M dividing N and its L-function is $L(\chi_1, s)L(\chi_2, s)$ so the reducible representation $\rho = \chi_1 \oplus \chi_2$ satisfies equation 3.1.

From now on, assume that f is a cusp form. By theorem 1.4.1, there is a number field K containing all the eigenvalues a_p and values of the character $\chi(p)$ for $p \nmid N$, which we can assume to be Galois over $\mathbf{Q}$. Define $\mathcal{L}$ to be the set of primes $p \in \mathbf{Z}$ which split completely in K. By Chebotarev density theorem, this set is infinite. For each $l \in \mathcal{L}$, choose a prime λ_l in K above l. By construction, the residue field of λ_l is isomorphic to $\mathbf{F}_l$.

Assumption 1. "There exists a semisimple representation

$$\rho_l : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F}_l)$$

which is unramified outside Nl such that for each prime $p \nmid Nl$ we have

$$\det(1 - \rho_l(\mathrm{Frob}_p)T) \equiv 1 - a_pT + \chi(p)T^2 \mod \lambda_l\text{"}$$

Write G_l for the image of ρ_l in $\mathrm{GL}_2(\mathbf{F}_l)$.

Assumption 2. "There is a constant A such that $|G_l| \leq A$ for all $l \in \mathcal{L}$ "

Fix such a constant A. Note that adding finitely many elements of $\overline{\mathbf{Q}}$ to K and taking its Galois closure can only make $\mathcal{L}$ smaller. So there is no harm in assuming that K contains all n-th roots of unity, for $n \leq A$. Set

$$Y = \left\{(1 - \alpha T)(1 - \beta T) \mid \alpha, \beta \text{ roots of unity of order } \leq A\right\}.$$

Now fix a prime p not dividing N. For every prime $l \neq p$, we know that $\rho_l(\mathrm{Frob}_p) \in \mathrm{GL}_2(\mathbf{F}_l)$ has order at most A and the eigenvalues of its characteristic polynomial are roots of unity in $\overline{\mathbf{F}}_l$, which are reductions of roots of unity in $\overline{\mathbf{Q}}$. In other words, we have

$$1 - a_pT + \chi(p)T^2 \equiv det(1 - \rho(\mathrm{Frob}_p)T) \equiv R(T) \mod \lambda_l$$

for some $R(T) \in Y$. Since a similar congruence holds for every $l \in \mathcal{L}$ and since Y is a finite set, there is a fixed element of Y such that the congruence holds for infinitely many primes λ_l with $l \in \mathcal{L}$. This implies genuine equality, so $1 - a_pT + \chi(p)T^2 \in Y$. Here we use that if two elements in $\mathcal{O}_K$ are congruent modulo infinitely many primes, they are equal. Continuing with this idea, set

$$\mathcal{L}' = \left\{l \in \mathcal{L} \mid l > A \text{ and } \forall R, S \in Y : R \neq S \Rightarrow R \not\equiv S \mod \lambda_l\right\}.$$

The set $\mathcal{L} \setminus \mathcal{L}'$ is contained in the set of all primes l for which $R \equiv S \mod \lambda_l$ for some $R, S \in Y$ with $R \neq S$. This happens only finitely many times so $\mathcal{L} \setminus \mathcal{L}'$ is finite, hence the set $\mathcal{L}'$ is infinite. Fix a prime $l \in \mathcal{L}'$. Since $|G_l| \leq A$, the prime l doesn't divide $|G_l|$. By theorem 2.5.5, the representation $G_l \to \mathrm{GL}_2(\mathbf{F}_l)$ is the reduction of a representation $G_l \to \mathrm{GL}_2(\mathcal{O}_{\lambda_l})$. So the composite

$$\rho : G_{\mathbf{Q}} \to G_l \to \mathrm{GL}_2(\mathcal{O}_{\lambda_l}) \hookrightarrow \mathrm{GL}_2(\mathbf{C})$$

is a continous representation of $G_{\mathbf{Q}}$ which is unramified outside of Nl. But for a prime p not dividing Nl, $\det(1 - \rho(\mathrm{Frob}_p)T)$ belongs to Y since $|G_l| \leq A$ and

$$\det(1 - \rho(\mathrm{Frob}_p)T) \equiv 1 - a_pT + \chi(p)T^2 \mod \lambda$$

so by definition of $\mathcal{L}'$ (since both sides are elements of Y) we deduce equality on the characteristic zero level i.e.

$$\det(1 - \rho(\mathrm{Frob}_p)T) = 1 - a_pT + \chi(p)T^2, \ \forall p \nmid Nl$$

We play the same game for a different $l' \in \mathcal{L}'$ and obtain a representation $\rho' : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{C})$ which is unramified outside Nl' and satisfies $\det(1 - \rho'(\mathrm{Frob}_p)T) = 1 - a_pT + \chi(p)T^2$ for all p not dividing Nl'. Corollary 2.5.2 implies that ρ and ρ' are isomorphic and so equation 3.1 holds for all p not dividing N. So the representation ρ satisfies equation 3.1 for all primes $p \nmid N$ and is unramified outside N.

The last step in the proof is to show that ρ is irreducible. Suppose not, then it would be the sum of two one-dimensional representations χ_1 and χ_2. So that $a_p = \chi_1(p) + \chi_2(p)$. But then

$$\sum_{p \nmid N} |a_p|^2 p^{-s} = 2\sum_{p \nmid N} p^{-s} + \sum_{p \nmid N} \chi_1(p)\bar{\chi_2}(p)p^{-s} + \sum_{p \nmid N} \bar{\chi_1}(p)\chi_2(p)p^{-s}$$

Now $\chi_1 \neq \chi_2$ since $\chi = \chi_1\chi_2$ satisfies $\chi(-1) = -1$. This implies that

$$2\sum_{p\nmid N} p^{-s} = 2\log\left(\frac{1}{s-1}\right) + O(1) \quad (s \xrightarrow{>} 1)$$

$$\sum_{p\nmid N} \chi_1(p)\bar{\chi_2}(p)p^{-s} = O(1) \quad (s \xrightarrow{>} 1)$$

But this contradicts the following estimate:

Assumption 3. "The sum $\sum_{p\nmid N}|a_p|^2p^{-s}$ converges for $\Re(s) > 1$ and

$$\sum_{p\nmid N}|a_p|^2p^{-s} \leq \log\left(\frac{1}{s-1}\right) + O(1) \qquad (s \xrightarrow{>} 1)."$$

We conclude that ρ is irreducible and the proof is complete. □

The next sections will get rid of the assumptions made in the previous proofs. Section 3.2 will prove assumption 1. Section 3.3 will prove assumption 3. Section 3.4 (using some results from section 3.3) will prove assumption 2.

3.2. l-adic and mod l representations

In the proof of theorem 3.1.1 we assumed for every prime $l \in \mathcal{L}$ the existence of a semisimple representation $G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F}_l)$ where the equality 3.1 was true mod λ_l for all primes p not dividing Nl. For a modular form of weight $k \geq 2$, such representations can be acquired by starting with an l-adic representation (as given by theorem 3.2.1 below), reducing it mod l and taking its semisimplification. For a modular form f of weight one, we don't have such representations but we can use the following trick: we multiply f by an Eisensten series $E_k \in M_k(\mathrm{SL}_2(\mathbf{Z}))$ to get a modular form fE_k of weight $k+1$. If f is an eigenformn E_kf need not to be one but by choosing k appropriately we can make it to be an eigenform modulo a prime l. This will turn out to be sufficient for our purposes.

3.2.1. l-adic representations

Recall (theorem 1.4.1) that the eigenvalues of the Hecke operators are algebraic integers which generate a field extension of $\mathbf{Q}$ of finite degree.

Theorem 3.2.1 (Deligne)**.** Let $k \geq 2$ and $f \in M_k(N, \chi)$ be a nonzero modular form such that $T_pf = a_pf$ (with $a_p \in \mathbf{C}$) for all $p \nmid N$. Let K be a number field containing a_p and $\chi(p)$ for all $p \nmid N$. For a rational prime $l \in \mathbf{Z}$, let λ be a prime in K above l. Let K_λ the λ-adic completion of K. Then there exists a unique semisimple representation

$$\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(K_\lambda)$$

which is unramified outside Nl such that for all $p \nmid Nl$ we have

$$\det(1 - \rho(\mathrm{Frob}_p)T) = 1 - a_pT + \chi(p)p^{k-1}T^2 \tag{3.2}$$

Proof. See [Del71] □

Remark 3.2.2. By corollary 2.5.2, ρ is unique up to isomorphism. Since $\det(\rho(\mathrm{Frob}_p)) = \chi(p)p^{k-1}$, the representation does not have finite image (since $k \geq 2$).

The case $k = 2$ is rather explicit and was known by Shimura. Deligne proved the general case using techniques from étale cohomology.

3.2.2. Reduction mod l

Before we state the theorem, let's introduce some notation. Let K be a number field with ring of integers $\mathcal{O}_K$. We will always see number fields as subfields of $\mathbf{C}$. Let λ be a prime of $\mathcal{O}_K$ above $l \in \mathbf{Z}$. Write $\mathcal{O}_\lambda$ for the localization of $\mathcal{O}_K$ at λ. It is a discrete valuation ring with maximal ideal m_λ and residue field k_λ.

We will use the concept of a modular form on $\overline{\mathbf{F}}_l$, but only implicitly and the naive definition will suffice for our purposes. Say a modular form $f \in M_k(N, \chi)$ is λ-integral (resp. $f \equiv 0 \mod \lambda$) if its Fourier coefficients at infinity $\{a_n\}_{n\geq 0}$ are in $\mathcal{O}_\lambda$ (resp. in m_λ). If f is λ-integral, say f is an eigenvector of $T_p \bmod \lambda$ with eigenvalue $a_p \in k_\lambda$ if $T_p f - a_p f \equiv 0 \mod \lambda$.

The following theorem is the main result of this section.

Theorem 3.2.3. With the above notation, let $f \in M_k(N, \chi)$ be a modular form with Fourier coefficients in K. Suppose that f is λ-integral, $f \not\equiv 0 \mod \lambda$ and f is an eigenvector of $T_p \bmod \lambda$ with eigenvalue $a_p \in k_\lambda$ for all primes $p \nmid Nl$. Let k_f be the subfield of k_λ generated by the elements a_p and the reductions of $\chi(p)$ for $p \nmid Nl$.

Then there exists a semisimple representation

$$\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(k_f)$$

which is unramified outside of Nl such that for all primes $p \nmid Nl$ we have

$$\det(1 - \rho(\mathrm{Frob}_p)T) = 1 - a_p T + \chi(p)p^{k-1}T^2 \mod \lambda \tag{3.3}$$

Proof. We will proceed in several steps.

Step 1. First of all, note that there is no harm in changing f and K as long as the conclusion of the theorem doesn't change. More precisely, suppose we are given the data $(K', \lambda', f', \chi', (a'_p))$ with the same notation and assumptions as in the statement of the theorem such that K' contains K, the prime λ' lies above λ and

$$a_p \equiv a'_p \mod \lambda'$$
$$p^{k-1}\chi(p) \equiv p^{k'-1}\chi'(p) \mod \lambda'$$

for all $p \nmid Nl$. Then proving the theorem for f is equivalent with proving it for f', since the conditions imposed on the sought representation are equivalent for f and f'.

Step 2. Next, we show that we only have to prove the theorem for weight k at least two. Indeed, suppose that $k = 1$, so $f \in M_1(N, \chi)$. Let E_n be the normalized Eisenstein series on $\mathrm{SL}_2(\mathbf{Z})$ of weight n:

$$E_n(z) = 1 - \frac{2n}{B_n}\sum_{n\geq 1}\sigma_{n-1}(m)q^m.$$

We want to find an n such that $fE_n \equiv f \mod \lambda$. By the theorem of Von Staudt-Clausen (see theorem A.1.1 in the appendix), we know that when B_n is written as a fraction in lowest terms, its denominator is the product of all primes p such that $p-1$ divides n. So it suffices to choose $n = l-1$ and we have

$$fE_n \equiv f \mod \lambda.$$

Now $n+1 \equiv 1 \mod l-1$ so $\chi(p)p^{(n+1)-1} \equiv \chi(p)p^{1-1} \mod \lambda$ so the conditions of Step 1 are satisfied, and proving the theorem for f is equivalent with proving it for fE_n. So from now on, assume that the weight k is at least two.

Step 3. We now have an $f \in M_k(N,\chi)$ which is an eigenform mod λ, but to apply theorem 3.2.1 we need a genuine eigenform. We invoke the following lemma, whose proof is purely algebraic and will be given in the appendix (theorem A.2.1).

Lemma 3.2.4 (Deligne-Serre lifting lemma)**.** Let $\mathcal{O}$ be a discrete valuation ring with maximal ideal m, residue field $k = \mathcal{O}/m$ and fraction field K. Let M be a free $\mathcal{O}$-module of finite rank. Let $\mathcal{T} \subset \mathrm{End}_{\mathcal{O}}(M)$ be a commuting family of endomorphisms of M. Suppose $0 \neq f \in M/mM$ satisfies $T(f) = a_T f$ $(a_T \in k)$ for all $T \in \mathcal{T}$.

Then there is a discrete valutation ring $\mathcal{O}'$ with maximal ideal m' where $\mathcal{O} \subset \mathcal{O}'$, $m' \cap \mathcal{O} = m$ and the fraction field of $\mathcal{O}'$ is a finite extension of K such that the system of eigenvalues $\{a_T\}_{T\in\mathcal{T}}$ has a lift to $M' = M \otimes_{\mathcal{O}} \mathcal{O}'$: there exists a nonzero $f' \in M'$ such that

$$T(f') = a'_T f' \quad \forall T \in \mathcal{T}$$

with $a'_T \in \mathcal{O}'$ such that $a'_T \equiv a_T \mod m'M'$.

