Ribet's converse to Herbrand

Part III essay
by
Kaloyan Slavov

Emmanuel College
Cambridge University
May 1, 2008

Acknowledgements.

I want to thank my adviser Dr. Tobias Berger first for setting this incredibly interesting and engaging essay topic, and also for helping me clean up some details from the readings, and especially from the proof of the Deligne–Serre lemma.

Chapter 1

Introduction

Classically, Bernoulli numbers B_k defined by

$$\frac{t}{e^t-1}+\frac{t}{2}-1=\sum_{k\geq 2}\frac{B_k}{k!}t^k$$

were studied in connection with the class number of the cyclotomic field $\mathbb{Q}(\mu_p)$, where p is a prime number. Namely, Kummer proved that a prime p divides the class number of $\mathbb{Q}(\mu_p)$ if and only if $p|B_k$ for some even k, with $2\leq k\leq p-3$. In [10], Ribet refines this result and proves that if $p|B_k$, then in fact p divides the order of a certain isotypic component of a quotient of the class group of $\mathbb{Q}(\mu_p)$, considered as a representation of the Galois group $G(\mathbb{Q}(\mu_p)/\mathbb{Q})$ (the converse of this result is due to Herbrand). This, together with a result about abelian unramified extensions of $\mathbb{Q}(\mu_p)$ of type $(p,...,p)$, come as consequences of the main theorem (Theorem 1.3 in [10]) that we discuss in our exposition.

Let p be a prime, let $G_{\mathbb{Q}}=G(\overline{\mathbb{Q}}/\mathbb{Q})$ be the absolute Galois group of $\mathbb{Q}$, and let $\chi:G_{\mathbb{Q}}\to\mathbb{Z}_p^*$ be the standard $\pmod p$−cyclotomic character,

$$\chi:G_{\mathbb{Q}}\longrightarrow\mathbb{Z}_p^* \qquad \text{giving the action on } p-\text{power roots of unity,}$$
$$\sigma\mapsto(b_n)_{n\geq 1}, \qquad \text{where} \qquad \sigma(\mu_{p^n})=\mu_{p^n}^{b_n}.$$

Let $\overline{\chi}:G_{\mathbb{Q}}\to\mathbb{Z}_p^*\to\mathbb{F}_p^*$ be the reduction of χ modulo p.

The main result that we present here, following [10], reads:

Main Theorem 1. *Let k be an even integer, $2\leq k\leq p-3$, and suppose $p|B_k$. Then there exists a (continuous) Galois representation*

$$\overline{\rho}:G_{\mathbb{Q}}\longrightarrow GL(2,\mathbb{F}),$$

where $\mathbb{F}$ is a finite field with char$(\mathbb{F}) = p$, which satisfies the following properties:

i) $\overline{\rho}$ is unramified at all primes $l \neq p$;

ii) With respect to an appropriate basis, $\overline{\rho}$ has the matrix form

$$\begin{pmatrix} 1 & * \\ 0 & \overline{\chi}^{k-1} \end{pmatrix}$$

but is not semisimple.

iii) If D_p denotes a decomposition group for p in $G_{\mathbb{Q}}$, then $\overline{\rho}|_{D_p}$ is diagonalizable.

We construct the representation $\overline{\rho}$ and prove that it satisfies i) and ii); proving that it also satisfies iii) is beyond our scope.

Once the representation $\overline{\rho}$ is constructed, looking at the number field corresponding to its kernel easily yields abelian unramified extensions of $\mathbb{Q}(\mu_p)$ with certain special properties, coming from (i)–(iii), and then using class field theory, one can prove the divisibility by p of the appropriate isotypic component of the quotient of the class group of $\mathbb{Q}(\mu_p)$. This is the subject of Chapter 5. Ribet calls these consequences the main result of his paper; from our point of view, however, the main result from [10] is the construction of the Galois representation $\overline{\rho}$.

Ribet constructs the representation $\overline{\rho}$ from a certain modular form. The remarkable construction that allows one to associate a $\mathfrak{p}-$adic Galois representations to a newform f is explained in Chapter 2. The Eichler–Shimura relation then gives the trace and determinant of the action of a Frobenius element in $G_{\mathbb{Q}}$ under the action of this representation: namely, they are determined by the eigenvalues of the Hecke operators T_l acting on the newform f. It turns out, as discussed in Chapter 3, that an appropriate newform (one which has the desired eigenvalues of the Hecke operators) will yield the desired Galois representation: the key in proving this, is, of course, the Eichler–Shimura relation.

So, we are left in Chapter 4 to construct a newform with certain eigenvalues modulo $\mathfrak{p}$. To give an indication for the proof, first, a certain Eisenstein series $G_{2,\varepsilon}$ has precisely these eigenvalues under the Hecke algebra, so it will suffice to construct a newform which is congruent to this Eisenstein series modulo $\mathfrak{p}$. The key is to construct a $\pmod{\mathfrak{p}}-$eigenform for the Hecke operators with desired eigenvalues, and then use the Delign–Serre lifting lemma and lift it to an actual eigenform. The condition that $p|B_k$ translates to the

one that the leading term c of $G_{2,\varepsilon}$ is divisible by $\mathfrak{p}$. Now, roughly, it suffices to construct a suitable modular form g with constant term 1, because then $G_{2,\varepsilon} - cg$ will give rise to the $\pmod{\mathfrak{p}}-$eigenform that we seek (it has zero constant term and is in fact a cuspform).

Chapter 2

Modular forms and Galois representations

In this chapter, we follow mostly [6] but also [10] on some places, and give the background from the theory of modular forms and associated Galois representations.

2.1 Basic theory of modular forms

Here we set some notation and quickly state facts about modular forms that will be used later. For a more detailed exposition, see [6].

For an integer $k \geq 1$, recall the right action of weight k of the group $\mathrm{GL}_2^+(\mathbb{Q})$ on meromorphic functions on the upper half plane $\mathcal{H}$ given by

$$f([\gamma]_k)(\tau) = (\det \gamma)^{k-1}(c\tau + d)^{-k} f(\gamma\tau), \quad \text{where} \quad \gamma = \begin{pmatrix} a & b \\ c & b \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{Q}).$$

Let $k \geq 1$ be an integer, and let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup of some level N. The space of modular forms of weight k for Γ is denoted $M_k(\Gamma)$, and the space of cusp forms is denoted $S_k(\Gamma)$. For a Dirichlet character $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$, define

$$M_k(N, \varepsilon) = \left\{ f \in M_k(\Gamma_1(N)) \mid f \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} \right]_k = \varepsilon(d) f, \text{ for all } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \right\},$$

and similarly $S_k(N, \varepsilon)$. Also, define $E_k(N, \varepsilon) = M_k(N, \varepsilon)/S_k(N, \varepsilon)$. Any modular form for $\Gamma_1(N)$ can be expanded as a Fourier series $\sum a_n q^n$, where

$q = e^{2\pi i\tau}$ as usual, since $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ belongs to $\Gamma_1(N)$. The case of interest for us is when $N = p$ is a prime number, and $k \in \{1, 2\}$. Namely, when ε is a nontrivial even character, consider

$$G_{2,\varepsilon} = \frac{L(-1,\varepsilon)}{2} + \sum_{n\geq 1}\sum_{d|n} \varepsilon(d) dq^n \tag{2.1}$$

and

$$s_{2,\varepsilon} = \sum_{n\geq 1}\sum_{d|n} \varepsilon\left(\frac{n}{d}\right) dq^n, \tag{2.2}$$

where $L(s,\varepsilon)$ is the usual Dirichlet $L-$function. These two series belong to $M_2(p,\varepsilon)$ and represent a basis of $E_2(p,\varepsilon)$. Moreover, the space of semi–cusp forms

$$\left\{ \sum_{n=0}^{\infty} a_n q^n \in M_2(p,\varepsilon) \mid a_0 = 0 \right\}$$

is generated by $s_{2,\varepsilon}$ and the cusp forms. For a prime $l \neq p$, the Hecke operator T_l acts on these Eisenstein series as

$$T_l G_{2,\varepsilon} = (1 + l\varepsilon(l)) G_{2,\varepsilon} \qquad \text{and} \qquad T_l s_{2,\varepsilon} = (l + \varepsilon(l)) s_{2,\varepsilon}. \tag{2.3}$$

Also, associated to the trivial character $\varepsilon = \mathbf{1}$, we have the Eisenstein series

$$G_{2,\mathbf{1}} = \frac{p-1}{24} + \sum_{n\geq 1}\sum_{\substack{d|n \\ p\nmid d}} dq^n. \tag{2.4}$$

Finally, we know that for an odd character χ, the series

$$G_{1,\varepsilon} = \frac{L(0,\varepsilon)}{2} + \sum_{n\geq 1}\sum_{d|n} \varepsilon(d) q^n \tag{2.5}$$

belongs to $M_1(p,\varepsilon)$.

Focusing on cusp forms, the space $S_k(\Gamma_1(N))$ is an inner product space with respect to the Petersonn inner product. For each divisor $d|N$, there is a map

$$\begin{aligned} i_d : (S_k(\Gamma_1(Nd^{-1})))^2 &\longrightarrow S_k(\Gamma_1(N)) \qquad \text{given by} \\ (f,g) &\longmapsto f + g\left[\begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix}\right]_k \end{aligned}$$

showing that some cusp forms of level N come from lower levels. Define

$$S_k(\Gamma_1(N))^{\text{old}} = \sum_{p|N} \text{im}(i_p) \subset S_k(\Gamma_1(N))$$

and let $S_k(\Gamma_1(N))^{\text{new}}$ be the orthogonal complement of $S_k(\Gamma_1(N))^{\text{old}}$ in $S_k(\Gamma_1(N))$.

Let $\mathbb{T}_{\mathbb{Z}}$ be the $\mathbb{Z}-$subalgebra of $\text{End}_{\mathbb{C}}(S_2(\Gamma_1(N)))$ generated by the Hecke operators T_n and $\langle n \rangle$, for $n \in \mathbb{N}$, and recall that $\mathbb{T}_{\mathbb{Z}}$ is commutative. Recall that a newform is an element $f = \sum_{n=1} a_n q^n \in S_k(\Gamma_1(N))^{\text{new}}$ which is an eigenform for all the Hecke operators T_n, $\langle n \rangle$, $n \in \mathbb{N}$, and such that $a_1 = 1$. As a consequence of the Main Lemma in the theory of Hecke operators, if $f = \sum_{n \geq 1} a_n q^n \in S_k(\Gamma_1(N))^{\text{new}}$ is a nonzero eigenform for the Hecke operators T_n and $\langle n \rangle$, with $(n, N) = 1$, then in fact it is a Hecke eigenform for all the Hecke operators, and $a_1 \neq 0$, so a multiple of f is a newform. If $f = \sum_{n \geq 1} a_n q^n$ is a newform, $T_n f = a_n f$. Any newform belongs to some eigenspace $S_2(N, \varepsilon)$, for a character $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}$.

2.2 Galois representations attached to modular forms

Here we explain the construction which is the heart of Ribet's paper, namely the Galois representation one associates to a newform. The key result is the Eichler–Shimura relation, whose proof requires deep results from algebraic geometry. A proof assuming these results can be found in [6]. Here we give the necessary definitions for the statement.

Recall that $X(\Gamma) = \Gamma \backslash \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$ has a natural structure of a Riemann surface. Denote $X_1(N) = X(\Gamma_1(N))$. The space of holomorphic one–forms on $X_1(N)$ is denoted by $\Omega(X_1(N))$, and the holomorphic map $i : \mathcal{H} \to X_1(N)$ yields an isomorphism

$$\Omega(X_1(N) \simeq S_2(\Gamma_1(N)),\ \omega \mapsto f, \qquad \text{where} \qquad i^*\omega = f(\tau)\ d\tau.$$

For a complex vector space V, set $V^\vee = \text{Hom}_{\mathbb{C}}(V, \mathbb{C})$. The dual of the above isomorphism yields in turn

$$S_2(\Gamma_1(N))^\vee \simeq \Omega(X_1(N))^\vee. \tag{2.6}$$

For a compact Riemann surface X of genus g, let $A_1, ..., A_g$ be the g equatorial loops around each hole, and let $B_1, ..., B_g$ be the g meridial loops.

The $2g$ elements $\int_{A_i}, \int_{B_i}$, $(i = 1, ..., g)$ of the $2g-$dimensional real vector space $\Omega(X)^{\vee}$ form an $\mathbb{R}-$basis, and so

$$H_1(X, \mathbb{Z}) = \mathbb{Z} \int_{A_1} \oplus \cdots \oplus \mathbb{Z} \int_{A_g} \oplus \mathbb{Z} \int_{B_1} \oplus \cdots \oplus \mathbb{Z} \int_{B_g}$$

is a lattice in $\Omega(X)^{\vee}$. We also denote by $H_1(X_1(N), \mathbb{Z})$ the image of $H_1(X_1(N), \mathbb{Z})$ in $S_2(\Gamma_1(N))^{\vee}$ under the isomorphism (2.6).

