PONTIFICIA
UNIVERSIDAD
CATÓLICA
DE CHILE

FACULTAD DE MATEMÁTICAS

Ribet's modular construction in weight k and Class Field Theory

by

Anibal Aravena

A thesis presented to the Pontificia Universidad Católica de Chile
in fulfillment of the thesis requirement for the degree of
Master of Mathematics.

Professor Advisor: Ricardo Menares

Thesis Committee:
Ricardo Menares (Pontificia Universidad Católica de Chile)
Hector Pastén (Pontificia Universidad Católica de Chile)
Nicolas Billerey (Université Clermont Auvergne)

August 2022

Santiago, Chile.

Acknowledgements

First, I would like to thank my Professor Advisor Ricardo Menares who has been supporting me academically and financially since I was an undergraduate student. His comments and advice in writing mathematics have been very helpful to the process of creating this thesis. Also, I would like to thank him for introducing me to the concept of group representations, which is part of the subject of this work and has become my favorite topic.

I would further like to thank my committee members Professor Hector Pastén and Professor Nicolas Billerey who took the time to read my thesis. A special thanks to the second professor for his quick and careful comments that helped the final version of this work.

Lastly, I would like to thank my family members for their unconditional love and support throughout all these years. I love you all!

This thesis was partially supported by FONDECYT 1211858 and 1171329.

Introduction

An odd prime p is said to be irregular if p divides the class number of $K = \mathbb{Q}(\mu_p)$, where $\mu_p = \langle e^{2\pi i/p} \rangle$. In 1850, Kummer showed a connection between irregular primes and the set of Bernoulli numbers $\{B_k\}_{k\geq 0}$. Those numbers are defined by the Taylor series

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

Each B_k is in fact rational and we may write pB_k if p divides the numerator of B_k. Kummer proved the following.

Theorem 1 ([Was97], Thm. 5.34)**.** *If $p \mid B_k$ for some $2 \leq k \leq p-3$ even, then p is irregular.*[1]

This result was strengthened in the following way. Define to be A_K the class group of K and consider the $\mathbb{F}_p$-vector space

$$C = A_K/A_K^p,$$

with the natural action of $\Delta = \mathrm{Gal}(K/\mathbb{Q})$[2]. With this notation Kummer's Theorem may be written as

$$p|B_k \text{ for some } 2 \leq k \leq p-3 \text{ even} \Rightarrow C \neq 0.$$

Now let $\zeta \in \mu_p$ be a primitive pth-root of unity. The (canonical) isomorphism $\chi : \Delta \to \mathbb{F}_p^*$ defined by the relation

$$\sigma(\zeta) = \zeta^{\chi(\sigma)} \qquad \forall \sigma \in \Delta,$$

generates the set $\{\chi^i : i \mod p-1\}$ of characters of Δ. Since Δ has order co-prime with p, one obtains a canonical decomposition for C

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

where $C(\chi^i)$ is the χ^i-eigenspace of C

$$C(\chi^i) = \{x \in C : g \cdot x = \chi^i(g)x \text{ for all } g \in \Delta\}.$$

In 1976, Ribet proved the following stronger result.

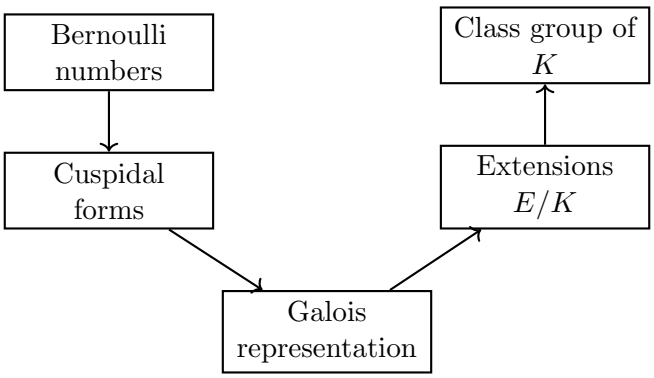
[1] Kummer also proved the converse, but in this thesis we focus only in this direction.

[2] For a class $a \in A_K$, consider a representative fractional ideal I of K, then $\sigma \cdot a$ is the (well defined) class containing $\sigma(I)$.