Note that we do not assert that $\tilde{f}$ lifts f: it is the eigenvalues of f that have lifts but this is enough to apply Step 1. Indeed, apply the lemma to the case where $\mathcal{O} = \mathcal{O}_\lambda$, $\mathcal{T} = \{T_p \mid p \nmid Nl\}$ and M the $\mathcal{O}_\lambda$-module of λ-integral forms in $M_k(N,\chi)$. By lemma 1.4.2, M is a free $\mathcal{O}_\lambda$-module of finite type and behaves well under base change. We know by definition that the coefficients q-expansion of $T_p f - a_p f$ lie in m_λ. Let $\pi \in \mathcal{O}_\lambda$ be a generator of m_λ. Then we know that $T_p f - a_p f = \pi g$ where g is a λ-integral form. This shows that $f \in M/m_\lambda M$ indeed satisfies the conditions of the Deligne-Serre lifting lemma[1]. This implies that there is a modular form f' which is an eigenform for all T_p $(p \nmid Nl)$ for which clearly the conditions of Step 1 are satisfied. We conclude that we may assume that f is an eigenform for T_p $(p \nmid Nl)$ with eigenvalue a_p.

Step 4. If l does not divide N then T_l is semisimple and commutes with T_p for $p \nmid Nl$ so we may assume that f is an eigenform of all the Hecke operators T_p with $p \nmid N$ with eigenvalue a_p. By theorem 3.2.1 there exists a semisimple representation

$$\rho_\lambda : G_{\mathbf{Q}} \to \mathrm{GL}_2(K_\lambda)$$

satisfying equation 3.2 of the theorem. The λ-adic completion $\widehat{\mathcal{O}}_\lambda$ of $\mathcal{O}_\lambda$ is a PID with fraction field K_λ, so we may suppose (see lemma 2.1.4) that ρ_λ takes values in $\mathrm{GL}_2(\widehat{\mathcal{O}}_\lambda)$. Reducing mod λ we get a representation $\tilde{\rho}_\lambda : G_{\mathbf{Q}} \to \mathrm{GL}_2(k_\lambda)$. Taking the semi-simplification of $\tilde{\rho}$ (the sum of its Jordan-Hölder factors), we obtain a semi-simple representation

$$\phi : G_{\mathbf{Q}} \to \mathrm{GL}_2(k_\lambda).$$

[1]The last three sentences are necessary because it is a priori not obvious that a λ-integral form which has coefficients of its q-expansion in m_λ lies in $m_\lambda M$. Otherwise put, an argument is needed why the canonical map $M/m_\lambda M \to (\mathcal{O}_\lambda/m_\lambda)[[q]]$ is injective. This is called the 'q-expansion principle' and is explained in [DI94, §12.3].

Since ρ_λ is unramified outside of Nl it factors through a (possibly infinite) Galois extension $K/\mathbf{Q}$ which is unramified outside Nl. So the same is true for ρ_λ hence ϕ as well, which shows that ϕ is unramified outside Nl. By construction, the equation 3.3 is satisfied.

Step 5. The last thing to show is that ϕ is realizable over k_λ. But since k_λ is a finite field, this amounts to proving that $\phi^\sigma \simeq \phi$ for all $\sigma \in \mathrm{Gal}(k_\lambda/k_f)$ (because the Schur indices are always 1 by Wedderburn's theorem, see [Kar92, §14.4, Theorem 4.1]). By Brauer-Nesbitt and since all terms in equation 3.3 are in k_f we conclude that $\rho \simeq \rho^\sigma$ so the proof of the theorem is complete.

□

3.3. An application of the Rankin-Selberg method

In this section we establish an analytic result which is proved using the convolution of two Dirichlet series, nowadays called the Rankin-Selberg method. It is roughly analogous to twisting an L-series of a modular form by a dirichlet character, but in this case we 'twist' by another modular form. To illustrate the method, let f, g be normalized newforms of weight k on $\Gamma_0(N)$ with character χ and ψ respectively:

$$f = \sum_{n\geq 1} a_n q^n,$$
$$g = \sum_{n\geq 1} b_n q^n.$$

Write $L(f,s) = \sum_{n\geq 1} a_n n^{-s}$ and $L(g,s) = \sum_{n\geq 1} b_n n^{-s}$ for the associated L-functions. Since f and g are newforms, the L-functions have an Euler product which looks like

$$L(f,s) = \prod_{p|N}(1 - a_p p^{-s})^{-1} \prod_{p\nmid N} \left(1 - a_p p^{-s} + \chi(p)p^{k-1-2s}\right)^{-1}$$

and similarly for g. The goal is to derive analytic properties of the L-function $\sum_{n\geq 1} a_n b_n n^{-s} = \sum_{n\geq 1} c_n n^{-s}$. Since $a_n, b_n = O(n^{k/2})$, we know this series converges absolutely and is holomorphic on the half-plane $\Re(s) > k$. Since $a_{mn} = a_m a_n$ for m, n coprime and similarly for b_n, the same holds true for the product of the two and all the information is contained in the coefficients at the prime powers. If p is a 'bad prime' and divides N, we have $c_{p^r} = c_p^r$ hence

$$\sum_{r\geq 0} c_{p^r} p^{-rs} = (1 - c_p p^{-s})^{-1} = (1 - a_p b_p p^{-s})^{-1}.$$

If p does not divide N, the recurrence relation is a bit more involved. We invoke the following lemma:

Lemma 3.3.1. Let $(u_r)_{r\geq 0}$ and $(v_r)_{r\geq 0}$ be sequences satisfying linear recurrence relations of order two of the form

$$u_r = a u_{r-1} + b u_{r-2}$$
$$v_r = c v_{r-1} + d v_{r-2}$$

for $r \geq 2$ where $(u_0, u_1) = (1, a)$ and $(v_0, v_1) = (1, b)$. Let λ_1, λ_2 be the solutions of the equation $X^2 - aX - b$ and μ_1, μ_2 the solutions to the equation $X^2 - cX - d$. Then the sequence $(w_r)_{r\geq 0} = (u_r v_r)$ satisfies a linear recurrence relation of order four and the following identity of formal power series holds:

$$\sum_{r\geq 0} u_r v_r T^r = \frac{1 - bdT^2}{(1 - \lambda_1\mu_1 T)(1 - \lambda_1\mu_2 T)(1 - \lambda_2\mu_1 T)(1 - \lambda_2\mu_2 T)}$$

Proof. A tedious but straightforward calculation. □

In our interest, we take $u_r = a_{p^r}$ and $v_r = b_{p^r}$ (where $p \nmid N$) and so the lemma implies that we have the identity

$$\sum_{r\geq 0} a_{p^r} b_{p^r} p^{-rs} = \frac{1-\chi(p)\psi(p)p^{2k-2-2s}}{(1-\lambda'_p\mu'_p p^{-s})(1-\lambda_p\mu_p p^{-s})(1-\lambda'_p\mu_p p^{-s})(1-\lambda'_p\mu'_p p^{-s})}$$

where λ_p, λ'_p are the roots of $X^2 - a_p X + \chi(p)p^{k-1}$ and μ_p, μ'_p the roots of $X^2 - b_p X + \chi(p)p^{k-1}$.

Definition 3.3.2. The convolution of the L-series $L(f,s)$ and $L(g,s)$ is

$$L(f\otimes g, s) = \prod_{p\nmid N} (1-\lambda_p\mu_p p - s)^{-1}(1-\lambda_p\mu'_p p^{-s})^{-1}(1-\lambda'_p\mu_p p^{-s})^{-1}(1-\lambda'_p\mu'_p p^{-s})^{-1}$$

The notation $f \otimes g$ is purely formal[2]. The above calculations show that

$$L(f\otimes g, s) = L(\chi\psi, 2s+2-2k)\left(\sum_{n\geq 1} a_n b_n n^{-s}\right) \tag{3.4}$$

where $L(\chi\psi, s)$ is the L-function attached to the Dirichlet character $\chi\psi$ of modulus N. Note that if $\chi\psi$ is trivial, $L(\chi\psi, s) = \prod_{p\nmid N}(1-p^{-s})^{-1}$ is the partial zeta function $\zeta_N(s)$, defined as

$$\zeta_N(s) = \sum_{(n,N)=1} n^{-s}$$

Moreover, if $f \in S_k(N,\chi)$ is a normalized newform on $\Gamma_0(N)$ with character χ, then $z \mapsto \overline{f(-\bar{z})}$ is a normalized newform on $\Gamma_0(N)$ as well, with character $\bar{\chi}$. Its Fourier coefficients are given by the complex conjugates of those of f, so we denote this form by $\bar{f}$ (although it is not litterally the complex conjugate of f, which is not even holomorphic). Setting $g = \bar{f}$ in equation 3.4 gives

$$L(f\otimes\bar{f}, s) = \zeta_N(2s+2-2k)\left(\sum_{(n,N)=1} |a_n|^2 n^{-s}\right)$$

Adding the Euler factors at the bad primes and replacing ζ_N by ζ yields

$$L(f\otimes\bar{f}, s) = \left(\prod_{p|N}\left(1-|a_p|^2 p^{-s}\right)\left(1-p^{-2s-2+2k}\right)\right)\zeta(2s+2-2k)\left(\sum_{n\geq 1}|a_n|^2 n^{-s}\right) \tag{3.5}$$

Using non-holomorphic Eisenstein series, one can prove the following fact:

Lemma 3.3.3 (Rankin)**.** Under the above assumptions, the function $L(f\otimes\bar{f}, s)$ has a meromorphic continuation to the complex plane. It is holomorphic everywhere except at $s = k$ where it has a simple pole.

Proof. See theorem 3 of [Ogg69] or [Ran39].

□

[2]Or is it? Modular forms are related to automorphic forms on GL_2 and so $f \otimes g$ should correspond to an automorphic form on $\mathrm{GL}_2 \times \mathrm{GL}_2$, see [Ram00] and [Jac72].

We are now ready to prove the proposition needed for the main theorem.

Proposition 3.3.4. Let $f \in S_k(N,\chi)$ be a cusp form such that $T_p f = a_p f$ for all primes p not dividing N. Then the sum $\sum_{p\nmid N}|a_p|^2 p^{-s}$ converges for real $s > k$ and the following inequality holds:

$$\sum_{p\nmid N}|a_p|^2 p^{-s} \leq \log\left(\frac{1}{s-k}\right) + O(1) \quad (s \xrightarrow{+} k) \tag{3.6}$$

(meaning that the difference between the left and right hand side is bounded above as $s \xrightarrow{+} k$).

Proof. Since f is in the same $\mathbf{T}_{(N)}$-eigenspace as some newform (on a possibly lower level), we may assume f itself is a newform. Hence f has a q-expansion of the form

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

and the above discussion applies to f. Indeed, if λ_p, μ_p are the roots of the polynomial $X^2 - a_p X + \chi(p)p^{k-1}$ (for $p \nmid N$) then

$$L(f\otimes\bar{f},s) = \prod_{p\nmid N}(1-\lambda_p\bar{\lambda}_p p^{-s})^{-1}(1-\lambda_p\bar{\mu}_p p^{-s})^{-1}(1-\mu_p\bar{\lambda}_p p^{-s})^{-1}(1-\mu_p\bar{\mu}_p p^{-s})^{-1}$$

and by equation by equation 3.5:

$$L(f\otimes\bar{f},s) = H(s)\zeta(2s+2-2k)\left(\sum_{n\geq 1}|a_n|^2 n^{-s}\right),$$

where

$$H(s) = \prod_{p\,|N}\left(1-|a_p|^2p^{-s}\right)\left(1-p^{-2s-2+2k}\right).$$

By lemma 3.3.3, the function $L(f\otimes\bar{f},s)$ has a meromorphic continuation to the complex plane which is holomorphic except at $s=k$ where it has a simple pole. Since $|a_p| < p^{k/2}$ if p divides N (see proposition 1.4.3) we see that $H(s)$ has no zeros in the half-plane $\Re(s) > k$. The same is true for $\zeta(2s+2-2k)$ and $\sum|a_n|^2n^{-s}$ so $L(f\otimes\bar{f},s)$ is non-zero for $\Re(s) > k$. Now we have at least formally the following equality of Dirichlet series:

$$\log(L(f\otimes\bar{f},s)) = \sum_{p\nmid N}\sum_{m\geq 1}\frac{|\lambda_p^m+\mu_p^m|^2p^{-ms}}{m} \tag{3.7}$$

and the right hand side converges absolutely for $\Re(s) > k$ since

$$\begin{aligned}|\lambda_p^m+\mu_p^m|^2 &\leq (|\lambda_p^m|+|\mu_p^m|)^2\\ &\leq 4|\lambda_p\mu_p|^m\\ &= 4p^{m(k-1)}\end{aligned}$$

so the n-th coefficient is of order $O(n^{k-1})$. Since $L(f\otimes\bar{f},s)$ has a simple pole at $s=k$, we know that $\log((s-k)L(f\otimes\bar{f},s))$ is bounded as $s\xrightarrow{+}k$, hence

$$\begin{aligned}\sum_{p\nmid N}|a_p|^2p^{-s} &= \sum_{p\nmid N}|\lambda_p+\mu_p|^2p^{-s}\\ &\leq \sum_{p\nmid N}\sum_{m\geq 1}\frac{|\lambda_p^m+\mu_p^m|^2p^{-ms}}{m}\\ &= \log(L(f\otimes\bar{f},s))\\ &= \log\left(\frac{1}{s-k}\right)+O(1)\quad(s\xrightarrow{+}k)\end{aligned}$$

which proves the desired claim.

□

We see that for $k = 1$, this was exactly assumption 3 in the proof of theorem 3.1.1. The following proposition will be useful for the next section. It tells us in some sense that the Fourier coefficients a_p of a weight one eigenform have controllable growth. Recall that if $\mathcal{P}$ denotes the set of prime numbers, then the Dirichlet densitiy of a subset $X \subset \mathcal{P}$ is defined as

$$\delta(X) = \limsup_{s \to +1} \frac{\sum_{p \in X} p^{-s}}{\log\left(\frac{1}{s-1}\right)}$$

We always have $\delta(X) \in [0, 1]$. We use the lim sup in this definition instead of a limit to guarantee that it is well-defined for every subset $X \subset \mathcal{P}$.