The Hecke algebra $\mathbb{T}_{\mathbb{Z}}$ acts on $S_2(\Gamma_1(N))^{\vee}$ via composition on the right, and in fact preserves the lattice $H_1(X_1(N), \mathbb{Z})$, so it acts on the quotient

$$J_1(N) = S_2(\Gamma_1(N))^{\vee} / H_1(X_1(N), \mathbb{Z}),$$

which is a $g-$dimensional complex torus. Recall the isomorphism

$$\mathrm{Pic}^0(X_1(N)) \simeq \Omega(X)^{\vee} / H_1(X_1(N), \mathbb{Z}) \simeq J_1(N)$$

from Abel's theorem.

Let $f = \sum_{n \geq 1} a_n q^n \in S_2(\Gamma_1(N))$ be a newform. Consider the eigenvalue map

$$\begin{array}{lll} \mathbb{T}_{\mathbb{Z}} \longrightarrow \mathbb{C} & \text{given by} & \\ T \longmapsto \lambda, & \text{such that} & Tf = \lambda f. \end{array}$$

The image of this map is the ring $\mathcal{O}_f = \mathbb{Z}[\{a_n \mid n \in \mathbb{N}\}]$, and we let I_f denote its kernel. Each a_n is an algebraic integer, and in fact $\mathcal{O}_f$ is a finitely–generated $\mathbb{Z}-$module, so $\mathcal{O}_f$ generates a number field denoted $K = K_f$. Now, $\mathbb{T}_{\mathbb{Z}}/I_f$ and hence its isomorphic image $\mathcal{O}_f$ acts on the abelian variety associated to the newform f,

$$A_f = J_1(N)/I_f J_1(N),$$

which, as an abelian group, is a complex torus of dimension $d = [K : \mathbb{Q}]$.

Let p be a prime. For each $n \geq 1$, denote by $A_f[p^n]$ the p^n-torsion subgroup of A_f. Consider the $p-$adic Tate module

$$\mathrm{Ta}_p(A_f) = \varprojlim A_f[p^n],$$

where the maps are given by multiplication by p. Since $\mathbb{T}_{\mathbb{Z}}/I_f$ and hence $\mathcal{O}_f$ acts on $A_f[p^n]$ and the action is linear hence compatible with the inverse

system, it makes $\mathrm{Ta}_p(A_f)$ an $\mathcal{O}_f-$module. Note that $A_f[p^n] \simeq (\mathbb{Z}/p^n\mathbb{Z})^{2d}$ and so choosing bases of each p^n-torsion subgroup compatibly gives an isomorphism $\mathrm{Ta}_p(A_f) \simeq \mathbb{Z}_p^{2d}$, making $\mathrm{Ta}_p(A_f)$ also a $\mathbb{Z}_p-$module. Therefore, $V_p(A_f) = \mathrm{Ta}_p(A_f) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a module over $K_f \otimes_{\mathbb{Z}} \mathbb{Z}_p = K \otimes_{\mathbb{Q}} \mathbb{Q}_p$. In fact, $V_p(A_f)$ is a free $K \otimes_{\mathbb{Q}} \mathbb{Q}_p-$module of rank 2. If $\mathfrak{p}$ is a prime ideal in the ring of integers of K lying over p, we deduce that the $\mathfrak{p}-$adic Tate module

$$V_{\mathfrak{p}}(A_f) = V_p(A_f) \otimes_{K \otimes \mathbb{Q}_p} K_{\mathfrak{p}}$$

is a 2–dimensional $K_{\mathfrak{p}}-$vector space.

The remarkable fact is that $V_p(A_f)$ and hence $V_{\mathfrak{p}}(A_f)$ also comes equipped with an action of the absolute Galois group $G_{\mathbb{Q}} = G(\overline{\mathbb{Q}}/\mathbb{Q})$. There exists a smooth projective algebraic curve $X_1(N)_{alg}$ defined over $\mathbb{Q}$, and such that the compact Riemann surface associated to the smooth projective algebraic curve $X_1(N)_{alg,\mathbb{C}}$ over $\mathbb{C}$ (regarding the polynomials defining $X_1(N)_{alg}$ as having coefficients in $\mathbb{C}$), is in fact $X_1(N)$. From now on, $X_1(N)$ denotes the smooth projective algebraic curve $X_1(N)_{alg}$ defined over $\mathbb{Q}$, $X_1(N)_{alg,\mathbb{C}}$ denotes the corresponding smooth projective algebraic curve over $\mathbb{C}$, and $X_1(N)_{\mathbb{C}}$ denotes the latter curve when regarded as a compact Riemann surface. Thus, $G_{\mathbb{Q}}$ acts on $X_1(N)$, and induces an action on $\mathrm{Div}^0(X_1(N))$ and on $\mathrm{Pic}^0(X_1(N))$. Moreover, $G_{\mathbb{Q}}$ acts on the p^n-torsion subgroup $\mathrm{Pic}^0(X_1(N))[p^n]$ for all n, and the action is compatible with multiplication by p. Therefore, $G_{\mathbb{Q}}$ acts on the $p-$adic Tate module

$$\mathrm{Ta}_p(\mathrm{Pic}^0(X_1(N))) = \varprojlim \mathrm{Pic}^0(X_1(N))[p^n],$$

where the maps are multiplication by p. Recall that we can identify the field of meromorphic functions on the compact Riemann surface $X_1(N)_{\mathbb{C}}$ with the function field of the smooth complex projective curve $X_1(N)_{alg,\mathbb{C}}$. The group $\mathrm{Pic}^0(X_1(N))$ can be regarded as a subgroup of $\mathrm{Pic}^0(X_1(N)_{\mathbb{C}})$, and so the isomorphism from Abel's theorem, combined with $J_1(N) \to A_f$, yields a map

$$\mathrm{Pic}^0(X_1(N))[p^n] \longrightarrow A_f[p^n].$$

This map is surjective and its kernel is stable under $G_{\mathbb{Q}}$, hence the map induces an action of $G_{\mathbb{Q}}$ on $A_f[p^n]$. These actions for all n assemble to give an action of $G_{\mathbb{Q}}$ on $\mathrm{Ta}_p(A_f)$, which, in fact, commutes with the action on $\mathrm{Ta}_p(A_f)$ of the Hecke algebra $\mathbb{T}_{\mathbb{Z}}/I_f \simeq \mathcal{O}_f$. Thus, $G_{\mathbb{Q}}$ acts on the $K \otimes_{\mathbb{Q}} \mathbb{Q}_p-$module $V_p(A_f) = \mathrm{Ta}_p(A_f) \otimes_{\mathbb{Z}} \mathbb{Q}$, and so acts on the rank-two $K_{\mathfrak{p}}-$module $V_{\mathfrak{p}} =$

$V_{\mathfrak{p}}(A_f)$. This action is continuous with respect to the Krull topology on $G_{\mathbb{Q}}$ and the $\mathfrak{p}-$adic topology on $V_{\mathfrak{p}}(A_f)$ as a finite–dimensional vector space over a $p-$adic field.

In brief, the newform $f = \sum_{n\geq 1} a_n q^n \in S_2(N,\varepsilon)$ gives rise to a $2-$dimensional Galois representation

$$\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}_{K_{\mathfrak{p}}}(V_{\mathfrak{p}}(A_f)).$$

This representation is unramified at every prime $l \nmid pN$. For any prime $l \nmid pN$, consider an absolute Frobenius element $\mathrm{Frob}_l \in G_{\mathbb{Q}}$ (it is well–defined up to conjugation and an inertia subgroup $I_l \subset G_{\mathbb{Q}}$). The Eichler–Shimura relation states that then $\mathrm{tr}\rho(\mathrm{Frob}_l)$ and $\det\rho(\mathrm{Frob}_l)$, which are well-defined elements of $K_{\mathfrak{p}}$, are respectively a_l and $l\varepsilon(l)$. We give more remarks on the Eichler–Shimura relation in the next section.

Proposition 1. *The $2-$dimensional representation $\rho : G_{\mathbb{Q}} \to Aut_{K_{\mathfrak{p}}}(V_{\mathfrak{p}}(A_f))$ is irreducible.*

Proof. (see [10]) Suppose ρ is reducible, so with respect to an appropriate $K_{\mathfrak{p}}-$basis of $V_{\mathfrak{p}}(A_f)$, it has the form

$$\begin{pmatrix} \rho_1 & * \\ 0 & \rho_2 \end{pmatrix}, \tag{2.7}$$

where $\rho_1, \rho_2 : G_{\mathbb{Q}} \to K_{\mathfrak{p}}^*$ are characters. Results of Serre imply that we can write $\rho_i = \chi^{n_i}\varepsilon_i$, where ε_i is a character of finite order, and recall that χ is the standard cyclotomic character

$$\begin{aligned} \chi : G_{\mathbb{Q}} \longrightarrow \mathbb{Z}_p^* \subset K_{\mathfrak{p}}^* \qquad & \text{giving the action on } p-\text{power roots of unity,} \\ \sigma \mapsto (b_n)_{n\geq 1}, \qquad & \text{where} \qquad \sigma(\mu_{p^n}) = \mu_{p^n}^{b_n}. \end{aligned}$$

Note that for a prime $l \neq p$, any element Frob_l acts by $\mu_{p^n} \mapsto \mu_{p^n}^l$ on $\mathbb{Q}(\mu_{p^n})$, $I_l \subset \ker\chi$, and so $\chi(\mathrm{Frob}_l) = l$. Also, since ε_i is a finite–order abelian character, by the Kronecker–Weber theorem, it factors through $Gal(\mathbb{Q}(\mu_{N_i})/\mathbb{Q}) \to K_{\mathfrak{p}}^*$, for some integer N_i. Thus, there are Dirichlet characters $\tilde{\varepsilon_i}$, such that for all sufficiently large l, $\varepsilon_i(\mathrm{Frob}_l) = \tilde{\varepsilon_i}(l)$.

Now, for such primes l, the trace and determinant of $\rho(\mathrm{Frob}_l)$, which we know from the Eichler–Shimura relation, can also be expressed from (2.7), and so

$$\begin{aligned} l^{n_1+n_2}\tilde{\varepsilon_1}(l)\tilde{\varepsilon_2}(l) &= \det(\rho(\mathrm{Frob}_l)) = l\varepsilon(l) \\ \tilde{\varepsilon_1}(l)l^{n_1} + \tilde{\varepsilon_2}(l)l^{n_2} &= \mathrm{tr}(\rho(\mathrm{Frob}_l)) = a_l. \end{aligned}$$

Raising the first equation to an appropriate power and using that the characters ε and $\tilde{\varepsilon_i}$ have finite order, we find that $n_1 + n_2 = 1$, so without loss of generality, $n_1 \geq 1$ and $n_2 \leq 0$. The second equation above can now be regarded in $\mathbb{C}$, and taking absolute values yields

$$|a_l| \geq l - 1,$$

for sufficiently large l. However, this contradicts the bound

$$|a_l| \leq 2\sqrt{l}$$

due to Deligne, and so proves the Proposition. □

2.3 Brief remarks on the Eichler–Shimura relation

We now very briefly give the necessary definitions to state the Eichler–Shimura relation as in [6], and indicate how it implies the version stated earlier. This section provides only a sketch, and is not logically part of the remaining exposition, so can be omitted by the reader. For the proper exposition of the theory, see [6].

If l is a prime with $l \nmid N$, the smooth projective algebraic curve $X_1(N)$ defined over $\mathbb{Q}$ has good reduction at l; let $\tilde{X}_1(N)$ be the reduced smooth projective algebraic curve defined over $\mathbb{F}_l$ (we do not give the precise rather technical definition of good reduction). If $\lambda \subset \overline{\mathbb{Z}}$ is a maximal ideal over l, we have a reduction map $\mathbb{P}^r(\overline{\mathbb{Q}}) \to \mathbb{P}^r(\overline{\mathbb{F}_l})$, which in turn yields a surjection $X_1(N) \to \tilde{X}_1(N)$. The induced reduction map $\mathrm{Div}^0(X_1(N)) \to \mathrm{Div}^0(\tilde{X}_1(N))$ sends principal divisors to principal divisors, and hence induces a map $\mathrm{Pic}^0(X_1(N)) \to \mathrm{Pic}^0(\tilde{X}_1(N))$. The Frobenius automorphism $\sigma_l : x \mapsto x^l$ of $\overline{\mathbb{F}_l}$ gives a morphism $\sigma_l : \tilde{X}_1(N) \to \tilde{X}_1(N)$.