Theorem A ([Rib76]). *If $p|B_k$ for some $2 \leq k \leq p-3$ even, then $C(\chi^{1-k}) \neq 0$.*[3]

Under the assumption $p|B_k$, Ribet begins by constructing a cuspidal eigenform of weight 2 and level p whose q-coefficients satisfy certain congruence conditions mod p. Then, he uses the Eichler–Shimura relation to obtain a Galois representation ρ over a p-adic field. This representation has a special reduction $\overline{\rho}$ which cuts out an nontrivial unramified abelian extension E/K with a prescribed action of Δ on $\mathrm{Gal}(E/K)$. The non-triviality of this extension is a consequence of a crucial property of the representation $\overline{\rho}$ which is obtained using Raynaud's theory on groups schemes of type $(p, p, ..., p)$[4]. Then Theorem A follows from Class Field Theory.

In summary, we see that Ribet's argument is divided into the following parts



The main part of this thesis focuses on proving Theorem A following this scheme, but instead of working in weight 2 we will work directly in weight k. Since the weight is $k > 2$, we use Deligne's construction to obtain a Galois representation ρ over a p-adic field. This Galois representation will have a reduction $\overline{\rho}$ satisfying the same properties as in Ribet's construction but for the proof of the crucial property, we follow an approach using a result of Mazur and Wiles about p-ordinary modular forms. This approach avoids the use of Raynaud's theory.

The first Chapter is intended to provide the necessary tools which we will use. The definitions of modular forms and Hecke operators are omitted and well known results are just cited. We also state without proof important Theorems such as Deligne's construction of Galois representations and Mazur-Wiles Theorem on p-ordinary modular forms. The proof of those results require advance tools which are far from the scope of this thesis and the author's background.

The second Chapter is dedicated on proving Theorem A. The proof is divided in four sections where each section represents one arrow of the scheme.

In the last chapter, following a recent work of Lang and Wake ([LW21], Section 3), we prove some new results on the Class Field Theory of the extension E/K constructed during the proof of Ribet's Theorem. In particular, we obtain information on the splitting of primes

[3] Its reciprocal is also true and it was proved by Herbrand in 1935. Thus Ribet's result is also know as Herbrand converse.

[4] See part (iv) of Theorem 2.4 for this crucial property

Theorem B. *Assume that $p|B_k$. Let $\mathfrak{q}$ be a prime of K above a rational prime $q \neq p$. If $q^{k-1} \not\equiv 1 \mod p$, then $\mathfrak{q}$ splits completely in the extension E.*

Theorem C. *There exist (infinitely many) primes $\mathfrak{q}$ in K above a prime q satisfying $q^{k-1} \equiv 1 \mod p$ which do not split completely in the extension E/K.*

At the end of the chapter, we show that the extension E/K may be defined canonically from K. Thus obtaining general statements for both Theorems.

Sources. During the writing of this thesis, I found very helpful Mazur's paper [Maz11] and Dalawat's paper [Dal09]. The mind scheme is borrowed from Mazur's paper. For information on cyclotomic fields, see [Was97].

Contents

Chapter 1

Preliminaries

1.1 Modular forms

For $k \geq 0$ even, we denote $\mathcal{M}_k$ and $\mathcal{S}_k$ the $\mathbb{C}$-vector space of modular forms and cusp forms of weight k respectively. For a definition of modular form, see Diamond and Shurman book [DS05]. Since we will be working only in level 1, Serre's book [Ser73] is also useful.

1.1.1 A basis for $\mathcal{M}_k$ and $\mathcal{S}_k$

In this subsection, we prove the existence of a basis for the spaces $\mathcal{M}_k$ and $\mathcal{S}_k$ satisfying certain properties. Roughly speaking, the properties of this basis will allow us to change the set of scalars $\mathbb{C}$ to an algebraic extension $\mathbb{K}$ of $\mathbb{Q}$, in other words, passing from analytic objects to algebraic ones.
We start by remembering some classical modular forms. For $k > 2$ even, we have the Eisenstein series

$$E_k(\tau) = -\frac{B_k}{2k} + \sum_{n\geq 1} \sigma_{k-1}(n) q^n \in \mathcal{M}_k \qquad q = e^{2\pi i \tau},$$

where $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$. For $k = 12$ we have the Δ cusp form

$$\Delta(\tau) = q \prod_{n\geq 1} (1-q^n)^{24} = \sum_{n\geq 1} \tau(n) q^n \in \mathcal{S}_k \qquad q = e^{2\pi i \tau}.$$

Using Eisenstein series E_k and the cusp form Δ, it is possible to give a general description of the space of modular forms and cusp forms.

Theorem 1.1. *([Ser73], Pag. 88) Let $k \geq 0$ even.*

(1) For $k \geq 4$, we have $\mathcal{M}_k = \mathbb{C}E_k \bigoplus \mathcal{S}_k$, and so $\operatorname{Dim} \mathcal{M}_k = \operatorname{Dim} \mathcal{S}_k + 1$.