Proposition 3.3.5. Using the notation of the previous proposition, assume $k = 1$. For every real $\eta > 0$ there is a finite set $Y_\eta \subset \mathbf{C}$ such that

$$\delta\left(\left\{p \in \mathcal{P} \mid a_p \in Y_\eta\right\}\right) \geq 1 - \eta. \tag{3.8}$$

Proof. We know the a_p and $\chi(p)$ are algebraic integers in a finite extension K of $\mathbf{Q}$. For each $c \geq 0$, set

$$Y(c) = \left\{a \in \mathcal{O}_K \mid |\sigma(a)|^2 \leq c,\ \forall \sigma : K \hookrightarrow \mathbf{C}\right\}.$$

Then $Y(c)$ is a finite set, since the coefficients of the minimal polynomials of elements of $Y(c)$ are bounded. It suffices to prove that $\delta(\{p \mid a_p \in Y(c)\})$ tends to 1 as $c \to \infty$. By theorem 1.4.1, we know that for each embedding $\sigma : K \to \mathbf{C}$ the coefficients $\sigma(a_p)$ are the eigenvalues of a modular form f^σ on $\Gamma_1(N)$ so proposition 3.3.4 shows that

$$\sum_\sigma \sum_{p \nmid N} |\sigma(a_p)|^2 p^{-s} \leq [K : \mathbf{Q}] \log\left(\frac{1}{s-1}\right) + O(1) \quad (s \xrightarrow{+} 1)$$

where the sum is over all embeddings $\sigma : K \to \mathbf{C}$ and all primes $p \nmid N$. If $a_p \notin Y_\eta$ then $\sum_\sigma |\sigma(a_p)|^2 \geq c$ hence

$$\sum_{a_p \notin Y(c)} p^{-s} \leq c^{-1}[K : \mathbf{Q}] \log\left(\frac{1}{s-1}\right) + O(1),$$

So $\delta(\{p \mid a_p \in Y(c)\}) \geq 1 - c^{-1}[K : \mathbf{Q}]$ which proves the proposition. □

Remark 3.3.6. Once theorem 3.1.1 is completely proven, we know that the set $\{a_p \mid p \nmid N\}$ is in fact finite!

3.4. Subgroups of $\mathrm{GL}_2(\mathbf{F}_l)$

We only have to remedy assumption 2 from the proof of theorem 3.1.1 which said that the images of the local representations $\rho_l : G_\mathbf{Q} \to \mathrm{GL}_2(\mathbf{F}_l)$ have bounded cardinality. In this section we will analyze subgroups of $\mathrm{GL}_2(\mathbf{F}_l)$ to reach the desired conclusion. First, some notation.

Definition 3.4.1. Let G be a subgroup of $\mathrm{GL}_2(\mathbf{F}_l)$ with l a prime number. We say G is semisimple if the inclusion $G \to \mathrm{GL}_2(\mathbf{F}_l)$ is a semisimple representation. If M is a positive real number, we say G is M-sparse if G has a subset $H \subset G$ such that $|H| \geq \frac{3}{4}|G|$ and

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

Proposition 3.4.2. For every $M \geq 0$, there exists an $A \geq 0$ such that $|G| \leq A$ for every prime l and every semi-simple M-sparse $G \leq \mathrm{GL}_2(\mathbf{F}_l)$.

Proof. If $G \leq \mathrm{GL}_2(\mathbf{F}_l)$ is a semi-simple subgroup, G satisfies one of the following ([Ser72, §2, Proposition 14.15] or [Dic58]):

1. G contains $\mathrm{SL}_2(\mathbf{F}_l)$ (G is big),
2. G is conjugates to a subgroup of $\left\{ \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \right\}$ (which means it stabilizes two lines in $\mathbf{F}_l^2$),
3. G conjugates to a subgroup of the normalizer of the subgroup $\left\{ \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \right\}$,
4. the image of G in $\mathrm{PGL}_2(\mathbf{F}_l)$ under the projection $\mathrm{GL}_2(\mathbf{F}_l) \to \mathrm{PGL}_2(\mathbf{F}_l)$ is isomorphic to A_4, S_4 or A_5 (exceptional).

By examining each of these cases separately, we can bound the cardinality of G, see [DS74, Proposition 7.2]. We will only illustrate the method and do the second case as an example. In this case, at most two elements of G have the same characteristic polynomial. Since G is M-sparse, we have

$$|G| \leq \frac{4}{3}|H| \leq \frac{4}{3}(2M)$$

which indeed proves that $|G|$ is bounded.

□

We can now prove assumption 3 in the proof of theorem 3.1.1. Keep the same notation as in the proof in section 3.1. So we have for each prime l splitting completely in K, a subgroup $G_l \leq \mathrm{GL}_2(\mathbf{F}_l)$. We claim that there exists an M such that G_l is M-sparse for all l. Indeed, by proposition 3.3.5 we know that there exists a finite set $Y \subset \mathbf{C}$ such that

$$\delta\left(\left\{p \in \mathcal{P} \mid a_p \in Y\right\}\right) \geq 3/4.$$

Write $X = \{p \in \mathcal{P} \mid a_p \notin Y\}$. Then $\delta(X) \leq 1/4$. Let $\mathcal{M}$ be the finite set of polynomials of the form $1 - a_p T + \chi(p)T^2$ with $p \notin X$, denote its cardinality by M. We claim that G_l is M-sparse for all $l \in \mathcal{L}$. Indeed, if H_l denotes the subset of G_l consisting of all elements $\rho_l(\mathrm{Frob}_p)$ ($p \notin X$) and their conjugates, then Chebotarev density theorem tells us that $|H_l| \geq \frac{3}{4}|G_l|$. On the other hand if $h \in H_l$ then $\det(1 - hT)$ is the reduction mod λ_l of an element of $\mathcal{M}$. So there are at most M possibilities for $\det(1 - hT)$. This proves that G_l is M-sparse for all $l \in \mathcal{L}$. By proposition 3.4.2, the cardinalities of the G_l are indeed bounded so assumption 3 is proven.

3.5. From Galois representations to modular forms

For a $\mathbf{T}_{(N)}$-eigenform $f \in S_k(N, \chi)$, write ρ_f for the two-dimensional Artin representation associated to f given by theorem 3.1.1.

Proposition 3.5.1. Let $f \in S_k(N, \chi)$ be a newform.

1. The Artin conductor of ρ_f equals N. In particular, the representation is ramified at all prime divisors of N.

2. $L(f, s) = L(\rho_f, s)$.

Proof. Write $\rho = \rho_f$ to ease the notation a bit. Let's try to exploit the functional equations of $L(f, s)$ and $L(\rho, s)$. Write $f = \sum_{n\geq 1} a_n q^n$. Let $g = f|_{\omega_N} = N^{-1/2} z^{-1} f(-1/Nz)$ and $\tilde{f} = \sum_{n\geq 1} \bar{a}_n q^n$. Since f is a newform, g and $\tilde{f}$ will be in the newspace $S_k^{new}(N, \bar{\chi})$ with the same $\mathbf{T}_{(N)}$-eigenvalues. By strong multiplicity one, there is a nonzero constant $\lambda \in \mathbf{C}$ such that $g = \lambda \tilde{f}$. By theorem 1.1.1 we obtain the functional equation

$$\Lambda_f(1 - s) = i\Lambda(g, s) = i\lambda\Lambda_{\tilde{f}}(s) \tag{3.9}$$

where $\Lambda_f(s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(f, s)$.

Let M be the conductor of ρ. Since $\det(\rho(c)) = -1$, complex conjugation acts non-trivially (we say the infinite prime of $\mathbf{Q}$ ramifies) and the correct factor at infinity is $(2\pi)^{-s}\Gamma(s)$ (proposition 2.3.6). Put

$$\xi(s) = M^{s/2}(2\pi)^{-s}\Gamma(s)L(\rho, s),$$

then the functional equation reads

$$\xi(\rho, 1 - s) = \nu\xi(\bar{\rho}, s) \tag{3.10}$$

with $\nu \in \mathbf{C}$ a nonzero constant and $\bar{\rho}$ the contragradient representation.

So set

$$F(s) = \frac{\Lambda_f(s)}{\xi(\rho, s)} = \left(\frac{N}{M}\right)^{s/2} \frac{L(f, s)}{L(\rho, s)}$$
$$\tilde{F}(s) = \frac{\Lambda_{\tilde{f}}(s)}{\xi(\bar{\rho}, s)} = \left(\frac{N}{M}\right)^{s/2} \frac{L(\tilde{f}, s)}{L(\bar{\rho}, s)}.$$

The above equations show that

$$F(1 - s) = \omega\tilde{F}(s) \tag{3.11}$$

with $\omega = i\lambda/\nu$. By the construction of ρ, the Euler factors of $\Lambda_f(s)$ and $\xi(\rho, s)$ agree if $p \nmid N$, so we can write $F(s)$ as a finite product

$$F(s) = A^s \prod_{p|N} F_p(s)$$

with $A = (N/M)^{1/2}$ and

$$F_p(s) = \frac{(1 - b_p p^{-s})(1 - c_p p^{-s})}{(1 - a_p p^{-s})}$$

where $\det(1 - \rho|_{V^{I_p}}(\mathrm{Frob}_p)) = (1 - b_p p^{-s})(1 - c_p p^{-s})$ (we allow b_p or c_p to be zero). We would be done if we could show that $F_p = 1$ for all $p \mid N$, for then the functional equation reads $A^{1-s} = A^s$ hence $A = 1$. If F_p is not equal to 1, then F_p has infinitely many zeroes or poles. Note that if $(1 - \alpha p^{-s}) = 0$ then $p^{\Re(s)} = |\alpha|$. So if $s \in \mathbf{C}$ is a zero of F_p then by the functional equation 3.11 we know that both $p^{\Re(s)}$ and $p^{1-\Re(s)}$ equal the absolute value of some α appearing in an Euler factor $(1 - \alpha p^{-s})$ of F or $\tilde{F}$. We claim that for every such α we have $|\alpha| < p^{1/2}$. This would give a contradiction since then $p^{\Re(s)}p^{1-\Re(s)} < p$. Indeed, if α comes from an Euler factor from

$L(\rho, s)$ this is clear since the eigenvalues of Frob_p are roots of unity. If $\alpha = a_p$ then this follows from proposition 1.4.3.

□

Corollary 3.5.2. For every $\mathbf{T}_{(N)}$-eigenform $f \in S_k(N, \chi)$ the representation ρ_f satisfies the Artin conjecture i.e. $L(\rho_f, s)$ is entire.

Proof. Indeed, f has the same $\mathbf{T}_{(N)}$-eigenvalues as some $g(z)$ where g is a newform in $S_k(M, \chi)$ and $M \mid N$. So we may as well assume that f is a newform. But then by proposition 3.5.1 we have $L(\rho_f, s) = L(f, s)$. Since $\Lambda_f(s) = (2\pi)^{-s}\Gamma(s)L(f, s)$ is entire (theorem 1.1.1) and $\Gamma(s)$ has no zeros the function $L(f, s)$ is entire as well. □

The assignment $f \mapsto \rho_f$ defines a map

$$\left\{\begin{matrix}\text{Newforms on } \Gamma_0(N) \\ \text{of type } (1, \chi)\end{matrix}\right\} \to \left\{\begin{matrix}\text{Irreducible representations } \rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{C}) \\ \text{of conductor } N \text{ with determinant } \chi\end{matrix}\right\}$$

where the representations under consideration are up to isomorphism. By strong multiplicity one this map is injective, so the question remains what its image is. It is now known (see [KW09]) that this map is a bijection. The proof of this result is outside of the scope of this essay, but we can still say something interesting about it. The first step is to characterise the image in a different way, which relates it to the Artin conjecture. If we assume the L-functions of ρ and sufficiently many of its twists satisfy certain holomorphy conditions then we can apply Weil's converse theorem (theorem 1.1.4) and conclude:

Proposition 3.5.3 (Weil-Langlands)**.** Let $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{C})$ be an irreducible representation with conductor N and $\det(\rho) = \chi$ satisfying:

1. ρ is odd, i.e. $\det(\rho(c)) = -1$ for any choice of complex conjugation $c \in G_{\mathbf{Q}}$.
2. there is an integer $M \geq 1$ such that for every one-dimensional representation $\psi : G_{\mathbf{Q}} \to \mathbf{C}^\times$ of conductor prime to M, the Artin L-function $L(\rho \otimes \psi, s)$ is entire.

then there exists a newform on $\Gamma_0(N)$ of type $(1, \chi)$ such that $L(f, s) = L(\rho, s)$.

Proof. See [Wei71]. □

The representation ρ_f obtained from a newform f satisfies the conditions of proposition 3.5.3 since a twist of a modular form is again a modular form (see theorem 1.1.2). So the above proposition shows that an odd irreducible representation ρ is 'modular' (i.e. of the form ρ_f) if and only if sufficiently many of its twists satisfy the Artin conjecture. By studying the image of the associated projective representation $G_{\mathbf{Q}} \to \mathrm{PGL}_2(\mathbf{C})$ we will explicitly show that a large class of representations is modular using Hecke L-functions (the dihedral representations).

3.6. Estimates of Fourier coefficients

Theorem 3.1.1 shows that the L-function of a normalised newform of weight one is the Artin L-function of a two-dimensional representation. This has consequences on the growth of the coefficients.

Corollary 3.6.1. Let f be a non-zero modular form on $\Gamma_0(N)$ of type $(1, \chi)$ such that $T_p f = a_p f$ for all primes $p \nmid N$. Then

$$|a_p| \leq 2, \quad \forall p \nmid N.$$

Proof. Indeed, by theorem 3.1.1 we see that $a_p = Tr(\rho(\mathrm{Frob}_p))$ is the sum of the eigenvalues of $\rho(\mathrm{Frob}_p)$ which are roots of unity. □

This proves the Ramanujan-Petersson conjecture for weight one: for general weight k it says that the eigenvalues a_p of the Hecke operators T_p for $p \nmid N$ satisfy $|a_p| \leq 2p^{\frac{k-1}{2}}$. In his proof of the Weil conjectures, Deligne proved the Ramanujan-Petersson conjecture for weight $k \geq 2$ (see [Del74]).