For d prime to N, we have the Hecke operator $\langle d \rangle : X_1(N) \to X_1(N)$ defined by $\Gamma_1(N)\tau \mapsto \Gamma_1(N)\gamma(\tau)$, where $\gamma = \begin{pmatrix} a & b \\ c & \delta \end{pmatrix} \in \Gamma_0(N)$ with $\delta \equiv d \pmod{N}$ (we take $\langle d \rangle = 0$ if d is not prime to N). Recall that a morphism α of algebraic curves induces forward and reverse maps α_* and α^* of Picard groups. There exists a morphism $\langle \tilde{d} \rangle : \tilde{X}_1(N) \to \tilde{X}_1(N)$ such that the

following diagram commutes:

$$\begin{array}{ccc} \mathrm{Pic}^0(X_1(N)) & \xrightarrow{\langle d\rangle_*} & \mathrm{Pic}^0(X_1(N)) \\ \downarrow & & \downarrow \\ \mathrm{Pic}^0(\tilde{X}_1(N)) & \xrightarrow{\langle \tilde{d}\rangle_*} & \mathrm{Pic}^0(\tilde{X}_1(N)) \end{array}$$

Also, for a prime l, the other Hecke operator on the level of divisor groups is given by

$$\begin{aligned} T_l : \mathrm{Div}(X_1(N)_{\mathbb{C}}) &\longrightarrow \mathrm{Div}(X_1(N)_{\mathbb{C}}) \\ \Gamma_1(N)\tau &\longmapsto \sum_j \Gamma_1(N)\beta_j(\tau), \end{aligned}$$

where $\beta_j = \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}$, $0 \leq j < l$, and also including $\beta_\infty = \begin{pmatrix} m & n \\ N & l \end{pmatrix}\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$ when $l \nmid N$; here $\begin{pmatrix} m & n \\ N & l \end{pmatrix}$ is in $\mathrm{SL}_2(\mathbb{Z})$. In fact, after identifying $X_1(N)_{\mathbb{C}}$ with $X_1(N)_{alg,\mathbb{C}}$, the operaator T_l maps $\overline{\mathbb{Q}}-$points to $\overline{\mathbb{Q}}-$points, and so induces

$$\begin{aligned} T_l : \mathrm{Div}(X_1(N)) &\longrightarrow \mathrm{Div}(X_1(N)) \quad \text{and in turn} \\ T_l : \mathrm{Pic}^0(X_1(N)) &\longrightarrow \mathrm{Pic}^0(X_1(N)). \end{aligned}$$

The version of the Eichler–Shimura relation from [6] states that if $l \nmid N$, the following diagram commutes:

$$\begin{array}{ccc} \mathrm{Pic}^0(X_1(N)) & \xrightarrow{T_l} & \mathrm{Pic}^0(X_1(N)) \\ \downarrow & & \downarrow \\ \mathrm{Pic}^0(\tilde{X}_1(N)) & \xrightarrow{\sigma_{l,*}+\langle \tilde{l}\rangle_*\sigma_l^*} & \mathrm{Pic}^0(\tilde{X}_1(N)) \end{array}$$

Let p be a prime. Recall the injection $\mathrm{Pic}^0(X_1(N)) \hookrightarrow \mathrm{Pic}^0(X_1(N)_{\mathbb{C}}) \simeq J_1(N)$. Its restricts to p^n-torsion is an isomorphism

$$i_n : \mathrm{Pic}^0(X_1(N))[p^n] \simeq \mathrm{Pic}^0(X_1(N)_{\mathbb{C}})[p^n] \simeq J_1(N)[p^n] \simeq (\mathbb{Z}/p^n\mathbb{Z})^{2g},$$

where g is the genus of $X_1(N)_{\mathbb{C}}$. Next, if l is a prime with $l \nmid N$, recall that $X_1(N)$ has good reduction at l, and we have a surjection $\mathrm{Pic}^0(X_1(N)) \to \mathrm{Pic}^0(\tilde{X}_1(N))$. In fact, when $l \nmid pN$, this induces an isomorphism

$$\pi_n : \mathrm{Pic}^0(X_1(N))[p^n] \to \mathrm{Pic}^0(\tilde{X}_1(N))[p^n]. \tag{2.8}$$

We already defined the action of $G_{\mathbb{Q}}$ on the $p-$adic Tate module

$$\mathrm{Ta}_p(\mathrm{Pic}^0(X_1(N))) = \varprojlim \mathrm{Pic}^0(X_1(N))[p^n] \simeq \varprojlim (\mathbb{Z}/p^n\mathbb{Z})^{2g} \simeq \mathbb{Z}_p^{2g},$$

which gives a continuous $2g-$dimensional Galois representation

$$\rho_{X_1(N),p} : G_{\mathbb{Q}} \to \mathrm{GL}_{2g}(\mathbb{Z}_p) \subset \mathrm{GL}_{2g}(\mathbb{Q}_p).$$

We have defined the action of the Hecke operators $\langle d \rangle$ and T_l on $\mathrm{Pic}^0(X_1(N))$; thus we obtain an action of the Hecke algebra $\mathbb{T}_{\mathbb{Z}}$ on $\mathrm{Pic}^0(X_1(N))$. This action is linear, restricts compatibly to p^n-torsion, and hence defines an action of $\mathbb{T}_{\mathbb{Z}}$ on the Tate group $\mathrm{Ta}_p(\mathrm{Pic}^0(X_1(N)))$, which is in fact compatible with the Galois action.

Let l be a prime with $l \nmid pN$, and let $\lambda \subset \overline{\mathbb{Z}}$ be a maximal ideal over it. Reductions to $\overline{\mathbb{F}_l}$ will be with respect to λ. Let $I_\lambda \subset D_\lambda \subset G_{\mathbb{Q}}$ be the inertia and decomposition groups of λ. The Galois group $G_{\mathbb{F}_l} = G(\overline{\mathbb{F}_l}/\mathbb{F}_l)$ acts on $\mathrm{Pic}^0(\tilde{X}_1(N))$ and in fact also on p^n-torsion. The reduction map $D_\lambda \to G_{\mathbb{F}_l}$ and the isomorphism π_n from (2.8) give rise to a commutative diagram

$$\begin{array}{ccc} D_\lambda & \longrightarrow & \mathrm{Aut}(\mathrm{Pic}^0(X_1(N))[p^n]) \\ \downarrow & & \downarrow \\ G_{\mathbb{F}_l} & \longrightarrow & \mathrm{Aut}(\mathrm{Pic}^0(\tilde{X}_1(N))[p^n]) \end{array}$$

where the vertical map on the right is an isomorphism. Since I_λ is contained in the kernel of the vertical map on the left, it is also contained in the kernel of the horizontal map on the top, which shows that I_λ acts trivially on $\mathrm{Pic}^0(X_1(N))[p^n]$ for all n, hence also on $\mathrm{Ta}_p(\mathrm{Pic}^0(X_1(N)))$. In other words, $I_\lambda \subset \ker \rho_{X_1(N),p}$, i.e., $\rho_{X_1(N),p}$ is unramified at l.

Next, the diagram from the Eichler–Shimura relation, restricted to p^n-torsion, yields a commutative diagram

$$\begin{array}{ccc} \mathrm{Pic}^0(X_1(N))[p^n] & \xrightarrow{T_l} & \mathrm{Pic}^0(X_1(N))[p^n] \\ \downarrow & & \downarrow \\ \mathrm{Pic}^0(\tilde{X}_1(N))[p^n] & \xrightarrow{\sigma_{l,*}+\langle \tilde{l} \rangle_* \sigma_l^*} & \mathrm{Pic}^0(\tilde{X}_1(N))[p^n] \end{array}$$

Of course, σ_l^* is the map given by $P \mapsto l\sigma_l^{-1}(P)$ and since Frob_λ reduces

to σ_l by definition, we also have a commutative diagram

$$\begin{array}{ccc} \mathrm{Pic}^0(X_1(N))[p^n] & \xrightarrow{\mathrm{Frob}_\lambda + \langle l\rangle_* l\mathrm{Frob}_\lambda^{-1}} & \mathrm{Pic}^0(X_1(N))[p^n] \\ \downarrow & & \downarrow \\ \mathrm{Pic}^0(\tilde{X}_1(N))[p^n] & \xrightarrow{\sigma_{l,*} + \langle \tilde{l}\rangle_* \sigma_l^*} & \mathrm{Pic}^0(\tilde{X}_1(N))[p^n] \end{array}$$

But, the vertical maps in these diagrams are isomorphisms, hence we must have

$$T_l = \mathrm{Frob}_\lambda + \langle l\rangle_* l\mathrm{Frob}_\lambda^{-1}$$

as operators on $\mathrm{Pic}^0(X_1(N))[p^n]$. Compose with Frob_λ on the right to conclude that

$$\mathrm{Frob}_\lambda^2 - T_l\mathrm{Frob}_\lambda + \langle l\rangle_* l = 0$$

as operators on $\mathrm{Ta}_p(\mathrm{Pic}^0(X_1(N)))$. Now, one can deduce the version of the Eichler–Shimura relation stated earlier because on the level of A_f (recall that $f \in S_2(N, \varepsilon)$ is a newform), the Hecke operator T_l acts as a_l, and $\langle l\rangle$ acts as $\varepsilon(l)$. Here we regard $a_l, \varepsilon(l)$ first as elements of $\mathcal{O}_f \simeq \mathbb{T}_{\mathbb{Z}}/I_f$, and then take their images in $K_{\mathfrak{p}}$.

Chapter 3

A suitable newform gives rise to the desired representation $\overline{\rho}$

Here we prove that constructing a suitable newform f suffices for the proof of Theorem 1, as a suitable reduction of the Galois representation attached to it satisfies properties i–iii (we verify (i) and (ii) only). Once we know what may be referred to as the main property of the Galois representation attached to a newform, namely, the Eichler–Shimura relation, the arguments in this chapter involve mainly simple linear algebra, in addition to a result known as the Brauer–Nesbitt theorem. We follow [10].

We postpone the proof of the following theorem till the next chapter.

Theorem 1. *Suppose $2 \leq k \leq p-3$ is an even integer, and $p|B_k$. Then there exists a newform $f = \sum_{n\geq 1} a_n q^n \in S_2(p, \varepsilon)$, for a suitable Dirichlet character ε modulo p, such that*

$$a_l \equiv 1 + l^{k-1} \pmod{\mathfrak{p}}$$

for all primes $l \neq p$, where $\mathfrak{p}|p$ is a fixed prime ideal of the number field $K = K_f$ attached to f. Here the character ε satisfies

$$\varepsilon(l) \equiv l^{k-2} \pmod{\mathfrak{p}},$$

for all primes $l \neq p$.

In this chapter, we deduce Theorem 1 from Theorem 1.

Let

$$\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}_{K_{\mathfrak{p}}}(V_{\mathfrak{p}})$$

be the Galois representation attached to the newform f from Theorem 1, where $V_{\mathfrak{p}} = V_{\mathfrak{p}}(A_f)$.

Let π be a uniformizer in the valuation ring $\mathcal{O}_{\mathfrak{p}}$ of $K_{\mathfrak{p}}$, and let $\mathbb{F} = \mathcal{O}_{\mathfrak{p}}/\pi\mathcal{O}_{\mathfrak{p}}$ be the residue field of $\mathcal{O}_{\mathfrak{p}}$. A lattice in $V_{\mathfrak{p}}$ is a subgroup of the form $\mathcal{O}_{\mathfrak{p}}\alpha \oplus \mathcal{O}_{\mathfrak{p}}\beta$, where α, β is a $K_{\mathfrak{p}}-$basis of $V_{\mathfrak{p}}$. If a lattice $T = \mathcal{O}_{\mathfrak{p}}\alpha \oplus \mathcal{O}_{\mathfrak{p}}\beta$ of $V_{\mathfrak{p}}$ is invariant under $G_{\mathbb{Q}}$, then using α, β as a $K_{\mathfrak{p}}-$basis of $V_{\mathfrak{p}}$, we may regard

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O}_{\mathfrak{p}}).$$

Also, $G_{\mathbb{Q}}$ acts on the quotient $T/\pi T$, which is a $2-$dimensional $\mathbb{F}-$vector space, and with respect to the $\mathbb{F}-$basis $\alpha + \pi T, \beta + \pi T$, the action of $G_{\mathbb{Q}}$ on $T/\pi T$ is described matricially by the reduction

$$\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O}_{\mathfrak{p}}) \to \mathrm{GL}_2(\mathbb{F}).$$

Proposition 2. *Let $T \subset V_{\mathfrak{p}}$ be any lattice in $V_{\mathfrak{p}}$ which is $G_{\mathbb{Q}}-$stable. Then the induced $G_{\mathbb{Q}}-$action on the quotient $T/\pi T$ is reducible, and its semisimplification is described by the two characters $1, \overline{\chi}^{k-1} : G_{\mathbb{Q}} \to \mathbb{F}^*$.*