We furthermore have the following estimates, which hold for a general modular form of weight one on a congruence subgroup [DS74, §9]:

Corollary 3.6.2. Let $f = \sum_{n \geq 1} a_n e^{2\pi i n z / M}$ be a modular form of weight one on a congruence subgroup of $\mathrm{SL}_2(\mathbf{Z})$.

1. $|a_n| = O(n^\delta)$ for each $\delta > 0$.
2. The set of all $n \in \mathbf{Z}_{\geq 1}$ such that $a_n \neq 0$ has density zero.

The density here considered in the natural density on $\mathbf{Z}_{\geq 1}$: a subset $S \subset \mathbf{Z}_{\geq 1}$ has density c if

$$\lim_{x \to +\infty} \frac{|\{n \in S \mid n \leq x\}|}{x} = c.$$

4. Examples and computations

In this chapter we will give some explicit examples of modular forms of weight one and their associated Galois representations. The website `http://www.lmfdb.org/` and the computer algebra software `SAGE` ([The18]) can be of help for routine calculations.

4.1. The projective image

A representation $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{C})$ has finite image, hence by composing with the projection $\mathrm{GL}_2(\mathbf{C}) \to \mathrm{PGL}_2(\mathbf{C})$ we obtain a projective representation $\tilde{\rho}$ with finite image. Call the image of $\tilde{\rho}$ the projective image of ρ. The following lemma tells us what the projective images can be:

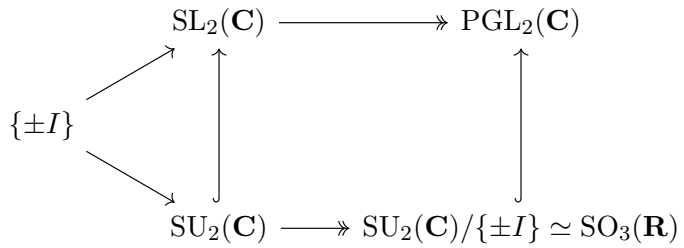
Lemma 4.1.1. Let G be a finite subgroup of $\mathrm{PGL}_2(\mathbf{C})$. Then G is one of the following:

1. G is cyclic
2. G is dihedral
3. G is isomorphic to A_4, S_4 or S_5.

Proof. Let $\pi : \mathrm{SL}_2(\mathbf{C}) \to \mathrm{PSL}_2(\mathbf{C}) = \mathrm{PGL}_2(\mathbf{C})$ be the projection map. The kernel of π is $\{\pm I\}$ and so $\tilde{G} = \pi^{-1}(G)$ is a finite subgroup of $\mathrm{SL}_2(\mathbf{C})$. By taking a hermitian form $\langle , \rangle$ on $\mathbf{C}^2$ and averaging it, i.e. setting

$$\langle v, w \rangle_{\tilde{G}} = \sum_{\sigma \in \tilde{G}} \langle \sigma(v), \sigma(w) \rangle$$

we see that $\tilde{G}$ stabilizes some hermitian form, hence after conjugation we can assume that $\tilde{G}$ is a subgroup of $\mathrm{SU}_2(\mathbf{C})$. But $\mathrm{SU}_2(\mathbf{C})/\{\pm I\}$ is isomorphic to $\mathrm{SO}_3(\mathbf{R})$, which can be seen using quaternions (conjugating pure quaternions by unit quaternions defines a surjective morphism $\mathrm{SU}_2(\mathbf{C}) \to \mathrm{SO}_3(\mathbf{R})$ whose kernel is $\{\pm I\}$). So the image of $\tilde{G}$ in $\mathrm{SO}_3(\mathbf{R})$ is isomorphic to G. But finite subgroups of $\mathrm{SO}_3(\mathbf{R})$ are classified by cones (cyclic), double cones (dihedral) and the platonic solids (A_4, S_4 and S_5). This completes the proof. The diagram below summarizes the situation.



□

Remark 4.1.2. The argument essentially shows that $\mathrm{SO}_3(\mathbf{R})$ is a maximal compact subgroup of $\mathrm{PGL}_2(\mathbf{C})$.

Given a representation $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{C})$, the image of ρ is a central extension of its projective image i.e. there is an exact sequence

$$1 \longrightarrow Z \longrightarrow \mathrm{im}\,\rho \longrightarrow \mathrm{im}\,\tilde{\rho} \longrightarrow 1$$

where Z is the subgroup of scalar matrices in $\mathrm{im}\,\rho$, which is contained in the center of $\mathrm{im}\,\rho$. Since a central extension of a cyclic group is abelian, it follows that the projective image of ρ cannot be cyclic if ρ is irreducible. The other cases do occur (as we will see later) and we will say the type of an irreducible representation ρ is dihedral, tetrahedral (A_4), octahedral (S_4) or icosahedral (A_5) according to the projective image of ρ. The proof of lemma should make the geometric interpretation of the terminology clear.

If $f \in S_1(N, \chi)$ is an eigenform for the Hecke operators T_p with $p \nmid N$, write ρ_f for the irreducible representation $G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{C})$ attached to f by theorem 3.1.1. Then we say f is dihedral, tetrahedral, octahedral or icosahedral according to the type of ρ_f.

4.2. Dihedral representations

We will study the simplest case where the projective image is dihedral, i.e. isomorphic to the dihedral group D_n of order $2n$ for some $n \geq 2$.

Lemma 4.2.1. Let $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{C})$ be a dihedral representation. Then ρ is induced from a one-dimensional $\psi : G_K \to \mathbf{C}^\times$ where K is a quadratic number field.

Proof. Let M be the Galois number field cut out by ρ i.e. such that ρ factors through a faithful representation $\mathrm{Gal}(M/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{C})$. Let $L/\mathbf{Q} \subset M/\mathbf{Q}$ be the subfield of M cut out by the projective representation $\tilde{\rho} : G_{\mathbf{Q}} \to \mathrm{PGL}_2(\mathbf{C})$. Then $\mathrm{Gal}(L/\mathbf{Q}) \simeq D_n$ for some $n \geq 2$ by assumption. Since D_n has a cyclic subgroup C_n of index 2, there exists a number field $K/\mathbf{Q} \subset L/\mathbf{Q}$ of degree 2 such that $\mathrm{Gal}(L/K) \simeq C_n$. So $\rho|_{G_K} : G_K \to \mathrm{GL}_2(\mathbf{C})$ has cyclic projective image hence is reducible, which allows us to decompose it as

$$\rho|_{G_K} = \psi \oplus \psi'$$

for one-dimensional representations ψ, ψ' of G_K. Let $\widehat{\psi}$ be the induction of ψ to $G_{\mathbf{Q}}$. By Frobenius reciprocity we have

$$1 \leq \langle \rho|_{G_K}, \psi \rangle_{G_K} = \langle \rho, \widehat{\psi} \rangle_{G_{\mathbf{Q}}} \leq 1$$

So both equalities hold which implies that $\rho = \widehat{\psi}$. □

Conversely, suppose we start with a quadratic number field $K/\mathbf{Q}$ and a one-dimensional representation $\psi : G_K \to \mathbf{C}^\times$. Let ρ be the induction of ψ to $G_{\mathbf{Q}}$ and let $\tilde{\rho}$ be the associated projective representation. Let σ be the non-identity element of $\mathrm{Gal}(K/\mathbf{Q})$. We define $\psi^\sigma(g)$ as $\psi(\sigma^{-1} g \sigma)$. Recall that Δ_K denotes the discriminant and $\mathfrak{f}(\psi)$ the Artin conductor of ψ. The following proposition gives us more information on ρ [Ser75, §7.2.1]:

Proposition 4.2.2. 1. The representation ρ is irreducible if and only if $\psi \neq \psi^\sigma$. In that case, ρ is dihedral.

2. The conductor of ρ is $|\Delta_K| N_{K/\mathbf{Q}}(\mathfrak{f}(\psi))$.

3. The representation $\det(\rho)$ is odd if and only if one of the following holds:

   a) K is imaginary,

   b) K is real and has signature $(+,-)$ at infinity: if $c, c' \in G_K$ are complex conjugations associated to the two real places of K then $\{\chi(c), \chi(c')\} = \{1, -1\}$.

Proof. A matrix representation of ρ is given by

$$\rho(g) = \begin{pmatrix} \psi(g) & \psi(g\sigma) \\ \psi(\sigma^{-1}) & \psi(\sigma^{-1} g \sigma) \end{pmatrix} \tag{4.1}$$

where we set $\psi(g) = 0$ if $g \notin G_K$. So $\rho|_{G_K} = \psi \oplus \psi^\sigma$ and (1) follows by Frobenius reciprocity. If ρ is irreducible, the projective image of ρ has a cyclic subgroup of index 2 and so we see that ρ has to be dihedral. The second assertion follows from proposition 2.2.4. For 3, suppose first that K is imaginary. If c is a complex conjugation of $\mathbf{Q}$ then $c \notin G_K$ so in (4.1) we might as well take $\sigma = c$ which shows that

$$\rho(c) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

so ρ is indeed odd. If K is real and c is a complex conjugation of $\mathbf{Q}$ then c and $\sigma^{-1} c \sigma$ represent the complex conjugations associated to the real places of K. By (4.1) we see that ρ is odd if and only if $\psi(c) \neq \psi(\sigma^{-1} c \sigma)$. This proves the proposition. □

Recall that we say that a representation $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{C})$ is modular if there exists a $\mathbf{T}_{(N)}$-eigenform $f \in M_1(N, \chi)$ such that $\rho = \rho_f$.

Proposition 4.2.3. Every odd dihedral representation ρ is modular.

Proof. A dihedral representation is certainly irreducible. The conditions of proposition 3.5.3 are satisfied since $L(\rho, s) = L(\psi, s)$ where $\psi : G_K \to \mathrm{GL}_2(\mathbf{C})$ is a one-dimensional character by lemma 4.2.1 and satisfies a functional equation by theorem 1.3.3. □

Can we actually write down what the corresponding modular forms are? The answer is yes, in a very explicit way. Theorems 1.3.4 and 1.3.5 show that if $\psi : G_K \to \mathbf{C}^\times$ is a one-dimensional representation for which $\rho = \mathrm{Ind}_{G_K}^{G_{\mathbf{Q}}} \psi$ is odd and irreducible the function

$$f_\psi = \sum_{\mathfrak{a}} q^{N\mathfrak{a}}$$

is a cusp form of level $|\Delta_K| N(\mathfrak{m})$ of type $(1, \chi)$. So such modular forms correspond exactly to dihedral Galois representations!

If K is imaginary quadratic we can even be more explicit, which was first observed by Hecke in [Hec59]. There is a beautiful connection between the ideal class group of K and binary quadratic forms of discriminant Δ_K which was first studied by Gauss in his 'Disquisitiones Arithmeticae'. Let us briefly recall the relevant concepts. Let

$$Q(x, y) = ax^2 + bxy + cy^2$$

be a positive-definite binary quadratic form. This means that $a, b, c \in \mathbf{Z}$ with discriminant $\Delta_Q = b^2 - 4ac < 0$. We say two such forms Q, Q' are $\mathrm{SL}_2(\mathbf{Z})$-equivalent if a coordinate transformation of the form

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}, \quad \text{with } \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$$

which transforms Q into Q'. Let K be an imaginary quadratic number field with ring of integers $\mathcal{O}_K$, discriminant Δ_K and ideal class group Cl_K. For each ideal $\mathfrak{a}$ of $\mathcal{O}_K$, choose a $\mathbf{Z}$-basis for $\mathfrak{a}$ i.e. write it as

$$\mathfrak{a} = \mathbf{Z}\alpha_1 + \mathbf{Z}\alpha_2$$

where α_1, α_2 are chosen such that $\alpha_1\bar{\alpha}_2 - \alpha_2\bar{\alpha}_1 = N(I)\sqrt{\Delta_K}$ (a sign convention). Associate to $\mathfrak{a}$ the quadratic form

$$Q_{\mathfrak{a}} = \frac{1}{N(I)}(\alpha_1 x + \alpha_2 y)(\bar{\alpha}_1 x + \bar{\alpha}_2 y).$$

We will use the following classical result:

Theorem 4.2.4. Let K be an imaginary quadratic field. The set of binary quadratic forms of discriminant Δ_K up $\mathrm{SL}_2(\mathbf{Z})$-equivalence can be given the structure of an abelian group, denoted $Q(\Delta_K)$. The map

$$\begin{aligned} \mathrm{Cl}_K &\to Q(\Delta_K) \\ [\mathfrak{a}] &\mapsto Q_{\mathfrak{a}} \end{aligned}$$

is a well-defined group isomorphism.

Proof. See [Bue89, Theorem 6.20] or [Fro94, §VII.2]. □

Example 4.2.5. If $K = \mathbf{Q}(\sqrt{-5})$ then $\Delta_K = -20$ and $\mathrm{Cl}_K \simeq \mathbf{Z}/2$ where we have

$$2\mathcal{O}_K = (2, \sqrt{-5} + 1)^2$$

and $(2, \sqrt{-5} + 1)$ is non-principal. We conclude that there are two classes of binary quadratic forms of discriminant -20, represented by the forms:

$$\begin{aligned} Q_0 &= x^2 + 5y^2, \\ Q_1 &= 2x^2 + 2xy + 3y^2. \end{aligned}$$

So ideal classes can be represented by binary quadratic forms. Now it turns out that quadratic forms themselves have associated modular forms, using the theory of theta series. We explain what we need for our purposes, the interested reader might consult [Miy06, §4.9], [Iwa97, chapter 10] or [Sch74].