Proof. Let $l \neq p$ be any prime, and let $\mathrm{Frob}_l \in G_{\mathbb{Q}}$ be an absolute Frobenius element associated to l. Then by the Eichler–Shimura relation,

$$\mathrm{tr}(\overline{\rho}(\mathrm{Frob}_l)) \equiv a_l \equiv 1 + l^{k-1} = 1 + \overline{\chi}(\mathrm{Frob}_l)^{k-1} \pmod{\mathfrak{p}}$$

and similarly

$$\det(\overline{\rho}(\mathrm{Frob}_l)) \equiv l\varepsilon(l) \equiv l^{k-1} = \overline{\chi}(\mathrm{Frob}_l)^{k-1} \pmod{\mathfrak{p}}.$$

Since the set of Frobenius elements in $G_{\mathbb{Q}}$ associated to primes $l \neq p$ is dense in $G_{\mathbb{Q}}$ and the maps $\sigma \mapsto \mathrm{tr}(\overline{\rho}(\sigma))$, $\sigma \mapsto \det(\overline{\rho}(\sigma))$, and $\overline{\chi}$ are continuous, it follows that for all $\sigma \in G_{\mathbb{Q}}$, we have

$$\begin{aligned} \mathrm{tr}\overline{\rho}(\sigma) &= 1 + \overline{\chi}^{k-1}(\sigma) \\ \det \overline{\rho}(\sigma) &= \overline{\chi}^{k-1}(\sigma). \end{aligned}$$

Now the conclusion follows immediately from the Brauer–Nesbitt theorem ([4], combining (30.16) and (69.11)): if M, N are two representations of a finite group, in this case $G_{\mathbb{Q}}/(\ker\overline{\rho} \cap \ker\chi)$ (it is finite as a quotient of $G_{\mathbb{Q}}$ by a closed subgroup) over a finite field $\mathbb{F}$, and each element of the group acts via the same characteristic roots on both M and N (counted with multiplicities), then the representations M and N have the same composition factors. $\square$

To simplify notation, set $\varphi = \overline{\chi}^{k-1}$, a nontrivial character $G_{\mathbb{Q}} \to \mathbb{F}^*$ In order to prove Theorem 1, it remains to find an $\mathcal{O}_{\mathfrak{p}}-$lattice $L \subset V_{\mathfrak{p}}$, which is stable by $G_{\mathbb{Q}}$, and such that the reduction $\overline{\rho}$ of ρ associated to L has the form

$$\begin{pmatrix} 1 & * \\ 0 & \varphi \end{pmatrix}$$

and is not semisimple. We remark that a $G_{\mathbb{Q}}-$invariant lattice in $V_{\mathfrak{p}}$ exists because ρ is continuous and $G_{\mathbb{Q}}$ is compact ([6], p. 382).

Note that if α_1, α_2 is a basis of $V_{\mathfrak{p}}$ with respect to which $\rho(G_{\mathbb{Q}}) \subset \mathrm{GL}_2(\mathcal{O}_{\mathfrak{p}})$ then $\mathcal{O}_{\mathfrak{p}}\alpha_1 \oplus \mathcal{O}_{\mathfrak{p}}\alpha_2$ is of course an invariant lattice. So, if we fix a basis of an invariant lattice T and regard ρ as a homomorphism $G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O}_{\mathfrak{p}})$, then for any $B \in \mathrm{GL}_2(K_{\mathfrak{p}})$ such that $B\rho(G_{\mathbb{Q}})B^{-1} \subset \mathrm{GL}_2(\mathcal{O}_{\mathfrak{p}})$, the composition

$$G_{\mathbb{Q}} \to B\rho(G_{\mathbb{Q}})B^{-1} \subset \mathrm{GL}_2(\mathcal{O}_p) \to \mathrm{GL}_2(\mathbb{F})$$

describes the reduction of ρ with respect to a different lattice. Certainly, this reduction need not be isomorphic to the one associated to the original lattice T (unless $B \in \mathrm{GL}_2(\mathcal{O}_{\mathfrak{p}})$, in which case the two reductions can be identified using the matrix $\overline{B} \in \mathrm{GL}_2(\mathbb{F})$). If T' is any $G_{\mathbb{Q}}-$stable lattice, Proposition 2 implies that the reduction of ρ associated to T', with respect to an appropiate basis, has one of the forms

$$\begin{pmatrix} 1 & * \\ 0 & \varphi \end{pmatrix} \qquad \text{or} \qquad \begin{pmatrix} 1 & 0 \\ * & \varphi \end{pmatrix},$$

as clearly, the form $\begin{pmatrix} \varphi & * \\ 0 & 1 \end{pmatrix}$ corresponds to the second form above by swapping the elements in the basis.

Proposition 3. *Notation as above, there exists an $\mathcal{O}_{\mathfrak{p}}-$lattice $L \subset V_{\mathfrak{p}}$, such that the reduction of ρ associated to L has the form*

$$\begin{pmatrix} 1 & * \\ 0 & \varphi \end{pmatrix}$$

and is not semisimple.

Proof. Let $P = \begin{pmatrix} 1 & 0 \\ 0 & \pi \end{pmatrix} \in \mathrm{GL}_2(K_{\mathfrak{p}})$. We compute

$$P \begin{pmatrix} a & \pi b \\ c & d \end{pmatrix} P^{-1} = \begin{pmatrix} a & b \\ \pi c & d \end{pmatrix}. \tag{3.1}$$

Suppose the reduction of ρ with respect to a basis of an invariant lattice T has the form $\begin{pmatrix} 1 & 0 \\ * & \varphi \end{pmatrix}$. So, there is a matrix $\overline{B} \in \mathrm{GL}_2(\mathbb{F})$, such that $\overline{B}\overline{\rho}(\sigma)\overline{B}^{-1} \in \left\{ \begin{pmatrix} 1 & 0 \\ * & \varphi(\sigma) \end{pmatrix} \right\}$, all $\sigma \in G_{\mathbb{Q}}$. Using that the projection $\mathrm{GL}_2(\mathcal{O}_{\mathfrak{p}}) \to \mathrm{GL}_2(\mathbb{F})$ is onto, we consider a lift $B \in \mathrm{GL}_2(\mathcal{O}_{\mathfrak{p}})$ of $\overline{B}$. Replacing ρ by $B\rho B^{-1}$, we have

$$\rho(\sigma) \in \left\{ \begin{pmatrix} 1+\pi\mathcal{O}_{\mathfrak{p}} & \pi\mathcal{O}_{\mathfrak{p}} \\ * & \varphi(\sigma)+\pi\mathcal{O}_{\mathfrak{p}} \end{pmatrix} \right\}, \text{ all } \sigma \in G_{\mathbb{Q}}$$

(here the meaning of $\varphi(\sigma)+\pi\mathcal{O}_{\mathfrak{p}}$ as $\chi^{k-1}(\sigma)+\pi\mathcal{O}_{\mathfrak{p}} \subset \mathcal{O}_{\mathfrak{p}}$ is clear). Conjugate by P using (3.1) to deduce that with respect to a basis of an invariant lattice, which we now fix till the end of the proof, we have

$$\rho(\sigma) \in \left\{ \begin{pmatrix} 1+\pi\mathcal{O}_{\mathfrak{p}} & * \\ \pi\mathcal{O}_{\mathfrak{p}} & \varphi(\sigma)+\pi\mathcal{O}_{\mathfrak{p}} \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_{\mathfrak{p}}) \right\}, \quad \text{all} \qquad \sigma \in G_{\mathbb{Q}}. \quad (3.2)$$

To prove the Proposition, assume for the sake of contradiction that each reduction of ρ of the form $\begin{pmatrix} 1 & * \\ 0 & \varphi \end{pmatrix}$ is semisimple.

We define inductively a convergent sequence of matrices

$$M_i = \begin{pmatrix} 1 & t_i \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_p),$$

such that

$$M_i\rho(G_{\mathbb{Q}})M_i^{-1} \subset \left\{ \begin{pmatrix} * & \pi^i\mathcal{O}_{\mathfrak{p}} \\ \pi\mathcal{O}_{\mathfrak{p}} & * \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_{\mathfrak{p}}). \right\}$$

This will prove the Proposition, because then $M = \lim M_i$ will be a matrix in $\mathrm{GL}_2(\mathcal{O}_{\mathfrak{p}})$ (since this group is compact) such that

$$M\rho(G_{\mathbb{Q}})M^{-1} \subset \left\{ \begin{pmatrix} * & 0 \\ \pi\mathcal{O}_{\mathfrak{p}} & * \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_{\mathfrak{p}}) \right\},$$

which shows that $M\rho(G_{\mathbb{Q}})M^{-1}$ and hence ρ is a reducible representation, which contradicts Proposition 1.

To begin the induction, set $M_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and use (3.2). Suppose M_i has been chosen. Then (3.1) implies that

$$P^iM_i\rho(G_{\mathbb{Q}})M_i^{-1}P^{-i} \subset \left\{ \begin{pmatrix} * & * \\ \pi^{i+1}\mathcal{O}_{\mathfrak{p}} & * \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_{\mathfrak{p}}) \right\}.$$

Moreover, the reduction of $\sigma \mapsto P^i M_i \rho(\sigma) M_i^{-1} P^{-i}$ has the form $\begin{pmatrix} 1 & * \\ 0 & \varphi \end{pmatrix}$. Indeed, we compute directly that

$$\begin{aligned} P^i M_i \rho(\sigma) M_i^{-1} P^{-i} &= P^i M_i \begin{pmatrix} 1+\pi a & * \\ \pi b & \varphi(\sigma)+\pi c \end{pmatrix} M_i^{-1} P^{-i} \\ &= \begin{pmatrix} 1+\pi a' & * \\ \pi^{i+1} b' & \varphi(\sigma)+\pi c' \end{pmatrix} \end{aligned}$$

and hence the above reduces modulo π to the form $\begin{pmatrix} 1 & * \\ 0 & \varphi \end{pmatrix}$ and is therefore semisimple by assumption.

We now need an elementary Lemma:

Lemma 1. *Let $\rho' : G_{\mathbb{Q}} \to GL_2(\mathbb{F})$ be a representation of the form $\begin{pmatrix} 1 & * \\ 0 & \varphi \end{pmatrix}$ which is semisimple (diagonalizable). Then it is diagonalizable by some unipotent matrix $U = \begin{pmatrix} 1 & \overline{u} \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{F})$.*

Proof. Suppose $B \in \mathrm{GL}_2(\mathbb{F})$ is such that $B\rho'(\sigma)B^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & \varphi(\sigma) \end{pmatrix}$ for all $\sigma \in G_{\mathbb{Q}}$. Write $B_1 = \begin{pmatrix} \det B & 0 \\ 0 & 1 \end{pmatrix}$ and note that $B_1^{-1}B$ has the same property. Therefore, we can assume without loss of generality that $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F})$.

We compute

$$B^{-1} \begin{pmatrix} 1 & 0 \\ 0 & \varphi(\sigma) \end{pmatrix} B = \begin{pmatrix} ad - bc\varphi(\sigma) & bd - bd\varphi(\sigma) \\ -ac + ac\varphi(\sigma) & -bc + ad\varphi(\sigma) \end{pmatrix}. \tag{3.3}$$

Since φ is a nontrivial character[1], $ac = 0$ from the bottom left entry. If $a = 0$, then $-bc = \varphi$ from the bottom right entry, and so $-bc = 1$ from the top left entry, leading to $\varphi = 1$. If $a \neq 0$ but $c = 0$, we deduce that $ad = 1$. Thus, replacing a, d by 1 and b by bd, (3.3) shows that the matrix $U = \begin{pmatrix} 1 & bd \\ 0 & 1 \end{pmatrix}$ will satisfy the required condition. □

[1]This only simplifies slightly the argument in the concrete case of interest; we can prove the lemma without using this fact.

Therefore, by the Lemma, there exists $U = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_\mathfrak{p})$, such that $\overline{U}$ diagonalizes the reduction of $P^i M_i \rho M_i^{-1} P^{-i}$. Since also conjugation by U preserves the lower-left entry of a matrix, we deduce that

$$UP^i M_i \rho(G_\mathbb{Q}) M_i^{-1} P^{-i} U^{-1} \subset \left\{ \begin{pmatrix} * & \pi\mathcal{O}_\mathfrak{p} \\ \pi^{i+1}\mathcal{O}_\mathfrak{p} & * \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_\mathfrak{p}) \right\},$$

and hence

$$(P^{-i}UP^i M_i)\rho(G_\mathbb{Q})(P^{-i}UP^i M_i)^{-1} \subset \left\{ \begin{pmatrix} * & \pi^{i+1}\mathcal{O}_\mathfrak{p} \\ \pi\mathcal{O}_\mathfrak{p} & * \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_\mathfrak{p}) \right\}.$$

This allows us to define

$$M_{i+1} = P^{-i}UP^i M_i = \begin{pmatrix} 1 & t_i + \pi^i u \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & t_{i+1} \\ 0 & 1 \end{pmatrix},$$

and since $t_{i+1} \equiv t_i \pmod{\pi^i}$, the sequence $\{M_i\}$ converges. This completes the proof. □

Chapter 4

Constructing the required newform

We now prove the existence of the newform from Theorem 1, again following [10]. In brief, we have to find an eigenform for all the Hecke operators, with certain eigenvalues modulo a prime ideal $\mathfrak{p}$. We know that the Eisenstein series $G_{2,\varepsilon}$ has precisely these eigenvalues, and so if we find a cusp form congruent to this Eisenstein series, it will be a $\pmod{\mathfrak{p}}-$eigenform for the Hecke operators. Then once we have a $\pmod{\mathfrak{p}}-$eigenform, we can lift it by the key Delign–Serre lifting lemma ([5]) and obtain an eigenform in characteristic 0. So, the construction is reduced to investigating the $\pmod{\mathfrak{p}}-$expansion of certain Eisenstein series, and this is how Bernoulli numbers appear as leading terms of these expansions.

4.1 Constructing a suitable Eisenstain series.

Fix a prime $p > 2$, and consider the cyclotomic field $M = \mathbb{Q}(\mu_{p-1})$. The prime p splits completely in M, and we fix a prime $\mathfrak{p}$ of M dividing p. Since $\mathrm{ord}_{\mathfrak{p}}(p) = 1$, we will interchange congruences modulo p and modulo $\mathfrak{p}$ as appropriate without explicit notice. For simplicity of notation, let A be the ring of $\mathfrak{p}-$integers in M. We have that $\mathcal{O}_M/\mathfrak{p} \simeq \mathbb{Z}/p\mathbb{Z}$, and the $(p-1)-$st roots of unity μ_{p-1} are distinct when reduced to $\mathcal{O}_M/\mathfrak{p}$, hence there exists a

unique character

$$\omega : (\mathbb{Z}/p\mathbb{Z})^* \longrightarrow \mu_{p-1} \qquad \text{such that}$$
$$\omega(d) \equiv d \pmod{\mathfrak{p}}, \qquad \text{all} \qquad d \in \mathbb{Z};$$

this is the inverse of the reduction map $\mu_{p-1} \to (\mathcal{O}_M/\mathfrak{p})^*$. Note that $\omega(-1) = -1$ and ω is a character of order precisely $p-1$.

Fix an even integer k, $2 \leq k \leq p-3$. The goal of this section is to prove the following

Theorem 2. *There exists a modular form $g \in M_2(p, \omega^{k-2})$ all of whose $q-$expansion coefficients are in A, and whose constant coefficient is* 1.

It is natural to try to construct g from the explicit Eisenstein series (2.1), (2.5), and (2.4). Note that ω^{k-1} is an odd character, and ω^{k-2} is a nontrivial even character for $k > 2$, so we can use (2.5) and (2.1) for these two characters respectively. Thus, we begin by studying the $\pmod{\mathfrak{p}}$ $q-$expansions of $G_{2,\omega^{k-2}}$ and $G_{1,\omega^{k-1}}$. Congruences between $q-$expansions are to be understood coefficient-wise.

Lemma 2. *The coefficients of the $q-$expansions of $G_{1,\omega^{k-1}}$ and $G_{2,\omega^{k-2}}$ are in A, and moreover,*

$$G_{2,\omega^{k-2}} \equiv G_{1,\omega^{k-1}} \equiv -\frac{B_k}{2k} + \sum_{n\geq 1}\sum_{d|n} d^{k-1}q^n \pmod{\mathfrak{p}}.$$

Proof. The statement for $G_{2,\mathbf{1}}$ is automatic because $B_2 = \frac{1}{6}$. For the other cases, recall that $\omega^{k-2}(d)d \equiv \omega^{k-1}(d) \equiv d^{k-1} \pmod{\mathfrak{p}}$, so by the expansions (2.1) and (2.5), we only need to examine the constant terms. By a standard fact about Dirichlet $L-$functions (see [6], p. 137), for any nontrivial character ε modulo p, we have

$$L(0,\varepsilon) = -\frac{1}{p}\sum_{n=1}^{p-1}\varepsilon(n)\left(n - \frac{p}{2}\right) \tag{4.1}$$

$$L(-1,\varepsilon) = -\frac{1}{2p}\sum_{n=1}^{p-1}\varepsilon(n)\left(n^2 - pn + \frac{p^2}{6}\right). \tag{4.2}$$

We now need some congruences modulo $\mathfrak{p}^2$. If $\omega(n) = \zeta$, so $n = \zeta + \pi\alpha$, with $\pi \in \mathfrak{p}$, write $\zeta - n^p = \zeta - (\zeta + \pi\alpha)^p \equiv \zeta - \zeta^p - p\zeta^{p-1}\pi\alpha \equiv 0 \pmod{\mathfrak{p}^2}$ because $\zeta^p = \zeta$. Thus, $\omega(n) \equiv n^p \pmod{\mathfrak{p}^2}$. Using that the sum over the group $(\mathbb{Z}/p\mathbb{Z})^*$ of the nontrivial character ω^{k-1} is 0, we have

$$\begin{aligned} pL(0, \omega^{k-1}) &= -\sum_{n=1}^{p-1} \omega^{k-1}(n) \left(n - \frac{p}{2}\right) \\ &\equiv -\sum_{n=1}^{p-1} n^{1+p(k-1)} \pmod{\mathfrak{p}^2}. \end{aligned}$$

Similarly,

$$pL(-1, \omega^{k-2}) \equiv -\frac{1}{2} \sum_{n=1}^{p-1} n^{2+p(k-2)} \pmod{\mathfrak{p}^2},$$

where now we used that

$$\sum_{n=1}^{p-1} n^{1+p(k-2)} \equiv \sum_{n=1}^{p-1} n^{k-1} \equiv 0 \pmod{p},$$

(as is well–known, this follows easily since $0 < k-1 < p-1$ and $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic).

Recall the congruence

$$pB_t \equiv \sum_{n=1}^{p-1} n^t \pmod{p^2},$$

valid for any positive even integer t. We are now able to compare the special $L-$values with Bernoulli numbers, namely

$$\begin{aligned} L(0, \omega^{k-1}) &\equiv -B_{1+p(k-1)} \pmod{p} \\ L(-1, \omega^{k-2}) &\equiv -\frac{1}{2} B_{2+p(k-2)} \pmod{p}. \end{aligned}$$

Therefore, we have reduced the proof to the following congruence between Bernoulli numbers:

$$\begin{aligned} B_{1+p(k-1)} &\equiv \frac{B_k}{k} \pmod{p} \\ \frac{B_{2+p(k-2)}}{2} &\equiv \frac{B_k}{k} \pmod{p}. \end{aligned}$$

Recall a special case of the famous Kummer congruence (e.g., [9], p. 44): if $(p-1) \nmid k$, and $k \equiv k' \pmod{(p-1)}$, then $(1-p^{k-1})\frac{B_k}{k} \equiv (1-p^{k'-1})\frac{B_{k'}}{k'} \pmod{p}$. Applying this with $k' = 1+p(k-1)$ and $k' = 2+p(k-2)$ finishes the proof. $\square$

Now that we have a sufficient supply of modular forms with $\mathfrak{p}-$integral $q-$expansions, we want also to ensure that enough of them have constant term a $\mathfrak{p}-$unit.

Proposition 4. *Let*

$$t = \#\left\{n \quad even, \quad 2 \leq n \leq p-3 \mid p|B_n\right\}.$$

Then $t < \frac{p-1}{4}$.

Proof. Let h_p and h_p^- be the class numbers of $\mathbb{Q}(\mu_p)$ and $\mathbb{Q}(\mu_p + \mu_p^{-1})$ respectively, and let $h_p^* = \frac{h_p}{h_p^-}$; it is called the first factor of the class number of $\mathbb{Q}(\mu_p)$.

We first prove that $p^t | h_p^*$. A result by Greenberg ([7], formula on p. 250 applied to the case $k = \mathbb{Q}$ and using that the number of roots of unity in $\mathbb{Q}(\mu_p)$ is $2p$ and that ω generates the group of characters on $(\mathbb{Z}/p\mathbb{Z})^*$) implies that

$$h_p^* = 2^a p \prod_{\substack{k=2 \\ k \text{ even}}}^{p-1} L(0, \omega^{k-1}),$$

for some integer a. By (4.1) for $\varepsilon = \omega^{p-2}$, we have that $pL(0, \omega^{p-2})$ is $\mathfrak{p}-$integral in $\mathbb{Q}(\mu_{p-1})$. Now consider the remaining product

$$\prod_{\substack{k=2 \\ k \text{ even}}}^{p-2} L(0, \omega^{k-1}).$$

If $p|B_k$ for k even, $2 \leq k \leq p-3$, then by Lemma 2, $\mathfrak{p}$ divides the constant term of $G_{1,\omega^{k-1}}$, or in other words, $\mathfrak{p}|L(0, \omega^{k-1})$. Therefore, $\mathfrak{p}^t | h_p^*$ as stated.

Next, we estimate h_p^* based on an explicit formula proved in [3]. Namely, for r prime to p, let r' denote an integer which gives the inverse of r modulo p, and let $R(r) \in \{0, 1, ..., p-1\}$ be the residue of r modulo p. Consider the $\frac{p-1}{2} \times \frac{p-1}{2}$ determinant

$$D_p = \det(R(rs'))_{r,s'=1,...,\frac{p-1}{2}}.$$

Then $h_p^* = \pm \frac{D_p}{p^{\frac{p-3}{2}}}$. Next, an easy estimation

$$|D_p| \leq 2^{-\frac{p-1}{4}} p^{\frac{3(p-1)}{4}}$$

from [2] implies

$$h_p^* < p^{\frac{p-1}{4}}$$

(using that $h_p^* = 1$ for $p \leq 19$ and $2^{-\frac{p-1}{4}} < p^{-1}$ for $p \geq 19$).

Therefore,

$$p^t \leq h_p^* < p^{\frac{p-1}{4}},$$

hence the statement of the Proposition. □

We are now ready to prove Theorem 2.

Proof. Consider first the modular form $G_{2,\omega^{k-2}}$. If its constant term is not a $\mathfrak{p}-$unit, then $p|B_k$. Assume this is the case. For each pair of even integers m, n, such that $2 \leq m, n \leq p-3$, and $m+n \equiv k \pmod{p-1}$, we have that $G_{1,\omega^{m-1}} G_{1,\omega^{n-1}}$ is a modular form of weght 2, type $\omega^{m-1}\omega^{n-1} = \omega^{k-2}$, and has a $\mathfrak{p}-$integral $q-$expansion. Its constant term is a $\mathfrak{p}-$unit provided that $p \nmid B_m$ and $p \nmid B_n$. However, if we assume that for each pair (m, n) as above, at least one of the Bernoulli numbers B_m, B_n is divisible by p, an elementary counting argument (using that also $p|B_k$) shows $t \geq \frac{p-1}{4}$, which contradicts Proposition 4. □

4.2 Obtaining a cuspform

Now that we have the Eisenstein series g from Theorem 2, we no longer need to consider the auxiliary modular forms of weight 1. We now make the assumption that $p|B_k$. Since $B_2 = \frac{1}{6}$, we can therefore assume that the even integer k satisfies $4 \leq k \leq p-3$. So, $\varepsilon = \omega^{k-2} : (\mathbb{Z}/p\mathbb{Z})^* \to \mu_{p-1}$ is a nontrivial even character.

Using the main result from the previous section, we first construct a semi-cusp form which is a $\pmod{\mathfrak{p}}-$eigenform for the Hecke operators T_n, $(n, p) = 1$. Then, the key step is to use the Deligne–Serre lemma to obtain a semicusp form which is an eigenform for the Hecke operators with desired eigenvalues modulo $\mathfrak{p}$, and finally we easily note that this semicusp form is in fact a cusp form.

Proposition 5. *There exists a semi–cusp form $f \in M_2(p,\varepsilon)$ whose $q-$expansion coefficients are in A, and which is a $\pmod{\mathfrak{p}}-$eigenform for all the Hecke operators $T_n, (n,p)=1$, with eigenvalue of T_l equal to $1+\varepsilon(l)l \pmod{\mathfrak{p}}$.*

Proof. Let g be the modular form from Theorem 2. Let c be the constant coefficient of $G_{2,\varepsilon}$; then $c \equiv -\frac{B_k}{2k} \equiv 0 \pmod{\mathfrak{p}}$. So,

$$f = G_{2,\varepsilon} - cg \in M_2(p,\varepsilon)$$

is a semicusp form with $q-$expansion coefficients in A, and

$$f \equiv G_{2,\varepsilon} \pmod{\mathfrak{p}}.$$

Recall([6], p. 179) that if $\sum_{m=0}^{\infty} a_m q^m \in M_2(p,\varepsilon)$ is any modular form, then its image under the Hecke operator T_n is given by $\sum_{m=0}^{\infty} b_m q^m$, with

$$b_m = \sum_{d|(m,n)} \varepsilon(d) d^{k-1} a_{\frac{mn}{d^2}}.$$

In particular, applying Hecke operators to modular forms with $q-$expansion coefficients in A preserves congruences modulo $\mathfrak{p}$.