Let $A \in M_r(\mathbf{Z})$ be a symmetric matrix with integer coefficients. We suppose A is positive-definite of even rank $r = 2k$. We can associate a quadratic form Q_A to A:

$$Q_A(x) = \frac{1}{2}x^t A x,$$

where $x \in \mathbf{R}^r$. If $x = (x_i)$ we can write $Q_A(x)$ as

$$Q_A(x) = \sum_{i=1} \frac{1}{2}a_{ii}x_i^2 + \sum_{i \neq j} a_{ij}x_i x_j$$

where $A = (a_{ij})_{1 \leq i,j \leq r}$. So $Q_A(x)$ has half-integral coefficients on the diagonal and integral coefficients off the diagonal. We say A is even if moreover the a_{ii} are even integers. Let N be a positive integer such that the matrix NA^{-1} is integral and even. Set $D = \det(A)$ and $\Delta = (-1)^k D$, the determinant and discriminant of A respectively.

Theorem 4.2.6. Let $A \in \mathrm{Mat}_r(\mathbf{Z})$ be a symmetric, positive definite, integral even matrix of even rank $r = 2k$. Suppose $N \in \mathbf{Z}_{\geq 1}$ is a positive integer such that NA^{-1} is integral even. Let $\Delta = (-1)^k \det(A)$ and χ_Δ the character given by

$$\chi_\Delta = \left(\frac{\Delta}{\cdot}\right).$$

The theta function

$$\theta_A(z) = \sum_{m \in \mathbf{Z}^r} q^{\frac{1}{2} m^t A m}$$

is an element of $M_k(N, \chi_\Delta)$.

Proof. See [Miy06, Corollary 4.9.5]. □

For quadratic forms in two variables (i.e. binary quadratic forms) we therefore obtain modular forms of weight one.

Let's relate this to dihedral representations. Suppose that $\psi : G_K \to \mathbf{C}^\times$ is a one-dimensional representation with K an imaginary quadratic number field. Suppose furthermore that ψ is unramified, i.e. factors through the Hilbert class field of K. Then ψ defines a morphism $\psi : \mathrm{Cl}_K \to \mathbf{C}^\times$ and by theorem 1.3.4 the function

$$f_\psi = \sum_{\mathfrak{a}} \psi(\mathfrak{a}) q^{N\mathfrak{a}}$$

is an element of $M_1(N, \chi)$ with $\chi = \chi_{\Delta_K}$ the quadratic character of conductor Δ_K defined by the extension $K/\mathbf{Q}$. Write

$$f_\psi = \sum_{\mathcal{A} \in \mathrm{Cl}_K} \psi(\mathcal{A}) \sum_{\mathfrak{a} \in \mathcal{A}} q^{N\mathfrak{a}}.$$

Now fix an $\mathcal{A} \in \mathrm{Cl}_K$ and choose an integral ideal $\mathfrak{b} \in \mathcal{A}$. Then for an integral ideal $\mathfrak{a}$ we have $\mathfrak{a} \in \mathcal{A}$ if and only if $\mathfrak{a} = (k)\mathfrak{b}$ for some $k \in K^\times$ with $k \in \mathfrak{b}^{-1}$. If we choose a $\mathbf{Z}$-basis for $\mathfrak{b}$:

$$\mathfrak{b} = \mathbf{Z}\alpha_1 + \mathbf{Z}\alpha_2,$$

then its inverse is given by

$$\mathfrak{b}^{-1} = \frac{1}{N\mathfrak{b}} \left(\mathbf{Z}\bar{\alpha}_1 + \mathbf{Z}\bar{\alpha}_2\right).$$

If $k = \frac{1}{N\mathfrak{b}} \left(x\bar{\alpha}_1 + y\bar{\alpha}_2\right)$ is in $\mathfrak{b}^{-1}$ then

$$N(x\mathfrak{b}) = Q_{\mathfrak{b}}(x, y),$$

where $Q_{\mathfrak{b}}$ is the quadratic form associated to $\mathfrak{b}$. Note[1] that we have to order the basis $\{\alpha_1, \alpha_2\}$ in such a way that $\bar{\alpha_1}\alpha_2 - \bar{\alpha_2}\alpha_1 = N(I)\sqrt{\Delta_K}$. If we run over all elements of $\mathfrak{b}^{-1}$ we encounter every integral ideal $\mathfrak{a} \sim \mathfrak{b}$ exactly w times, where

$$w = |\mathcal{O}_K^\times| = \begin{cases} 4 & \text{if } K = \mathbf{Q}(i), \\ 6 & \text{if } K = \mathbf{Q}(\sqrt{-3}), \\ 2 & \text{otherwise.} \end{cases}$$

[1] A different ordering would give $Q_{\bar{\mathfrak{b}}}(x, y) = Q_{\mathfrak{b}}(x, -y)$. Since $Q_{\mathfrak{b}}$ and $Q_{\bar{\mathfrak{b}}}$ represent the same integers we will ignore the issue of ordering our basis in most examples since it is not a serious one.

In conclusion, we have

$$\sum_{\mathfrak{a}\in\mathcal{A}} q^{N\mathfrak{a}} = \frac{1}{w}\sum_{x,y\in\mathbf{Z}} q^{Q_{\mathcal{A}}(x,y)} \tag{4.2}$$

$$= w^{-1}\theta_{\mathcal{A}}(z) \tag{4.3}$$

where $\theta_{\mathcal{A}}$ is the theta series associated with the quadratic form $Q_{\mathcal{A}}$ by theorem 4.2.6. So f_ψ is a linear combination of theta series associated to quadratic forms of discriminant Δ_K.

Example 4.2.7. Suppose $\psi : G_K \to \mathbf{C}^\times$ is an unramified one-dimensional representation. Then ψ factors through the Hilbert class field H_K of K and defines a character $\psi : \mathrm{Gal}(H_K/K) \simeq \mathrm{Cl}_K \to \mathbf{C}^\times$. If σ is the nontrivial element of $\mathrm{Gal}(K/\mathbf{Q})$ then the map $g \mapsto \sigma g \sigma^{-1}$ under the isomorphism $\mathrm{Gal}(H_K/K) \simeq \mathrm{Cl}_K$ becomes the map $\mathfrak{a} \mapsto \sigma(\mathfrak{a})$. If we want $\rho = \mathrm{Ind}_{G_K}^{G_{\mathbf{Q}}}(\psi)$ to be irreducible we have to require that $\psi \neq \psi^\sigma$. Since $\mathfrak{a}^\sigma \sim \mathfrak{a}^{-1}$ in Cl_K we see that this condition is equivalent with $\psi^2 \neq 1$. So such $\psi : \mathrm{Cl}_K \to \mathbf{C}^\times$ can exist only if Cl_K is not an elementary 2-group. The smallest value of $|\Delta_K|$ for which this is true is $\Delta_K = -23$ i.e. $K = \mathbf{Q}(\sqrt{-23})$. Set $\delta = \frac{1+\sqrt{-23}}{2}$. We have $\mathrm{Cl}_K \simeq \mathbf{Z}/3$ and $2\mathcal{O}_K = (2,\delta)(2,\delta-1)$ where $(2,\delta)$ is non-principal. If $\mathcal{A}$ is the equivalence class of the ideal $(2,\delta)$ then $\mathcal{A}^2 \sim (2,\delta-1)$ and the associated quadratic forms are

$$Q_1 = x^2 + xy + 6y^2$$
$$Q_{\mathcal{A}} = 2x^2 + xy + 3y^2$$
$$Q_{\mathcal{A}^2} = 2x^2 - xy + 3y^2.$$

Since $Q_{\mathcal{A}}(x,-y) = Q_{\mathcal{A}^2}(x,y)$ these quadratic forms represent the same values, hence $\theta_{\mathcal{A}} = \theta_{\mathcal{A}^2}$. If $\psi : \mathrm{Cl}_K \to \mathbf{C}^\times$ is the character sending $\mathcal{A}$ to $\zeta_3 = e^{2\pi i/3}$ then

$$f_\psi = \frac{1}{2}\left(\theta_1 + \zeta_3\theta_{\mathcal{A}} + \zeta_3^2\theta_{\mathcal{A}^2}\right)$$
$$= \frac{1}{2}\left(\sum_{x,y\in\mathbf{Z}} q^{x^2+xy+3y^2} - \sum_{x,y\in\mathbf{Z}} q^{2x^2+xy+6y^2}\right).$$

which is an element of $S_1(23,\chi_{-23})$. But by [DS05, Proposition 3.2.2], the space $S_1(23,\chi_{-23})$ is spanned by the form

$$\eta(z)\eta(23z) = q\prod_{n\geq 1}(1-q^n)(1-q^{23n}),$$

where $\eta(z)$ is the Dedekind eta function. So this form is equal to f_ψ. Let's compute the associated representation. The Hilbert class field H of K is a degree 3 extension of K: it's the splitting field of the polynomial $X^3 - X - 1$. We have $\mathrm{Gal}(H/\mathbf{Q}) \simeq S_3 \simeq D_3$. If ρ is the induced representation of ψ on $\mathrm{Gal}(H/\mathbf{Q})$ then ρ is the unique two-dimensional irreducible representation of D_3. This representation is faithful, and $Tr(\rho(\mathrm{Frob}_p)) = a_p$ for every prime $p \neq 23$. A simple consequence of this is that for all $p \neq 23$ we have

$$a_p = \begin{cases} 2 & \text{if } \mathrm{Frob}_p \text{ has order 1,} \\ 0 & \text{if } \mathrm{Frob}_p \text{ has order 2,} \\ -1 & \text{if } \mathrm{Frob}_p \text{ has order 3.} \end{cases}$$

so the primes that split completely in H are exactly the primes such that $a_p = 2$. As an application, note that $\eta(z)\eta(23z) \equiv \Delta(z) \mod 23$ so if $\Delta(z) = \sum_{n\geq 1}\tau(n)q^n$ then the splitting behaviour of the polynomial $X^3 - X - 1$ is determined by the values of $\tau(p)$ mod 23. This is an example where a modular form encodes the splitting behaviour of a polynomial and hence provides us with a 'reciprocity law' in the non-abelian case. For more examples of this kind, see [HS17].

Example 4.2.8. Let $K = \mathbf{Q}(\sqrt{-14})$. Then $\mathrm{Cl}_K \simeq \mathbf{Z}/4$ with generator $\mathfrak{p} = (3, \sqrt{-14}+1)$. We have $\mathfrak{p}^2 \sim (2, \sqrt{-11})$ and $\mathfrak{p}^3 \sim (3, -\sqrt{-14}+1)$ so the associated quadratic forms are

$$\begin{aligned} Q_1 &= x^2 + 14y^2 \\ Q_{\mathfrak{p}} &= 3x^2 + 2xy + 5y^2 \\ Q_{\mathfrak{p}^2} &= 2x^2 + 7y^2 \\ Q_{\mathfrak{p}^3} &= 3x^2 - 2xy + 5y^2. \end{aligned}$$

There are two characters $\psi : \mathrm{Cl}_K \to \mathbf{C}^\times$ such that $\psi^2 \neq 1$. Choose ψ such that $\psi(\mathfrak{p}) = i$. We have

$$f_\psi = \frac{1}{2}\left(\sum_{x,y \in \mathbf{Z}} q^{x^2+14y^2} - \sum_{x,y \in \mathbf{Z}} q^{2x^2+7y^2} \right),$$

which is a cusp form of level 56 and character χ_{-56}.

The two above examples deal with characters $\psi : G_K \to \mathbf{C}^\times$ which are everywhere unramified and so that we can give the explicit description using quadratic forms. Can we do the same if ψ is ramified? Suppose ψ factors through some nontrivial modulus $\mathfrak{m}$: it defines a character of the ray class group mod $\mathfrak{m}$, denoted $\mathrm{Cl}(\mathfrak{m})$. Since the class group parametrizes quadratic forms up to $\mathrm{SL}_2(\mathbf{Z})$-equivalence, we might expect ray class groups to parametrize quadratic forms with extra data, since there is a surjective map $\mathrm{Cl}(\mathfrak{m}) \to \mathrm{Cl}_K$. This idea is further pursued in [ISE17], where the authors consider quadratic forms up to $\pm\Gamma_1(N)$-equivalence. For our purposes, we will interpret the ray class groups as quadratic forms with extra congruence conditions. Instead of trying to make this precise, let's give an example to illustrate the idea.

Example 4.2.9. Let $K = \mathbf{Q}(i)$ and $\mathfrak{m} = 6\mathcal{O}_K$. Using class field theory, we compute that

$$\mathrm{Cl}(\mathfrak{m}) \simeq \frac{(\mathbf{Z}/2 \times \mathbf{F}_9^\times)}{\{\pm 1, \pm i\}} \simeq \mathbf{Z}/4,$$

and the prime $\mathfrak{p} = (2+i) \in I(\mathfrak{m})$ is a generator for $\mathrm{Cl}(\mathfrak{m})$. So $\mathrm{Cl}(\mathfrak{m}) = \{1, \mathfrak{p}, \mathfrak{p}^2, \mathfrak{p}^3\}$. The set of integral ideals $\mathfrak{a}$ which are equivalent to (1) in $\mathrm{Cl}(\mathfrak{m})$ correspond to ideals of the form (x) where $x \in \mathcal{O}_K$ with $x \equiv 1 \mod 6\mathcal{O}_K$. The set of integral ideals $\mathfrak{a}$ equivalent to $\mathfrak{p}$ in $\mathrm{Cl}(\mathfrak{m})$ correspond to ideals of the form $(y)\mathfrak{p}$ with $y \equiv 1 \mod 6\mathcal{O}_K$ such that $(y)\mathfrak{p} \subset \mathcal{O}_K$. Equivalently, they correspond to ideals of the form (x) with $x \in \mathcal{O}_K$ and $x \equiv 2+i \mod 6\mathcal{O}_K$. There are analogous congruences for the other ideal classes. If $\psi : \mathrm{Cl}(\mathfrak{m}) \to \mathbf{C}^\times$ is a character that sends $\mathfrak{p}$ to i then

$$\begin{aligned} f_\psi &= \sum_{\mathfrak{a}} \psi(\mathfrak{a}) q^{N\mathfrak{a}} \\ &= \sum_{\mathcal{A} \in \mathrm{Cl}(\mathfrak{m})} \psi(\mathcal{A}) \sum_{\mathfrak{a} \in \mathcal{A}} q^{N\mathfrak{a}} \end{aligned}$$

Now

$$\sum_{\mathfrak{a} \sim (1)} q^{N\mathfrak{a}} = \sum_{\substack{x,y \in \mathbf{Z} \\ (x,y) \equiv (1,0) \mod 6}} q^{x^2+y^2}$$

by the above remarks, and similarly for the other ideal classes. Since the classes $\mathfrak{p}$ and $\mathfrak{p}^3$ in the sum cancel out, we are left with

$$\begin{aligned} f_\psi &= \sum_{\mathfrak{a}\sim(1)} q^{N\mathfrak{a}} - \sum_{\mathfrak{a}\sim\mathfrak{p}^2} q^{N\mathfrak{a}} \\ &= \sum_{\substack{x,y\in\mathbf{Z} \\ (x,y)\equiv(1,0) \\ \text{mod } 6}} q^{x^2+y^2} - \sum_{\substack{x,y\in\mathbf{Z} \\ (x,y)\equiv(3,4) \\ \text{mod } 6}} q^{x^2+y^2} \end{aligned}$$

if we switch the roles of x and y in the last sum, we can write f_ψ more compactly as follows:

$$f_\psi = \sum_{x,y} (-1)^y q^{x^2+y^2},$$

where the sum is taken over all $x, y \in \mathbf{Z}$ such that

$$\begin{cases} x \equiv 1 \mod 3, \\ y \equiv 0 \mod 3, \\ x+y \equiv 1 \mod 2. \end{cases}$$

This is a cusp form of level $|\Delta_K|N(\mathfrak{m}) = 144$ with character χ_{-4}. The ray class field mod $\mathfrak{m}$ is $E = \mathbf{Q}(i, \sqrt[4]{12})$ and $\mathrm{Gal}(E/\mathbf{Q}) \simeq D_4$. The representation associated to f_ψ is the unique two-dimensional irreducible representation of D_4.