Therefore, for a prime $l \neq p$, recalling the eigenvalue of T_l acting on $G_{2,\varepsilon}$ from (2.3), we obtain

$$T_l(f) \equiv T_l G_{2,\varepsilon} = (1+\varepsilon(l)l)G_{2,\varepsilon} \equiv (1+\varepsilon(l)l)f \pmod{\mathfrak{p}}.$$

□

Proposition 6. *There exists a nonzero cuspform $f' \in M_2(p,\varepsilon)$, which is an eigenform for all the Hecke operators $T_n, (p,n)=1$, and a prime ideal $\mathfrak{q}|\mathfrak{p}$ in the field generated over $\mathbb{Q}(\mu_{p-1})$ by the eigenvalues $\lambda(n)$ of T_n acting on f' for $(n,p)=1$, such that for any prime $l \neq p$, the eigenvalue $\lambda(l)$ satisfies the congruence*

$$\lambda(l) \equiv 1+\varepsilon(l)l \pmod{\mathfrak{q}}.$$

Proof. The key step here is the Deligne–Serre lemma (note that $A \subset \mathbb{Q}_{\mu_{p-1}}$ is a discrete valuation ring, and consider the space of semicusp forms, on which the subalgebra of $\mathbb{T}_{\mathbb{Z}}$ generated by $\langle d \rangle$ and $T_n, p \nmid n$ acts; see next section for the precise formulation of the Deligne–Serre lemma), which shows that the previous Proposition yields a semi cusp form $f' \in M_2(p,\varepsilon)$ satisfying all the requirements. We only have to prove that such a semi cusp form must

in fact be a cusp form. We recall the semi cusp form $s_{2,\varepsilon}$ from (2.2) and the fact that we can write the semi cusp form f' as

$$f' = g + as_{2,\varepsilon}$$

for some $a \in \mathbb{C}$, where g is a cusp form. For a prime $l \neq p$, apply the Hecke operator T_l to both sides above, and recall from (2.3) the action of T_l on $s_{2,\varepsilon}$:

$$T_l g + a(\varepsilon(l) + l)s_{2,\varepsilon} = T_l f' = \lambda(l)f' = \lambda(l)g + a\lambda(l)s_{2,\varepsilon}.$$

Thus,

$$T_l g - \lambda(l)g = a(\lambda(l) - \varepsilon(l) - l)s_{2,\varepsilon}.$$

The left–hand–side is a cusp form, hence so must be the right–hand–side. Either $s_{2,\varepsilon}$ is a cusp form, in which case so is $f' = g + as_{2,\varepsilon}$, or $a = 0$, in which case $f' = g$ in a cuspform to begin with, or, if we assume that these two fail, then

$$\lambda(l) = \varepsilon(l) + l$$

for all primes $l \neq p$. This is not possible, however. Indeed, ε is nontrivial, so there is some $r \in (\mathbb{Z}/p\mathbb{Z})^*$ with $\varepsilon(r) \neq 1$. Choose a prime $l \equiv r \pmod{p}$. Then $\varepsilon(l) + l = \lambda(l) \equiv 1 + l\varepsilon(l) \pmod{\mathfrak{q}}$, hence $\varepsilon(l)(1 - l) \equiv 1 - l \pmod{\mathfrak{p}}$ and because $l \neq 1 \pmod{p}$, we deduce $\varepsilon(l) \equiv 1 \pmod{\mathfrak{p}}$ and hence $\varepsilon(l) = 1$, which contradicts the choice of l. We conclude that f' is a cuspform. □

Theorem 1 now follows immediately from the discussion of section 2.1: since $S_2(\mathrm{SL}_2(\mathbb{Z}))$ is trivial, so is the space of oldforms $\mathrm{im}(i_p) = S_2(p, \varepsilon)^{\mathrm{old}}$. Therefore, by the theorem quoted at the end of section 2.1, a suitable multiple of f' is the desired newform $f = \sum_{n \geq 1} a_n q^n \in M_2(p, \varepsilon)$, with

$$a_l = \lambda(l) \equiv 1 + \varepsilon(l)l \equiv 1 + l^{k-1} \pmod{\mathfrak{p}},$$

for all primes $l \neq p$. Here we abuse notation and denote by $\mathfrak{p}$ the prime ideal $\mathfrak{q}$ of the ring of integers of the number field $K = \mathbb{Q}(\mu_{p-1}, \lambda(n) : (n, p) = 1) \supset \mathbb{Q}(\mu_{p-1})$ lying above the original prime ideal $\mathfrak{p}$ in the ring of integers of $\mathbb{Q}(\mu_{p-1})$.

4.3 The Deligne–Serre lemma

We devote this section to a detailed proof of the key commutative algebra result that allowed us to lift a $\pmod{\mathfrak{p}}$−eigenform to an actual eigenform.

Here we follow [5]. This section is different in flavor from the rest of our exposition as it is purely a piece of commutative algebra. The background from commutative algebra that is used in the proof can be found in [1].

Proposition 7. *Let $\mathcal{O}$ be a discrete valuation ring with maximal ideal m, field of fractions K, and residue field $k = \mathcal{O}/m$. Assume that K is perfect*[1]*. Let M be a finitely generated and free $\mathcal{O}-$module, and $\mathcal{H} \subset End_{\mathcal{O}}(M)$ a commutative $\mathcal{O}-$subalgebra of $\mathcal{O}-$endomorphisms of M. Consider M/mM as a $k-$vector space on which $\mathcal{H}$ acts, and suppose $f \neq 0, f \in M/mM$ is an eigenvector for all operators in $\mathcal{H}$, with eigenvalue of $T \in \mathcal{H}$ equal to $a_T \in k$. Then there exists a finite extension K'/K, such that if $\mathcal{O}'$ is the integral closure of $\mathcal{O}$ in K' (again a discrete valuation ring) and $m' \subset \mathcal{O}'$ is the maximal ideal of $\mathcal{O}'$, then there exists nonzero $f' \in \mathcal{O}' \otimes_{\mathcal{O}} M$ (which is regarded as a finitely generated and free $\mathcal{O}'-$module), which is an eigenvector of all $T \in \mathcal{H}$ (under the natural induced $\mathcal{O}'-$module action), with eigenvalues $a'_T \equiv a_T \pmod{m'}$, for all $T \in \mathcal{H}$.*

Proof. As an $\mathcal{O}-$module, $\mathrm{End}_{\mathcal{O}}(M)$ is isomorphic to $\mathrm{End}_{\mathcal{O}}(\mathcal{O}^r) \simeq \mathcal{O}^{r^2}$ for some r, and is therefore finitely–generated and free. Since $\mathcal{O}$ is a principal ideal domain, the submodule $\mathcal{H}$ is also finitely–generated and free as an $\mathcal{O}-$module. Consider $B = K \otimes_{\mathcal{O}} \mathcal{H}$ as a finite–dimensional $K-$vector space. The quotient of $K \otimes_{\mathcal{O}} \mathcal{H}$ by a prime ideal must be an integral domain, which is also finite–dimensional as a $K-$vector space; thus, multiplication by a nonzero element in the quotient is injective and hence also surjective. This shows that any such quotient is a field, i.e. every prime ideal of B is maximal. Since the ring is also Noetherian, it is an Artin ring, and each residue field is a finite extension of K. Let $K' \supset K$ be the Galois closure of all the residue fields of B. If m_i are the prime ideals of B, let $K_i = B/m_i$; the exact sequence $0 \to m_i \to B \to K_i \to 0$ of $K-$modules and the flat homomorphism $K \to K'$ yield an exact sequence $0 \to K' \otimes_K m_i \to K' \otimes_K B \to K' \otimes_K K_i \to 0$. Also, the map $B \to K' \otimes_K B$ is injective. If $\mathfrak{q} \subset K' \otimes_K B$ is a prime ideal of $K' \otimes_K B$, then $\mathfrak{q} \cap B = m_i$ for some i, and $K' \otimes_K m_i \subset \mathfrak{q} \subset K' \otimes_K B$. Thus, the residue field $K' \otimes_K B/\mathfrak{q}$ is a quotient of $K' \otimes_K B/K' \otimes_K m_i \simeq K' \otimes_K K_i$. But, each quotient field of $K' \otimes_K K_i$ is isomorphic to K'. Indeed, we can write $K_i = K[x]/(f(x))$, where $f(x) \in K[x]$ and $f(x) = \prod(x - \alpha_i)$, with

[1] In [5], this assumption is not made, but we can make it for our purposes.

$\alpha_i \in K'$ distinct. Then

$$\begin{aligned} K' \otimes_K K_i &= K' \otimes_K (K[x]/(f(x))) = K'[x]/(f(x)) \\ &= K'[x]/\prod(x-\alpha_i) = \prod K'[x]/(x-\alpha_i) \\ &\simeq \prod K' \end{aligned}$$

as rings. Thus, we can choose a finite extension K' of K, such that $K' \otimes_{\mathcal{O}} \mathcal{H}$ is an Artin ring all of whose residue fields are isomorphic to K'.

Let $\mathcal{O}'$ be the integral closure of $\mathcal{O}$ in K', m' the maximal ideal of $\mathcal{O}'$, and $k' = \mathcal{O}'/m'$ the residue field. Let $M' = \mathcal{O}' \otimes_{\mathcal{O}} M$ and $\mathcal{H}' = \mathcal{O}' \otimes_{\mathcal{O}} \mathcal{H}$. Since M is torsion–free, we have an inclusion $\mathcal{O} \hookrightarrow \mathcal{H}$, and since $\mathcal{O}'$ is flat as an $\mathcal{O}-$module (it is finitely generated and free), we obtain an inclusion $\mathcal{O}' \hookrightarrow \mathcal{O}' \otimes_{\mathcal{O}} \mathcal{H} = \mathcal{H}'$. We will often identify $\mathcal{O}'$ with its image in $\mathcal{H}'$. Also, we have a natural map $\mathcal{H}' \to \mathrm{End}_{\mathcal{O}'}(M') = \mathcal{O}' \otimes_{\mathcal{O}} \mathrm{End}_{\mathcal{O}}(M)$, which is injective, since $\mathcal{H} \subset \mathrm{End}_{\mathcal{O}}(M)$ and $\mathcal{O}'$ is a flat $\mathcal{O}-$module. Let $\chi : \mathcal{H} \to k$ be the eigenvalue map sending $T \in \mathcal{H}$ to the eigenvalue $a_T \in k$. Let $\chi' : \mathcal{H}' \to k'$ be the induced map on $\mathcal{H}'$, $b \otimes h \mapsto \bar{b}\chi(h)$. Of course, χ' is surjective.

Next, $\ker \chi' \subset \mathcal{H}'$ is a maximal ideal of $\mathcal{H}'$, and clearly $m' \subset \ker \chi' \cap \mathcal{O}' \subsetneq \mathcal{O}'$. Thus, $m' = \ker \chi' \cap \mathcal{O}'$. Since $\mathcal{H}'$ is finitely–generated and free as an $\mathcal{O}'-$module, it is a flat $\mathcal{O}'-$module, hence the going–down theorem holds for the extension $\mathcal{O}' \hookrightarrow \mathcal{H}'$ (see [1], chapter 5, exercise 11), and so there is a prime ideal $\mathfrak{p} \subset \ker \chi'$ of $\mathcal{H}'$ such that $\mathfrak{p} \cap \mathcal{O}' = (0)$. The composition $\mathcal{O}' \hookrightarrow \mathcal{H}' \to \mathcal{H}'/\mathfrak{p}$ now gives an inclusion $\mathcal{O}' \hookrightarrow \mathcal{H}'/\mathfrak{p}$, which we claim is in fact an isomorphism.