Example 4.2.10. Let's compute all dihedral cusp forms of weight one and level 44. This is equivalent with finding all odd irreducible dihedral representations of $G_\mathbf{Q}$ of conductor 44. By proposition 4.2.2, all such representations are induced from a character $\psi : G_K \to \mathbf{C}^\times$ with K a quadratic field such that $|\Delta_K|N_{K/\mathbf{Q}}(\mathfrak{f}(\psi)) = 44$. So the possible values of K are

$$K = \mathbf{Q}(i), \mathbf{Q}(\sqrt{11}) \text{ or } \mathbf{Q}(\sqrt{-11}). \tag{4.4}$$

We examine each case seperately.

- If $K = \mathbf{Q}(i)$, we need a character $\psi : G_K \to \mathbf{C}^\times$ such that $N_{K/\mathbf{Q}}(\mathfrak{f}(\psi)) = 11$. But 11 is inert in K so there is no ideal of norm 11 in K.

- If $K = \mathbf{Q}(\sqrt{11})$ then $\psi : G_K \to \mathbf{C}^\times$ has to be everywhere unramified and $\psi^2 \neq 1$. But the class group of K is trivial, so no such ψ exists.

- The case $K = \mathbf{Q}(\sqrt{-11})$ is slightly more interesting. The class group of K is trivial, with associated quadratic form
$$Q = x^2 + xy + 3y^2.$$
We want a character $\psi : G_K \to \mathbf{C}^\times$ with conductor of norm 4. Since 2 is inert in K, the conductor equals $2\mathcal{O}_K$. We have to compute the ray class group mod $\mathfrak{m} = 2\mathcal{O}_K$. Using class field theory, we see that
$$\mathrm{Cl}(\mathfrak{m}) = \frac{\mathcal{O}_2^\times}{(1+2\mathcal{O}_2)\{\pm 1\}} \simeq \mathbf{F}_4^\times \simeq \mathbf{Z}/3\mathbf{Z}$$
where $\mathcal{O}_2$ denotes the (2)-adic completion of $\mathcal{O}_K$. If we put $\delta = \frac{1+\sqrt{-11}}{2}$ then $\mathfrak{p} = (\delta) \in I(\mathfrak{m})$ is a generator of $\mathrm{Cl}(\mathfrak{m})$. The integral ideals of K which are equivalent to (1) in $\mathrm{Cl}(\mathfrak{m})$ are precisely the ideals of the form $(x + y\delta)$ with $x, y \in \mathbf{Z}$ and $(x, y) \equiv (1, 0) \mod 2$. Similar descriptions hold for the other ideal classes, for example we have
$$\sum_{\mathfrak{a}\sim\mathfrak{p}} q^{N\mathfrak{a}} = \frac{1}{2} \sum_{\substack{x,y\in\mathbf{Z} \\ x \text{ even, } y \text{ odd}}} q^{x^2+xy+3y^2},$$

where we need to divide by 2 since each ideal $\mathfrak{a} \sim \mathfrak{p}$ appears twice in the sum on the right hand side since $-1 \equiv 1 \mod 2\mathcal{O}_K$. Now choose $\psi : \mathrm{Cl}(\mathfrak{m}) \to \mathbf{C}^\times$ such that $\psi(\mathfrak{p}) = \zeta_3 = e^{2\pi i/3}$. Then

$$f_\psi = \frac{1}{2}\left(\sum_{\mathfrak{a}\sim(1)} q^{N\mathfrak{a}} + \zeta_3 \sum_{\mathfrak{a}\sim\mathfrak{p}} q^{N\mathfrak{a}} + \zeta_3^2 \sum_{\mathfrak{a}\sim\mathfrak{p}^2} q^{N\mathfrak{a}}\right)$$

$$= \frac{1}{2}\left(\sum_{\substack{x,y\in\mathbf{Z}\\ x \text{ odd, } y \text{ even}}} q^{x^2+xy+3y^2} + \zeta_3 \sum_{\substack{x,y\in\mathbf{Z}\\ x \text{ even, } y \text{ odd}}} q^{x^2+xy+3y^2} + \zeta_3^2 \sum_{\substack{x,y\in\mathbf{Z}\\ x \text{ odd, } y \text{ odd}}} q^{x^2+xy+3y^2}\right)$$

Alternatively, noting that integral ideals $\mathfrak{a} \sim \mathfrak{p}$ are exactly ideals of the form $(x)\mathfrak{p}$ with $a \in \mathfrak{p}^{-1} = \frac{1}{N\mathfrak{p}}\bar{\mathfrak{p}}$ such that $x \equiv 1 \mod 2\mathcal{O}_K$ and $N\mathfrak{p} \equiv 1 \mod \mathfrak{p}$, we can write f_ψ using the quadratic forms attached to $\mathfrak{p}$ and $\mathfrak{p}^2 \sim \bar{\mathfrak{p}}$:

$$f_\psi = \frac{1}{2}\left(\sum_{\substack{x,y\in\mathbf{Z}\\ x \text{ odd, } y \text{ even}}} q^{x^2+xy+3y^2} + \zeta_3 q^{3x^2+xy+y^2} + \zeta_3^2 q^{3x^2-xy+y^2}\right)$$

$$= \frac{1}{2}\left(\sum_{\substack{x,y\in\mathbf{Z}\\ x \text{ odd, } y \text{ even}}} q^{x^2+xy+3y^2} + q^{3x^2+xy+y^2}\right).$$

the first coefficients of f_ψ are $q - q^3 - q^5 + q^{11} + q^{15} - q^{23} + O(q^{24})$. This is a newform of level 44 and type $(1, \chi_{-11})$. Since $f_\psi = f_{\psi^{-1}}$ it is the only dihedral form of level 44 and using computer calculations (see next section) one can prove that in fact this is the only form of level 44. How does the associated Galois representation look like? We first need to know the ray class field mod $2\mathcal{O}_K$ of K. We can either do this by bruteforce (i.e. by looking at a table on `http://www.lmfdb.org` of number fields of small discriminant) or using the theory of complex multiplication (for an introduction to this beautiful subject, see [Sil94]). Indeed, since K has class number one we know the elliptic curve $\mathbf{C}/\mathcal{O}_K$ has rational j-invariant. Via the approximation $j(z) = q^{-1} + 744 + 196884q + 21493760q^2 + O(q^3)$ we calculate using `SAGE` that

$$j\left(\frac{1+\sqrt{-11}}{2}\right) = -32768.$$

Using the universal elliptic curve or built-in databases in `SAGE` we see that the curve

$$E : y^2 + y = x^3 - x^2 - 7x + 10$$

has compex multiplication by $\mathcal{O}_K$. We obtain the ray class field mod $2\mathcal{O}_K$ by adding all x-coordinates of the 2-torsion points. In these coordinates the multiplication by 2-isogeny looks like

$$[2](x, y) = \left(\frac{x^4 + 14x^2 - 82x + 90}{4x^3 - 4x^2 - 28x + 41}, \cdots\right).$$

so adding all roots of the polynomial $4x^3 - 4x^2 - 28x + 41$ to $\mathbf{Q}$ gives a field extension $L/\mathbf{Q}$ of degree 6 with $\mathrm{Gal}(L/\mathbf{Q}) \simeq S_3 \simeq D_3$. The unique two-dimensional irreducible representation of D_3 is the one associated to f_ψ.

N	$\dim(S_1(\Gamma_1(N)))$
23	1
31	1
39	1
44	1
47	2
52	2
55	1
56	1
57	2
59	1
63	1
68	3
71	3
72	2

Table 4.1.: weight one cusp forms of small level

4.3. Computing all cusp forms of weight one: the exceptional cases

The only examples we have given so far are cusp forms of dihedral type, so the question remains whether we can explicitly construct forms with non-dihedral projective image. In fact, we might wonder if there are explicit algorithms to compute the space of cusp forms of weight one of a given level. For weight at least two, there exist explicit algorithms relying on the Eichler-Shimura isomorphism phrased in the language of modular symbols (see [Ste07]). New ideas were needed to provide algorithms for the weight one case. Buzzard and Lauder recently published a database [BL] which contains all newforms $f \in S_1(N, \chi)$ and their projective image of level $N \leq 1500$. This database was computed using the algorithm described in [Buz14] with the aid of the computer algebra package Magma. It goes roughly as follows: suppose we want to compute the space $S_1(\Gamma_1(N))$. Let $g \in S_k(\Gamma_1(N))$ be a modular form whose q-expansion can be computed to arbitrary precision (e.g. an Eisenstein series). The map

$$\begin{aligned} S_1(\Gamma_1(N)) &\to S_{k+1}(\Gamma_1(N)) \\ f &\mapsto f.g \end{aligned}$$

is injective, and the space on the right hand side can be explicitly computed using modular symbols. It follows that $S_1(\Gamma_1(N))$ is contained in the space of q-expansions $\{g^{-1}h \mid h \in S_{k+1}(\Gamma_1(N))\}$. Doing this for many g and taking intersections gives a good upper bound for the dimension of $S_1(\Gamma_1(N))$. To get a lower bound, we can compute all dihedral forms of level N by computing all odd dihedral representations of $G_{\mathbf{Q}}$ using class field theory (the conductors of the quadratic fields are bounded so this is in theory a finite process). Two possibilities can arise. Either the upper and lower bound agree so every cusp form is dihedral and the dimension is computed. In the other case, there is a possibility of having cusp forms of other then dihedral type. If h is a suspected cusp form of weight one which lies in the intersection of all our test spaces, then it is certainly meromorphic and weight k invariant so it suffices to prove that h^2 is a weight two modular form. If the q-expansions of h^2 and some weight two cusp form agree up to a high enough power of q (e.g. the Sturm bound), then we know for sure that h is holomorphic.

As an example, all dimensions of nonzero $S_1(\Gamma_1(N))$ up to $N \leq 60$ are given in table 4.1. In this range all levels containing a newform do not contain oldforms. We have already encountered some of these forms in example 4.2.7 and 4.2.10. The calculations of [BL] show that all cusp forms of level $N \leq 123$ are dihedral so can be computed in the same fashion as in section 4.2.

order	1	2	3
observed	7.7%	23.8%	68.5%
expected	8.3%	25%	66.6%

Table 4.2.: the A_4 example

Buzzard and Lauder determined the smallest levels for which there exist a cusp form of type A_4, S_4 and A_5. Let us briefly discuss this. We will not try to rigorously prove that these forms are of the desired type but only give heuristic arguments and an indication of how one could do this. The following straightforward lemma will be useful [BL, Lemma 1]:

Lemma 4.3.1. Let $g \in \mathrm{PGL}_2(\mathbf{C})$ be an element of finite order n and $\tilde{g} \in \mathrm{GL}_2(\mathbf{C})$ any lift of g. Then the complex number $Tr(\tilde{g})/\det(\tilde{g})$ is independent of the choice of $\tilde{g}$, and we denote it by $c(g)$. We have $c(g) = 2 + \zeta + \zeta^{-1}$ where ζ is a primitive nth root of unity so if g has order $1, 2, 3, 4$ then $c(g) = 4, 0, 1, 2$ respectively. If g has order 5 then $c(g) = \frac{1\pm\sqrt{5}}{2}$.