Indeed, first notice that the map $\mathcal{H}'/\mathfrak{p} \to \mathcal{H}'/\mathfrak{p} \otimes_{\mathcal{O}'} K'$ is injective: recall that if $S = \mathcal{O}' - \{0\}$, then we can identify $\mathcal{H}'/\mathfrak{p} \otimes_{\mathcal{O}'} K' = \mathcal{H}'/\mathfrak{p} \otimes_{\mathcal{O}'} (S^{-1}\mathcal{O}') \simeq S^{-1}(\mathcal{H}'/\mathfrak{p})$, and so if $a \in \mathcal{H}'/\mathfrak{p}$ becomes 0 in the localized ring, then $sa = 0$ in $\mathcal{H}'/\mathfrak{p}$ for some $a \in \mathcal{O}' - \{0\}$. This implies $a = 0$ because $\mathcal{H}'/\mathfrak{p}$ is a domain and hence a free $\mathcal{O}'-$module. Now, again using the identification $\mathcal{H}' \otimes_{\mathcal{O}'} K' = S^{-1}\mathcal{H}'$, we note that $\mathfrak{p} \cap S = \emptyset$, and therefore the extension $\tilde{\mathfrak{p}} = \mathfrak{p} \otimes_{\mathcal{O}'} K'$ of the ideal $\mathfrak{p}$ to the ring $\mathcal{H}' \otimes_{\mathcal{O}'} K'$ is a prime ideal. By constructing inverse maps in both directions, we can identify $\mathcal{H}'/\mathfrak{p} \otimes_{\mathcal{O}'} K' \simeq \mathcal{H}' \otimes_{\mathcal{O}'} K'/\tilde{\mathfrak{p}}$. The latter quotient is one of the residue fields of the ring $\mathcal{H} \otimes_{\mathcal{O}} K'$, hence isomorphic to K', by the choice of K'. We have found an injection $\mathcal{O}' \hookrightarrow \mathcal{H}'/\mathfrak{p} \hookrightarrow K'$, and since $\mathcal{O}'$ is integrally closed in K' and $\mathcal{H}'/\mathfrak{p}$ is integral over $\mathcal{O}'$, we deduce that indeed we must have an isomorphism $\mathcal{O}' \simeq \mathcal{H}'/\mathfrak{p}$. Since χ' sends elements of $\mathcal{O}'$ to their residue modulo m', we now obtain a factorization of χ' as the composition of a map $\psi : \mathcal{H}' \to \mathcal{O}'$ and the natural projection $\mathcal{O}' \to k'$.

Consider $M' \otimes_{\mathcal{O}'} K'$ as a module over $\mathcal{H}' \otimes_{\mathcal{O}'} K'$ and notice that the ideal $\tilde{\mathfrak{p}}$ belongs to its support. Indeed, if we assume that $(M' \otimes_{\mathcal{O}'} K')_{\tilde{\mathfrak{p}}} = 0$, then for any $m \in M'$, there exists $s \in \mathcal{H}' \otimes_{\mathcal{O}'} K' - \tilde{\mathfrak{p}}$ such that $s(m \otimes 1) = 0$ in $M' \otimes K'$. Notice that s can be written as $s = \alpha \otimes \frac{1}{b}$, some $b \in \mathcal{O}'$, where necessarily $\alpha \notin \mathfrak{p}$. So, $\alpha(m) \otimes \frac{1}{b} = 0$ in $M' \otimes K'$, hence $\frac{\alpha(m)}{b} = 0$ in $S^{-1}M'$, where again $S = \mathcal{O}' - \{0\}$. But, M' is a free $\mathcal{O}'-$module, hence $\alpha(m) = 0$. This implies that $\mathfrak{p}$ does not belong to the support M', when considered as a (finitely–generated) $\mathcal{H}'-$module. Thus, $\mathfrak{p} \not\supseteq \mathrm{Ann}_{\mathcal{H}'}(M') = 0$, which is a contradiction. In brief, $(M' \otimes_{\mathcal{O}'} K')_{\tilde{\mathfrak{p}}} \neq 0$.

In general, if A is an Artin ring with $\mathfrak{p} \subset A$ one of the prime ideals, and M is an $A-$module with $M_{\mathfrak{p}} \neq 0$, then there exists some nonzero $m \in M$ which is killed by $\mathfrak{p}$. Indeed, $A_{\mathfrak{p}}$ is a local Artin ring with maximal ideal $\mathfrak{p}$, which must be nilpotent since it equals the nilradical of the Artin ring $A_{\mathfrak{p}}$. So, $M_{\mathfrak{p}}$ is an $A_{\mathfrak{p}}-$module with $\mathfrak{p}^k M_{\mathfrak{p}} = 0$ for smallest k, $k \geq 1$. If $\frac{m}{b} \in \mathfrak{p}^{k-1} M_{\mathfrak{p}}$ is any nonzero element, then $m \in M$ is nonzero and is killed by $\mathfrak{p}$.

Therefore, in our setting, there exists some nonzero $\tilde{f} \in M' \otimes_{\mathcal{O}'} K'$, which is killed by the ideal $\tilde{\mathfrak{p}}$. We can write $\tilde{f} = f' \otimes \frac{1}{b}$, some $b \in \mathcal{O}'$ and $f' \in M'$ nonzero. From the definition of the map ψ, we have that for any $h \in \mathcal{O}'$, we have $\psi(h) \equiv h \pmod{\mathfrak{p}}$, and so $(h - \psi(h)) \otimes 1 \in \tilde{\mathfrak{p}}$ for all $h \in \mathcal{H}$. Now, $((h - \psi(h)) \otimes 1)(f' \otimes \frac{1}{b}) = \frac{(h-\psi(h))f'}{b} = 0$ in $S^{-1}M'$, and using again that M' is free as an $\mathcal{O}'-$module, we deduce $hf' = \psi(h)f'$, which implies the desired conclusion. $\square$

Chapter 5

Consequences of the Main Theorem

5.1 Constructing unramified $p-$extensions of $\mathbb{Q}(\mu_p)$

Theorem 1 gives unramified abelian extensions of $\mathbb{Q}(\mu_p)$ with Galois group of type $(p, ..., p)$. We just have to consider the Galois extension of $\mathbb{Q}$ defined as the fixed field of the kernel of $\overline{\rho}$, and translate the three properties of $\overline{\rho}$ into arithmetic properties of this number field.

We can change a basis of $\mathbb{F}^2$ such that the representation $\overline{\rho}$ from Theorem 1 in fact has the form

$$\overline{\rho}(\sigma) = \begin{pmatrix} 1 & \alpha(\sigma) \\ 0 & \overline{\chi}^{k-1}(\sigma) \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}), \text{ for all } \sigma \in G_{\mathbb{Q}},$$

where α is an appropriate function $G_{\mathbb{Q}} \to \mathbb{F}$.

Recall that the character $\overline{\chi}$ is given by

$$\overline{\chi} : G_{\mathbb{Q}} \to \Delta \to \mathbb{F}_p^*,$$

where $\Delta = G(\mathbb{Q}(\mu_p)/\mathbb{Q})$ is cyclic of order $p-1$. Note that $\ker \overline{\chi} = G(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_p))$, so $\ker \overline{\chi}$ corresponds by Galois theory to the field $\mathbb{Q}(\mu_p)$. Let $\mathbb{Q}(\mu_p^{\otimes(1-k)})$ be the field which corresponds to $\ker \overline{\chi}^{1-k} \subset G_{\mathbb{Q}}$. So, $\mathbb{Q}(\mu_p^{\otimes(1-k)})$ is the subfield of $\mathbb{Q}(\mu_p)$ with

$$G(\mathbb{Q}(\mu_p)/\mathbb{Q}(\mu_p^{\otimes(1-k)})) = \{\sigma \in \Delta \mid \sigma^{1-k} = 1\} = \{\sigma \in \Delta \mid \sigma^{\gcd(k-1,p-1)} = 1\},$$

which is the unique subgroup of Δ of order $\gcd(k-1, p-1)$, hence $\mathbb{Q}(\mu_p^{\otimes(1-k)})$ is the unique subfield of $\mathbb{Q}(\mu_p)$ whose degree over $\mathbb{Q}$ is $(p-1)/\gcd(k-1, p-1)$.

Corollary 1. *Suppose $2 \leq k \leq p-3$ is even and $p|B_k$. There exists a Galois extension $E'/\mathbb{Q}$ containing $\mathbb{Q}(\mu_p^{\otimes(1-k)})$, such that*

i) $E'/\mathbb{Q}(\mu_p^{\otimes(1-k)})$ is everywhere unramified.

ii) The Galois group $H' = G(E'/\mathbb{Q}(\mu_p^{\otimes(1-k)}))$ is abelian, nontrivial, and of type $(p, ..., p)$.

iii) For $\sigma \in G' = G(E'/\mathbb{Q})$ and $\tau \in H'$, we have $\sigma\tau\sigma^{-1} = \overline{\chi}^{1-k}(\sigma)\tau$.

Proof. The kernel $\ker\overline{\rho}$ is a closed normal subgroup of $G_{\mathbb{Q}}$, hence its fixed field E' is a finite Galois extension of $\mathbb{Q}$. Also, $\ker\overline{\rho} \subset \ker\overline{\chi}^{1-k}$, so $\mathbb{Q}(\mu_p^{\otimes(1-k)}) \subset E'$. By definition, $G(E'/\mathbb{Q}) \simeq \text{im } \overline{\rho}$, and under this identification, the natural restriction map $G_{\mathbb{Q}} \to G(E'/\mathbb{Q})$ becomes $\overline{\rho} : G_{\mathbb{Q}} \to \text{im } \overline{\rho}$.

If $\mathfrak{B}$ is any finite prime of E', and $\tilde{\mathfrak{B}} \subset \overline{\mathbb{Z}}$ is a maximal ideal with $\tilde{\mathfrak{B}} \cap E' = \mathfrak{B}$, then the decomposition group $D_{\mathfrak{B}} \subset G(E'/\mathbb{Q})$ for $\mathfrak{B}$ in $G(E'/\mathbb{Q})$ is the image of the decomposition group $D_{\tilde{\mathfrak{B}}}$ under the natural restriction $G_{\mathbb{Q}} \to G(E'/\mathbb{Q})$. Thus, $D_{\mathfrak{B}} = \overline{\rho}(D_{\tilde{\mathfrak{B}}})$. A similar statement holds for inertia groups.

We are now ready to verify the three required properties. To verify (ii), note that by definition,

$$H' = \left\{ \begin{pmatrix} 1 & \alpha(\sigma) \\ 0 & 1 \end{pmatrix} \mid \sigma \in G_{\mathbb{Q}}, \overline{\chi}^{1-k}(\sigma) = 1 \right\} \subset G' \subset \text{GL}(2, \mathbb{F}).$$

Clearly, H' is abelian and killed by p. It is nontrivial because by Theorem 1, (ii), the order of im $\overline{\rho}$ and hence the degree $[E'/\mathbb{Q}]$ is divisible by p: indeed, if $p \nmid |\text{im}(\overline{\rho})|$, then $\overline{\rho}$ can be viewed as a representation of the finite group $G_{\mathbb{Q}}/\ker\overline{\rho}$, whose order is prime to p, hence ordinary representation theory applies (e.g., [4], 10.8) and $\overline{\rho}$ would be semisimple. On the other hand, the degree $[\mathbb{Q}(\mu_p^{\otimes(1-k)}) : \mathbb{Q}]$ divides $p-1$ and is therefore prime to p.

Next, to verify (i), if $l \neq p$ and λ is a prime of E' over l, we have

$$I_\lambda = \overline{\rho}(I_{\tilde{\lambda}}) = \{1\},$$

since $\overline{\rho}$ is unramified outside p, namely $I_{\tilde{\lambda}} \subset \ker\overline{\rho}$ (here $\tilde{\lambda}$ is a maximal ideal of $\overline{\mathbb{Z}}$ lying over λ). Thus, $E'/\mathbb{Q}$ is unramified outside p.

Let $\mathfrak{p}$ be the unique prime of $\mathbb{Q}(\mu_p^{\otimes(1-k)})$ over p (we know that $\mathbb{Q}(\mu_p)/\mathbb{Q}$ and hence $\mathbb{Q}(\mu_p^{\otimes(1-k)})/\mathbb{Q}$ is totally ramified at p). Let $\mathfrak{B}$ be a prime of E'

over $\mathfrak{p}$, and let $D'_{\mathfrak{B}|\mathfrak{p}} \subset G(E'/\mathbb{Q}(\mu_p^{\otimes(1-k)}))$ be the decomposition group for $\mathfrak{B}$ over $\mathfrak{p}$. If $D_{\mathfrak{B}} \subset G(E'/\mathbb{Q})$ is the decomposition group for $\mathfrak{B}|p$, and $D_{\tilde{\mathfrak{B}}} \subset G_{\mathbb{Q}}$ is the absolute decomposition group of a maximal ideal of $\overline{\mathbb{Z}}$ over $\mathfrak{B}$, we have that

$$D'_{\mathfrak{B}|\mathfrak{p}} = D_{\mathfrak{B}} \cap H' = \overline{\rho}(D_{\tilde{\mathfrak{B}}}) \cap H' = \{1\}$$

because $\overline{\rho}(D_{\tilde{\mathfrak{B}}})$ has order prime to p by property (iii) in Theorem 1, while H' is a $p-$group. So, in fact, $\mathfrak{p}$ splits completely in E'.

Finally, for any $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in H'$ and $\begin{pmatrix} 1 & \alpha(\sigma) \\ 0 & \overline{\chi}^{k-1}(\sigma) \end{pmatrix} \in G(E'/\mathbb{Q})$ (for some $\sigma \in G_{\mathbb{Q}}$), we compute directly

$$\begin{pmatrix} 1 & \alpha(\sigma) \\ 0 & \overline{\chi}^{k-1}(\sigma) \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \alpha(\sigma) \\ 0 & \overline{\chi}^{k-1}(\sigma) \end{pmatrix}^{-1} = \begin{pmatrix} 1 & \overline{\chi}^{1-k}(\sigma)x \\ 0 & 1 \end{pmatrix}$$

which proves the conjugation formula (iii). □

Now, we can replace $\mathbb{Q}(\mu_p^{\otimes(1-k)})$ by $\mathbb{Q}(\mu_p)$ above to obtain abelian unramified $p-$extensions of $\mathbb{Q}(\mu_p)$.

Theorem 3. *Suppose $2 \leq k \leq p-3$ is even and $p|B_k$. There exists a Galois extension $E/\mathbb{Q}$ containing $\mathbb{Q}(\mu_p)$, such that*

i) $E/\mathbb{Q}(\mu_p)$ is everywhere unramified.

ii) The Galois group $H = G(E/\mathbb{Q}(\mu_p))$ is abelian, nontrivial, and of type $(p, ..., p)$.

iii) For $\sigma \in G = G(E/\mathbb{Q})$ and $\tau \in H$, we have $\sigma\tau\sigma^{-1} = \overline{\chi}^{1-k}(\sigma)\tau$.

Proof. Let E be the composite of $\mathbb{Q}(\mu_p)$ and the field E' from the last Corollary. It is then a Galois extension of $\mathbb{Q}$, and $E/\mathbb{Q}(\mu_p)$ is unramified. Since $E'/\mathbb{Q}(\mu_p^{\otimes(1-k)})$ is unramified at the prime $\mathfrak{p}$ of $\mathbb{Q}(\mu_p^{\otimes(1-k)})$ lying over p, and $\mathbb{Q}(\mu_p)/\mathbb{Q}(\mu_p^{\otimes(1-k)})$ is totally ramified over $\mathfrak{p}$, it follows that

$$E' \cap \mathbb{Q}(\mu_p) = \mathbb{Q}(\mu_p^{\otimes(1-k)}),$$

hence restriction induces an isomorphism

$$H = G(E/\mathbb{Q}(\mu_p)) \simeq H'.$$

This proves automatically (ii) and for (iii), note that H is normal in G and if $\sigma \in G$, $\tau \in H$, then

$$(\sigma\tau\sigma^{-1})|_{E'} = \sigma|_{E'}\tau|_{E'}\sigma^{-1}|_{E'} = \overline{\chi}(\sigma)^{1-k}\tau|_{E'} = (\overline{\chi}(\sigma)^{1-k}\tau)|_{E'},$$

so the isomorphism $H \simeq H'$ gives $\sigma\tau\sigma^{-1} = \overline{\chi}(\sigma)^{1-k}\tau$, as stated. □

5.2 Ribet's converse to Herbrand

As a second consequence of the Main Theorem 1, we present Ribet's proof of the converse to Herbrand's theorem. Assuming that $p|B_k$, class field theory allows one to identify a certain isotypic component of a quotient of the class group of $\mathbb{Q}(\mu_p)$ with a corresponding isotypic component of the Galois group $G(\tilde{E}/\mathbb{Q}(\mu_p))$, where $\tilde{E}$ is the largest abelian unramified extension of $\mathbb{Q}(\mu_p)$ of type $(p, ..., p)$. We know how to construct a nontrivial subfield of $\tilde{E}$ with certain properties from the previous section, which easily yields the desired nontrivial isotypic component.

Let A be the class group of the cyclotomic field $\mathbb{Q}(\mu_p)$, and consider the $\mathbb{F}_p-$vector space $C = A/A^p$. The Galois group $\Delta = G(\mathbb{Q}(\mu_p)/\mathbb{Q})$ acts on C, and we regard C as an $\mathbb{F}_p[\Delta]-$module. Recall that the character

$$\overline{\chi} : \Delta \to \mathbb{F}_p^*,$$

now viewed as a character on Δ, generates the character group of Δ.

Since $p \nmid |\Delta|$, the theory of ordinary representations implies that we have a decomposition

$$C = \bigoplus_{i \pmod{p-1}} C(\overline{\chi}^i),$$

where $C(\overline{\chi}^i)$ is the $\overline{\chi}^i-$isotypic component of C as an $\mathbb{F}_p[\Delta]$ module, i.e.,

$$C(\overline{\chi}^i) = \left\{ c \in C \mid \sigma c = \overline{\chi}^i(\sigma)c, \text{ all } \sigma \in \Delta \right\}.$$

Theorem 4. *Let k be an even integer, $2 \leq k \leq p-3$, and suppose $p|B_k$. Then $C(\overline{\chi}^{1-k}) \neq \{0\}$.*

Proof. We need the following result from class field theory: there exists a maximal abelian unramified extension L of $\mathbb{Q}(\mu_p)$, called the Hilbert class field of $\mathbb{Q}(\mu_p)$. If $I_{\mathbb{Q}(\mu_p)}$ is the group of fractional ideals of $\mathbb{Q}(\mu_p)$, recall that the map

$$I_{\mathbb{Q}(\mu_p)} \to G(L/\mathbb{Q}(\mu_p)), \qquad \mathfrak{p} \mapsto \mathrm{Frob}_{L/\mathbb{Q}(\mu_p)}(\mathfrak{p})$$

induces an isomorphism

$$Art : A \simeq G(L/\mathbb{Q}(\mu_p)).$$

Therefore, by Galois theory, abelian unramified extensions of $\mathbb{Q}(\mu_p)$ correspond to subgroups of A, and since A^p is the smallest subgroup of A such

that A/A^p is of type $(p,...,p)$, we have that there exists a maximal abelian unramified extension of type $(p,...,p)$ of $\mathbb{Q}(\mu_p)$, which we denote by $\tilde{E}$. Thus, now by Galois theory, the Artin map induces an isomorphism

$$Art : A/A^p \simeq \tilde{H} = G(\tilde{E}/\mathbb{Q}(\mu_p)). \tag{5.1}$$

We also recall from class field theory that $L/\mathbb{Q}$ is Galois. It follows that $\tilde{E}/\mathbb{Q}$ is Galois as well because for any $\sigma \in G(L/\mathbb{Q})$, we have $\sigma(\mathbb{Q}(\mu_p)) = \mathbb{Q}(\mu_p)$ and $\sigma(\tilde{E})$ is therefore an abelian unramified extension of $\mathbb{Q}(\mu_p)$ of type $(p,...,p)$, hence $\sigma(\tilde{E}) \subset \tilde{E}$ as $\tilde{E}$ is the maximal such extension of $\mathbb{Q}(\mu_p)$ by definition.

Therefore, $\tilde{H}$ is a normal subgroup of $\tilde{G} = G(\tilde{E}/\mathbb{Q})$, and we note that Δ acts on $\tilde{H}$ by conjugation. Namely, for $\overline{\sigma} \in \Delta$ and $\tau \in \tilde{H}$, consider a lift $\sigma \in G(\tilde{E}/\mathbb{Q})$ of $\overline{\sigma}$, and define $\overline{\sigma}.\tau = \sigma\tau\sigma^{-1} \in \tilde{H}$. This is well–defined (independent of choice of σ) because $\tilde{H}$ is abelian. Since $\tilde{H}$ is an abelian group of type $(p,...,p)$, it now becomes an $\mathbb{F}_p[\Delta]-$module.

Note that the Artin map (5.1) is now an isomorphism of $\mathbb{F}_p[\Delta]-$modules. Indeed, it suffices to recall that for a prime ideal $\mathfrak{p}$ in $\mathbb{Q}(\mu_p)$ and $\sigma \in G(\tilde{E}/\mathbb{Q})$, we have $\mathrm{Frob}_{\tilde{E}/\mathbb{Q}(\mu_p)}(\sigma(\mathfrak{p})) = \sigma\mathrm{Frob}_{\tilde{E}/\mathbb{Q}(\mu_p)}(\mathfrak{p})\sigma^{-1}$.

Therefore, to prove that $C(\overline{\chi}^{1-k}) \neq \{0\}$, it is equivalent to prove that $\tilde{H}(\overline{\chi}^{1-k}) \neq \{1\}$. In other words, the statement of the Theorem is equivalent to the following one: there exists $\tilde{\tau} \in \tilde{H}, \tilde{\tau} \neq 1$, such that for all $\sigma \in \tilde{G}$ (equivalently, for all $\overline{\sigma} \in \Delta$), we have $\sigma\tilde{\tau}\sigma^{-1} = \overline{\chi}^{1-k}(\sigma)\tilde{\tau}$.

Let E be the abelian unramified $p-$extension of $\mathbb{Q}(\mu_p)$ from Theorem 3, so $E \subset \tilde{E}$ by the definition of $\tilde{E}$. Also, $E/\mathbb{Q}$ is Galois and $H = G(E/\mathbb{Q}(\mu_p))$ is abelian, hence Δ acts on H by conjugation as before, and H can be regarded as an $\mathbb{F}_p[\Delta]-$module. Note that the natural restriction

$$\pi : \tilde{H} \to H$$

is a surjective map of $\mathbb{F}_p[\Delta]-$modules. Indeed, if $\tau \in \tilde{H}$ and $\overline{\sigma} \in \Delta$, choose a lift $\sigma \in G(\tilde{E}/\mathbb{Q})$; then

$$(\overline{\sigma}.\tau)|_E = (\sigma\tau\sigma^{-1})|_E = \sigma|_E\tau|_E\sigma^{-1}|_E = \overline{\sigma}.(\tau|_E).$$

Therefore, again using that $p \nmid |\Delta|$, we know from ordinary representation theory that $\tilde{H}$ is a semisimple $\mathbb{F}_p[\Delta]-$module, and hence $\ker\pi$ has a complement in $\tilde{H}$; therefore, there exists a lifting

$$i : H \hookrightarrow \tilde{H},$$

which is an $\mathbb{F}_p[\Delta]-$module map (and for $x \in H, \pi(i(x)) = x$).

Choose $\tau \in H$, $\tau \neq 1$, and set $\tilde{\tau} = i(\tau) \in \tilde{H}$, $\tilde{\tau} \neq 1$. Let $\sigma \in G(\tilde{E}/\mathbb{Q})$. Then $\sigma\tilde{\tau}\sigma^{-1} \in \tilde{H}$, and

$$(\sigma\tilde{\tau}\sigma^{-1})|_E = \sigma|_E\tau\sigma^{-1}|_E = \overline{\chi}^{1-k}(\sigma)\tau = (\overline{\chi}^{1-k}(\sigma)\tilde{\tau})|_E.$$

Since i is a map of $\Delta-$modules, we have $\sigma\tilde{\tau}\sigma^{-1} = \sigma i(\tau)\sigma^{-1} = i(\sigma\tau\sigma^{-1})$. The restrictions to E of two elements in im i are equal, and hence we must have

$$\sigma\tilde{\tau}\sigma^{-1} = \overline{\chi}^{1-k}(\sigma)\tilde{\tau},$$

as desired. $\square$

Bibliography

[1] Atiyah, M., Macdonald, I.: Introduction to commutative algebra, Westview Press, 1969.

[2] Carlitz, L.: A generalization of Maillet's determinant and a bound for the first factor of the class number. Proc. A.M.S. **12**, 256–261 (1961)

[3] Carlitz, L., Olson, F.R.: Maillet's determinant. Proc. A.M.S. **6**, 265–269 (1955)

[4] Curtis, C., Reiner, I., Representation theory of finite groups and associative algebras. New York: Interscience 1962

[5] Deligne, P., Serre, J-P.: Formes modulaires de poids 1. Ann. Acient. Ec. Norm. Sup., 4^{e} serie, **7**, 507–530 (1974).

[6] Diamond, F., Shurman, J.: A first course in modular forms, Graduate texts in mathematics, **228**, Springer, New York, 2005

[7] Greenberg, R.: A generalization of Kummer's criterion. Inventiones math. **21**, 247–254 (1973)

[8] Khare, C.: Notes on Ribet's converse to Herbrand

[9] Koblitz, N.: p-adic Numbers, p-adic Analysis, and Zeta–functions, 2nd ed., Springer–Verlag, 1984.

[10] Ribet, K.: A modular construction of unramified $p-$extensions of $\mathbb{Q}(\mu_p)$. Inventiones math. **34**, 151–162 (1976).