4.3.1. The A_4 case

The smallest N such that there exists an A_4 form is $N = 124 = 2^2 \times 31$. There are 4 newforms on $S_1(\Gamma_1(N))$ which are all tetrahedral. If $\zeta = e^{2\pi i/12}$ and $\omega = e^{2\pi/3}$ then one of these newforms is given by the q-expansion:

$$q - \zeta^3 q^2 + (\zeta - \zeta^3)q^3 - q^4 + \omega q^5 - \zeta^2 q^6 + (\zeta^3 - \zeta)q^7 + \zeta^3 q^8 + \zeta q^{10} \\ - \zeta q^{11} + (\zeta^3 - \zeta)q^{12} - \omega q^{13} + \zeta^2 q^{14} + \zeta^3 q^{15} + q^{16} - \zeta^2 q^{17} + (-\zeta^3 + \zeta)q^{19} + O(q^{20}).$$

It's character χ is determined by $\chi(63) = -1$ and $\chi(65) = \omega$. How can we prove that this form is of type A_4? A heuristic way goes as follows. Let $\rho = \rho_f$ be the associated representation and $\tilde{\rho}$ the associated projective representation. By lemma 4.3.1, we can calculate the orders of $\tilde{\rho}(\mathrm{Frob}_p)$ by computing $c(\tilde{\rho}(\mathrm{Frob}_p)) = a_p^2/\chi(p)$. Chebotarev density theorem guarantees that the orders of $\tilde{\rho}(\mathrm{Frob}_p)$ will reflect the orders of the projective image. In this case, only elements of order $1, 2, 3$ seem to appear and the frequency of the orders for primes below 1000 is reported in table 4.3.1. The expected orders are computed using the fact that A_4 has 12 elements of which $1, 3, 8$ are of order $1, 2, 3$ respectively. The similarity between the observed and expected frequencies strongly suggest that f is of type A_4. To prove this rigourously, we can use some tricks [BL] to see it could not be dihedral or of type S_4 and A_5. Or we explicitly compute a Galois representation of type A_4 of conductor 124 which is known to come from some newform [Buz14, Lemma 4]. The number field cut out by the projective representation is the splitting field of $x^4 + 7x^2 - 2x + 14$.

4.3.2. The S_4 case

The smallest level containing an S_4 form is $N = 148 = 2^2 \times 37$. There are two such forms of this level and they are Galois conjugate. The q-expansion of one of them starts as follows:

$$q - iq^3 - q^7 + iq^{11} + (i-1)q^{17} + (-i+1)q^{19} + iq^{21} + (i-1)q^{23} + iq^{25} \\ - iq^{27} + (-i-1)q^{29} + q^{33} - iq^{37} - iq^{41} + q^{47} + (i+1)q^{51} + q^{53} + (-i-1)q^{57} + O(q^{68}).$$

Table 4.3.2 shows the frequencies of the orders of the primes below 1000, against the frequencies of the orders in S_4. Since there are elements of order 4, it is certainly not an A_4 or A_5 form

order	1	2	3	4
observed	0.6%	38.7%	33.9%	26.8%
expected	0.4%	37.5%	33.3%	25%

Table 4.3.: the S_4 example

order	1	2	3	5
observed	0.6%	28.6%	33.9%	36.9%
expected	1.7%	25%	33.3%	40%

Table 4.4.: the A_5 example

(since these groups don't have elements of order 4). By computing all dihedral forms of level 148 using class field theory one can show that it is not dihedral either, so it is indeed of type S_4. The number field cut out by the projective Galois representation is the splitting field of $x^4 - x^3 + 5x^2 - 7x + 12$.

4.3.3. The A_5 case

The smallest level containing an icosahedral form is $N = 633 = 3 \times 211$. If $\zeta = e^{2\pi i/20}$ then the first coefficients of such a form are given by

$$q + (-\zeta^7 + \zeta^5)q^2 - \zeta^8 q^3 + (-\zeta^4 + \zeta^2 - 1)q^4 - \zeta^7 q^5 + (-\zeta^5 + \zeta^3)q^6 + \zeta^4 q^7 - \zeta^3 q^8 - \zeta^6 q^9 + (-\zeta^4 + \zeta^2)q^{10} + (\zeta^7 + \zeta^3 - \zeta)q^{11} + (\zeta^6 - \zeta^4)q^{12} - \zeta^4 q^{13} + O(q^{14}).$$

Table 4.3.3 shows the frequencies of the orders of the primes below 1000, against the frequencies of the orders in A_5. The field cut out by the projective Galois representation attached to this A_5 form is the splitting field of $x^5 - 211x^2 - 1266x - 1899$.

A. Additional proofs

A.1. Von-Staudt Clausen theorem

The main reference for this section is [AIK14]. Recall that the Bernoulli numbers $(B_n)_{n\geq 0}$ are defined by the following power series:

$$\sum_{n\geq 0} \frac{B_n}{n!} t^n = \frac{t}{e^t - 1}.$$

The first terms are $B_0 = 1, B_1 = -1/2$ and $B_2 = 1/6$. This seems to be a rather innocent definition but the Bernoulli numbers are closely connected with many deep arithmetic problems. Let us note that

$$\frac{t}{e^t - 1} + \frac{t}{2}$$

is an even function, hence $B_n = 0$ if $n \geq 3$ is odd. In what follows we give an elementary proof of the Von Staudt-Clausen theorem used in the proof of theorem 3.2.3.

Theorem A.1.1 (Von Staudt-Clausen)**.** For all $n \geq 1$ we have

$$B_n + \sum_{p-1|n} \frac{1}{p} \in \mathbf{Z},$$

where the sum is over all primes p such that $p - 1$ divides n.

Proof. The statement is true for $n = 1$ and since $B_n = 0$ for $n \geq 3$ odd we may assume that $n = 2m$ is even. Let's rewrite the generating function for B_n. We have the following equalities as formal power series:

$$\begin{aligned}
\frac{t}{e^t - 1} &= \frac{\log((e^t - 1) + 1)}{e^t - 1} \\
&= \frac{1}{e^t - 1} \sum_{k\geq 1} (-1)^{k+1} \frac{(e^t - 1)^k}{k} \\
&= \sum_{k\geq 0} (-1)^k \frac{(e^t - 1)^k}{k + 1} \\
&= \sum_{k\geq 0} \frac{(-1)^k}{k + 1} \left(\sum_{n\geq 1} \frac{t^n}{n!} \right)^k
\end{aligned}$$

But we can expand the right hand side by noting that

$$\left(\sum_{n\geq 1} \frac{t^n}{n!} \right)^k = \sum_{n\geq k} \left(\sum_{\substack{a_i \geq 1 \\ a_1 + \cdots + a_k = n}} \binom{n}{a_1, \ldots, a_k} \right) \frac{t^n}{n!}$$

A counting argument shows that

$$\sum_{\substack{a_i \geq 1 \\ a_1 + \cdots + a_k = n}} \binom{n}{a_1, \ldots, a_k} = k!\, S(n,k)$$

where $S(n,k)$ is the number of partitions of $\{1, \ldots, n\}$ in k non-empty subsets. The $S(n,k)$ are called the Stirling numbers of the second kind. In conclusion we obtain

$$B_n = \sum_{k \geq 0} \frac{(-1)^k k!}{k+1} S(n,k) \tag{A.1}$$

So the only primes appearing in the denominator of B_n are those dividing $k+1$ for some $k \in \{1, \ldots, n\}$. In fact one sees that if $k+1$ is composite and $k \neq 4$ then $k+1$ divides $k!$. But the Stirling numbers satisfy the identity (see [AIK14])

$$S(n,k) = \frac{1}{k!} \sum_{j=0}^{k} (-1)^{k+j} \binom{k}{j} j^n \tag{A.2}$$

so

$$S(n,3) = \frac{1}{3!} \left(\binom{3}{1} - 2^n \binom{3}{2} + 3^n \binom{3}{3} \right) \tag{A.3}$$

$$= \frac{1}{3!} \left(3^n - 3.2^n + 3\right) \tag{A.4}$$

so since n is even we get that $3!\, S(n,3) \equiv 3^n - 3.2^n + 3 \equiv 0 \mod 4$.

Conclusion: if k is composite then

$$\frac{(-1)^k k!}{k+1} S(n,k) \in \mathbf{Z}.$$

So the only case left to consider is if $p = k+1$ is prime. We show that

$$(-1)^k k!\, S(n,k) \equiv \begin{cases} -1 \mod p, & \text{if } p-1 \mid n \\ 0 \mod p, & \text{if } p-1 \nmid n \end{cases} \tag{A.5}$$

this is clear for $p = 2$ so assume p to be odd. We use formula A.2 for $k = p-1$ and obtain

$$(-1)^k k!\, S(n,k) = \sum_{j=0}^{p-1} (-1)^j \binom{p-1}{j} j^n$$

Now

$$\binom{p-1}{j} \equiv (-1)^j \mod p$$

and

$$\sum_{j=0}^{p-1} j^n \equiv \begin{cases} -1 \mod p, & \text{if } p-1 \mid n \\ 0 \mod p, & \text{if } p-1 \nmid n \end{cases}$$

hence we obtain the result. □

Remark A.1.2. Once one has developped the theory of p-adic integration there are more natural proofs of the Von Staudt-Clausen congruence.

A.2. Deligne-Serre lifting lemma

In this section we prove the Deligne-Serre lifting lemma. We use the notions of associated and support primes of a ring from commutative algebra. The reader is reminded of their definition and basic properties below the proof of the lifting lemma. The proof is an adaptation of the one given in [Sai09].

Lemma A.2.1 (Deligne-Serre lifting lemma)**.** Let $\mathcal{O}$ be a discrete valuation ring with maximal ideal m, residue field $k = \mathcal{O}/m$ and fraction field K. Let M be a free $\mathcal{O}$-module of finite rank. Let $\mathcal{T} \subset \mathrm{End}_{\mathcal{O}}(M)$ be a commuting family of endomorphisms of M. Suppose $0 \neq f \in M/mM$ satisfies $T(f) = a_T f$ $(a_T \in k)$ for all $T \in \mathcal{T}$.

Then there is a discrete valutation ring $\mathcal{O}'$ with maximal ideal m' where $\mathcal{O} \subset \mathcal{O}'$, $m' \cap \mathcal{O} = m$ and the fraction field of $\mathcal{O}'$ is a finite extension of K such that the system of eigenvalues $\{a_T\}_{T\in\mathcal{T}}$ has a lift to $M' = M \otimes_{\mathcal{O}} \mathcal{O}'$: there exists a nonzero $f' \in M'$ such that

$$T(f') = a'_T f' \; \forall T \in \mathcal{T}$$

with $a'_T \in \mathcal{O}'$ such that $a'_T \equiv a_T \mod m'M'$.

Proof. Let $\mathcal{H}$ be the $\mathcal{O}$-subalgebra of $\mathrm{End}_{\mathcal{O}}(M)$ generated by $\mathcal{T}$. Since M is a free $\mathcal{O}$-module of finite rank, $\mathrm{End}_{\mathcal{O}}(M)$ and hence $\mathcal{H}$ is a free $\mathcal{O}$-module of finite rank as well. Moreover, $\mathcal{H}$ is an integral extension of $\mathcal{O}$, since it is a finitely generated $\mathcal{O}$-module. So $\mathcal{H}_K = \mathcal{H} \otimes_{\mathcal{O}} K$ is a commutative finite K-algebra, hence is an Artinian ring. Since an Artinian ring is a direct product of Artinian local rings [AM69, Theorem 8.7] we can write

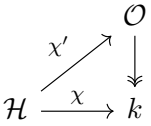
$$\mathcal{H}_K = \prod_{m \in \mathrm{Spec}(\mathcal{H}_K)} (\mathcal{H}_K)_m$$

where the product is over all maximal ideals of $\mathcal{H}_K$ and where $(\mathcal{H}_K)_m$ has residue field $\mathcal{H}_K/m$ which is a field extension of K of finite degree. By lemma A.2.2 and the fact that the tensor product of finite K-algebras distributes over direct products, we see that there exists a field extension K'/K of finite degree such that $\mathcal{H}_{K'} = \mathcal{H} \otimes_{\mathcal{O}} K' = \mathcal{H}_K \otimes_K K'$ is a direct product of Artinian local rings whose residue fields are isomorphic to K'. Let $\widetilde{\mathcal{O}}$ be the integral closure of $\mathcal{O}$ in K'. By the Krull-Akizuki theorem [Neu99, Proposition I.12.8], $\widetilde{\mathcal{O}}$ is a Dedekind domain as well (note that we don't assume the extension K'/K to be seperable). Take a maximal ideal m' of $\widetilde{\mathcal{O}}$. Define $\mathcal{O}'$ to be the localization of $\widetilde{\mathcal{O}}$ at m'. Then $\mathcal{O}'$ is a discrete valuation ring with maximal ideal m' and fraction field K', such that $\mathcal{O} \cap m' = m$. Replacing $\mathcal{O}$ by $\mathcal{O}'$, K by K', k by $\mathcal{O}'/m'$ and M by $M \otimes_{\mathcal{O}} \mathcal{O}'$, we can assume that $\mathcal{H}_K$ is a product of Artinian local rings whose residue fields are isomorphic to K. We will do this in what follows.

Define $\chi : \mathcal{H} \to k$ by sending $T \in \mathcal{H}$ to a_T where $T(f) = a_T f$. Since $\mathcal{O} \subset \mathcal{H}$, the homorphism χ is surjective and so the ideal $\ker(\chi)$ is maximal. Take a minimal prime ideal $\mathfrak{p}$ contained in $\ker(\chi)$ (such a $\mathfrak{p}$ exists by Zorn's lemma). By lemma A.2.3, $\mathfrak{p}$ is contained in the set of zero-divisors of $\mathcal{H}$. Since $\mathcal{O}$ is a domain, this implies that $\mathcal{O} \cap \mathfrak{p} = 0$. The prime ideals of $\mathcal{H}_K$ correspond to the prime ideals of $\mathcal{H}$ which intersect trivially with $\mathcal{O}$, so $\mathfrak{p}$ corresponds to a prime ideal $\mathcal{P}$ in $\mathcal{H}_K$ and

$$K \simeq \mathcal{H}_K/\mathcal{P} \simeq (\mathcal{H}/\mathfrak{p}) \otimes_{\mathcal{O}} K,$$

so the fraction field of $\mathcal{H}/\mathfrak{p}$ is isomorphic to K. Moreover, since $\mathcal{O} \hookrightarrow \mathcal{H}/\mathfrak{p}$ is an integral extension and $\mathcal{O}$ is integrally closed, we see that in fact $\mathcal{H}/\mathfrak{p} \simeq \mathcal{O}$. This provides us with a map $\chi' : \mathcal{H} \to \mathcal{H}/\mathfrak{p} \simeq \mathcal{O}$, defined by the canonical projection. Since the maximal ideal $\ker(\chi)$ gets mapped to a maximal ideal in $\mathcal{H}/\mathfrak{p} \simeq \mathcal{O}$ under χ', we see that in fact $\chi'(\ker(\chi)) \subseteq m$. Since $T - a_T \in \ker(\chi)$ we get $\chi'(T) \equiv a_T \mod m$ and the following diagram commutes:



It remains to show that $\mathcal{P}$ is an associated prime of $M_K = M \otimes_{\mathcal{O}} K$, i.e. is of the form $Ann_{\mathcal{H}_K}(f')$ for some non-zero element $f' \in M_K$. Because then we can suppose f' to be in M, and f' is annihilated by $T - \chi'(T)$ and so $T(f') = \chi'(T)f$ and $\chi'(T) = a_T \mod m$ so this f' satisfies the sought requirements of the lemma.

We first show that $\mathfrak{p} = Ann_{\mathcal{H}/m}(f)$, which is the same as showing that $\mathfrak{p} + m\mathcal{H} = Ann_{\mathcal{H}}(f)$. The inclusion '$\subseteq$' for the latter equality is clear. To show the other inclusion, take a $T \in Ann_{\mathcal{H}}(f)$. We know that $T - a'_T \in \mathfrak{p}$ and $a'_T - a_T \in m\mathcal{H}$ so we have $T \equiv a_T \mod \mathfrak{p} + m\mathcal{H}$. Since $Tf \equiv 0 \mod mM$ by assumption, we see that $a_T f \equiv 0 \mod mM$. But $f \neq 0$ in M/mM so $a_T = 0$ in k, hence $a_T \in m\mathcal{H}$. This shows that $T \in \mathfrak{p} + m\mathcal{H}$ so we have indeed the equality $Ann_{\mathcal{H}/m}(f) = \mathfrak{p}$. This shows that $\mathfrak{p}$ is a support prime of M/mM, hence it is an associated prime by lemma A.2.5. So $Ann_{\mathcal{H}/m}(M/mM) \subseteq \mathfrak{p}$. This implies that $Ann_{\mathcal{H}_K}(M_K) \subseteq \mathcal{P}$. So $\mathcal{P}$ is a support prime of M_K by lemma A.2.5, hence by the same lemma contains an associated prime $\mathfrak{P}$. Since $\mathfrak{p}$ is a minimal prime of $\mathcal{H}$, $\mathcal{P}$ is a minimal prime of $\mathcal{H}_K$. This implies that $\mathcal{P} = \mathfrak{P}$ is an associated prime itself. This concludes the proof of the theorem.

□

Lemma A.2.2. Let F/K be a field extension of finite degree. If a field E contains the normal closure of F/K and is of finite degree over K, the tensor product $F \otimes_K E$ is a direct product of Artinian local rings with residue fields isomorphic to E.

Proof. Let E be such a field, which we will see as a subfield of an algebraic closure $\overline{K}$ of K. We know that $F \otimes_K E$ is a direct product of Artinian local rings whose residue fields are finite extensions of E, hence of K. So the residue fields are precisely the images of E-algebra morphisms $F \otimes_K E \to \overline{K}$. Such morphisms correspond to K-algebra morphisms $F \to \overline{K}$. But such a morphism factors through $F \to E$ since E contains the normal closure of F/K. We conclude that every morphism $F \otimes_K E \to \overline{K}$ factors through $F \otimes_K E \to E$. So the image of such a morphism is a field which is an E-algebra and admits an E-algebra morphism to E; this implies that it must be equal to E. We conclude that $F \otimes_K E$ is a direct product of Artinian local rings with residue fields isomorphic to E. □

Lemma A.2.3. Let $\mathfrak{p}$ be a minimal prime ideal of a (commutative) ring A. Then $\mathfrak{p}$ is contained in the set of zero-divisors.

Proof. Let $s \in \mathfrak{p}$ be nonzero. The ring $A_{\mathfrak{p}}$ has only one prime ideal, so every element of $\mathfrak{p}A_{\mathfrak{p}}$ is nilpotent. So $s/1 \in A_{\mathfrak{p}}$ is nilpotent. So $s^n t = 0$ for some $n \geq 1$ and $t \in A \setminus \mathfrak{p}$. If the natural number n is taken to be minimal such that $s^n t = 0$, then $s^{n-1}t \neq 0$. So s is indeed a zero-divisor. □

Definition A.2.4. Let A be a commutative ring and M an A-module.

1. The annihilator of M is defined as

$$Ann_A(M) = \{x \in A \mid xm = 0 \, \forall m \in M\}.$$

If $m \in M$, we write $Ann_A(m)$ for $Ann_A(\langle m \rangle)$.

2. Say a prime ideal $\mathfrak{p}$ of A is an associated prime of M if $\mathfrak{p}$ is of the form $Ann_A(m)$ for some element $m \in M$. We write $Ass_A(M)$ for the set of associated primes of M.

3. Say a prime ideal $\mathfrak{p}$ of A is a support prime of M if $M_\mathfrak{p} \neq 0$. Equivalently, there exists an $m \in M$ such that $Ann_A(m) \subseteq \mathfrak{p}$. We write $Supp_A(M)$ for the set of support primes of M.

Lemma A.2.5. Let A be a noetherian ring, M an A-module and $\mathfrak{p}$ a prime ideal of A.

1. If M is non-zero, $Ass_A(M)$ is non-empty,

2. If M is finitely generated, then $\mathfrak{p} \in Supp_A(M) \Leftrightarrow Ann_A(M) \subseteq \mathfrak{p}$,

3. $Ass_A(M) \subseteq Supp_A(M)$,

4. If $\mathfrak{p}$ is a support prime, $\mathfrak{p}$ contains an associated prime of M.

Proof. 1. An application of Zorn's lemma.

2. If $\mathfrak{p}$ is a support prime, then $Ann_A(m) \subseteq \mathfrak{p}$ for some $m \in M$ so $Ann_A(M) \subseteq Ann_A(m) \subseteq \mathfrak{p}$. Conversely, suppose M has generators $m_1, \ldots, m_n$. If $\mathfrak{p}$ is not an associated prime, we know $M_\mathfrak{p} = 0$ so $s_i m_i = 0$ for some $s_i \in A \setminus \mathfrak{p}$ for each $1 \leq i \leq n$. But then $s = s_1 \ldots s_n \in A \setminus \mathfrak{p}$ annihilates all the m_i so $s \in Ann_A(M) \setminus \subset \mathfrak{p}$. This implies the claim by taking the contrapositive.

3. If $\mathfrak{p}$ is an associated prime, $Ann_A(m) = \mathfrak{p}$ for some $m \in M$ so indeed $Ann_A(M) \subseteq Ann_A(m) = \mathfrak{p}$.

4. Since $M_\mathfrak{p} \neq 0$, it has an associated prime $\mathfrak{q}$ which is of the form $Ann_A(y/s)$ for some $y \in M$, $s \in A \setminus \mathfrak{p}$ and $y/s \neq 0$. We want to show that $\mathfrak{q}$ is an associated prime. Let $a_1, \ldots, a_n$ be a set of generators for $\mathfrak{q}$. Then $a_i(y/s) = 0$ so $a_i t_i y = 0$ for some $t_i \in A \setminus \mathfrak{p}$. Write $t = t_1 \ldots t_n \in A \setminus \mathfrak{p}$. Since no element of $A \setminus \mathfrak{p}$ annihilates y/s, we see that $ty \neq 0$. So $\mathfrak{q}$ is the annihilator of $ty \in M$.

□

Bibliography

[AIK14] Tsuneo Arakawa, Tomoyoshi Ibukiyama, and Masanobu Kaneko. *Bernoulli numbers and Zeta functions*. Springer monographs in mathematics. Springer, 2014.

[AM69] M.F. Atiyah and I.G. MacDonald. *Introduction to commutative algebra*. Addison-Wesley series in mathematics. Addison-Wesley, Reading, Mass. ; London, 1969.

[BL] Kevin Buzzard and Alan Lauder. A computation of modular forms of weight one and small level. Arxiv Preprint, available at `https://arxiv.org/abs/1605.05346`.

[Bue89] Duncan A Buell. *Binary quadratic forms : classical theory and modern computations*. Springer, New York ; London, 1989.

[Buz14] Kevin Buzzard. Computing weight one modular forms over $\mathbf{C}$ and $\mathbf{F}_p$. In Gebhard Böckle and Gabor Wiese, editors, *Computations With Modular Forms*, volume 6. Springer, 2014.

[CR62] Charles W. Curtis and Irving Reiner. *Representation theory of finite groups and associative algebras*. Pure and applied mathematics : a series of texts and monographs ; vol. 11. Wiley-Interscience New York, 1962.

[Del71] Pierre Deligne. Formes modulaires et représentations l-adiques. *Séminaire Bourbaki*, 1968/1969, 1971.

[Del73] Pierre Deligne. Les constantes des equations fonctionnelles des fonctions l. In P. Deligne and W. Kuijk, editors, *Modular Functions of One Variable II*. Springer, Berlin, Heidelberg, 1973.

[Del74] Pierre Deligne. La conjecture de weil i. *Publ. Math. I.H.E.S.*, 43:273–307, 1974.

[DI94] F. Diamond and J. Im. Modular forms and modular curves. In V. Kumar Murty, editor, *Seminar on Fermat's last theorem*, volume 17, pages 39–133. Canadian Mathematical Society, 1994.

[Dic58] L. E. Dickson. *Linear groups: with an exposition of the Galois field theory*. Dover Publications Inc, New York, 1958.

[DS74] Pierre Deligne and Jean-Pierre Serre. Formes modulaires de poids 1. *Ann. Sci. École Norm. Sup (4)*, 7:507–530, 1974.

[DS05] Fred Diamond and Jerry Shurman. *A first course in modular forms.* Graduate texts in mathematics ; 228. Springer, New York, 2005.

[Fei67] Walter Feit. *Characters of finite groups*. Mathematics lecture notes. W. A. Benjamin, New York, 1967.

[Fro94] A. (Albrecht) Frohlich. *Algebraic number theory*. Cambridge studies in advanced mathematics ; 27. Cambridge University Press, Cambridge, 1st pbk. ed. edition, 1994.

[Hec59] Erich Hecke. *Mathematische Werke*. Vandenhoeck & Ruprecht, Gottingen, 1959.

[HS17] T. Hiramatsu and S. Saito. *An introduction to non-abelian class field theory*, volume 13 of *Series on Number Theory and Its Applications*. World Scientific Publishing Co. Pte. Ltd., 2017.

[ISE17] D. H. Shin I. S. Eum, J. K. Koo. Binary quadratic forms and ray class groups. Online available at `https://arxiv.org/abs/1712.04140`, 2017.

[Iwa97] H. Iwaniec. *Topics in classical automorphic forms*. American Mathematical Society, 1997.

[Jac72] H. Jacquet. *Automorphic Forms on* GL(2). Number 278 in Springer Lecture Notes in Mathematics. Springer-Verlag, Berlin, 1972.

[Kar92] Gregory Karpilovsky. *Group representations*. North-Holland mathematics studies ; 175. North-Holland, Amsterdam ; London, 1992.

[KW09] C. Khare and J.P. Wintenberger. Serre's modularity conjecture (i). *Inventiones Math.*, 178(3):485–504, 2009.

[Lan80] R. Langlands. *Base change for* GL_2. Annals of Math. Series. Princeton University Press, 1980.

[Li74] W. Li. Newforms and functional equations. *Math. Ann.*, 212:285–316, 1974.

[Mar77] J. Martinet. Character theory and artin l-functions. In Proc. Sympos. Univ. Durham, editor, *Algebraic number fields: L-functions and Galois properties*, pages 1–87, 1977.

[Miy06] Toshitsune Miyake. *Modular forms*. Springer monographs in mathematics. Springer-Verlag, 2006. Translated from Japanese by Yoshitaka Maeda.

[Neu99] Jürgen Neukirch. *Algebraic Number Theory*. Springer, 1999.

[Ogg69] A. P. Ogg. On a convolution of l-series. *Inventiones Math.*, 7(4):297–312, 1969.

[Ram00] D. Ramakrishnan. Modularity of the rankin-selberg l-series, and multiplicity one for (2). *Ann. of Math. (2)*, 152(1):45–111, 2000.

[Ran39] R. A. Rankin. Contributions to the theory of ramanujan's function $\tau(n)$ and similar arithmetical functions: Ii. the order of the fourier coefficients of integral modular forms. *Mathematical Proceedings of the Cambridge Philosophical Society*, 35(3):357–372, 1939.

[Sai09] A. Saikia. Ribet's construction of a suitable cusp eigenform. Online available at `https://arxiv.org/abs/0910.1408`, 2009.

[Sch74] Bruno Schoeneberg. *Elliptic modular functions : an introduction, Translated from the German by J. R. Smart and E. A. Schwandt.* Grundlehren der mathematischen Wissenschaften ; 203. Springer, Berlin ; New York, 1974.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones Math.*, 15:259–331, 1972.

[Ser75] Jean-Pierre Serre. Modular forms of weight one and galois representations. In Proc. Sympos. Univ. Durham, editor, *Algebraic number fields: L-functions and Galois properties*, pages 193–268, 1975.

[Ser77] Jean Pierre Serre. *Linear representations of finite groups; translated from the French by Leonard L. Scott.* Graduate texts in mathematics ; 42. Springer-Verlag, New York, 1977.

[Ser95] Jean Pierre Serre. *Local fields.* GTM. Springer-Verlag, New York, 2nd corr. print. edition, 1995.

[Shi94] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions.* Princeton University Press, 1994.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves.* Graduate texts in mathematics ; 151. Springer, London, 1994.

[Ste07] William A. Stein. *Modular forms, a computational approach.* Graduate studies in mathematics ; v. 79. American Mathematical Society, Providence, R.I., 2007.

[The18] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 8.1)*, 2018. `http://www.sagemath.org`.

[Tun81] J. Tunnel. Artin conjecture for representations of octahedral type. *Bull. A.M.S.*, 5:173–175, 1981.

[Wei71] A. Weil. *Dirichlet Series and Automorphic Forms*, volume 189 of *Lecture notes in mathematics.* Springer-Verlag Berlin Heidelberg, 1971.