(2) We have $\mathcal{M}_2 = \{0\}$, and for $k \in \{0, 4, 6, 8, 10\}$, $\mathcal{M}_k$ has dimension 1 with basis $1, E_4, E_6, E_8, E_{10}$ respectively.

(3) Multiplication by Δ defines an isomorphism from $\mathcal{M}_{k+12}$ onto $\mathcal{S}_k$.

Proposition 1.2. *Let $k \geq 0$ even. A basis for $\mathcal{M}_k$ is given by:*

$$\mathcal{B} = \left\{ E_4^{a_0} E_6^{b_0}, E_4^{a_1} E_6^{b_1} \Delta, \ldots, E_4^{a_n} E_6^{b_n} \Delta^n \right\},$$

where a_i, b_i, i are non negative integers satisfying $4a_i + 6b_i + 12i = k$ and $n = n(k)$ is the maximal integer i for which such integers exist.

Proof. We prove by induction on N that the Proposition is true for $k < 12N$. For $N = 1$, we have $k < 12$ and so $n(k) = 0$. The equation $4a_i + 6b_i = k$ has exactly one (non negative) integer solution except for $k = 2$ which has no solution. On the other hand we have

$$1 \in M_0, \qquad E_4 \in \mathcal{M}_4, \qquad E_6 \in \mathcal{M}_6, \qquad E_4^2 \in M_8, \qquad E_4 E_6 \in \mathcal{M}_{10},$$

and they form a basis by part (2) of Theorem 1.1. This proves the Proposition for $k < 12$.
Suppose it is true for N and let $12 \leq k < 12(N+1)$. Since $k - 12 < N$, we have a basis

$$\mathcal{B} = \left\{ E_4^{a_0} E_6^{b_0}, E_4^{a_1} E_6^{b_1} \Delta, \ldots, E_4^{a_n} E_6^{b_n} \Delta^n \right\},$$

for M_{k-12}. And by part (1) and (3) of Theorem 1.1, we have

$$\left\{ E_4^{a_0} E_6^{b_0+2} \right\} \bigcup \left\{ E_4^{a_0} E_6^{b_0} \Delta, E_4^{a_1} E_6^{b_1} \Delta^2, \ldots, E_4^{a_n} E_6^{b_n} \Delta^{n+1} \right\},$$

is a basis for $\mathcal{M}_k$. ∎

For $j \geq 0$ integer, we denote $\psi_j : \mathcal{M}_k \to \mathbb{C}$ the linear operator taking a modular form $f = \sum_{n \geq 0} a_n(f) q^n$ to its q^j-coefficient $a_j(f)$. The following Proposition describes the properties of our special basis.

Proposition 1.3. *Let $k \geq 0$ even. Then there exists basis for $\mathcal{M}_k$ and $\mathcal{S}_k$ of the form*

$$\mathcal{B} = \{f_0, f_1, \ldots, f_n\}, \qquad \mathcal{B}' = \{f_1, \ldots, f_n\},$$

respectively, where each element f_i has integer q-coefficients and satisfies

$$\psi_j(f_i) = \begin{cases} 1 & \text{if } j = i \\ 0 & \text{if } j < i \end{cases}.$$

Proof. Since $\operatorname{Dim} \mathcal{M}_k = \operatorname{Dim} \mathcal{S}_k + 1$, it is enough to prove the statement for $\mathcal{M}_k$. Let $\{E_4^{a_i} E_6^{b_i} \Delta^i\}_{i=0}^n$ be a basis for $\mathcal{M}_k$ as in last Proposition. Note that

$$\psi_j(E_4^{a_i} E_6^{b_i} \Delta^i) = 0$$

if $j < i$. Since $B_4 = -1/30$ and $B_6 = 1/42$, the formulas for E_k and Δ show that we may find integer λ_i such that the element $f_i = \lambda_i E_4^{a_i} E_6^{b_i} \Delta^i$ has integer q-coefficients and $\psi_i(f_i) = 1$. ∎

1.1.2 Modular forms with q-coefficients in some ring,

For any subring $A \subset \mathbb{C}$, we define $(\mathcal{M}_k)_A$ to be the subset of $\mathcal{M}_k$ of modular forms whose q-coefficients in the Fourier expansion belong to A. We make an analogous definition for $(\mathcal{S}_k)_A$.

Proposition 1.4. *$(\mathcal{M}_k)_A$ and $(\mathcal{S}_k)_A$ are free A-modules of rank $\mathrm{Dim}_k(\mathcal{M}_k)$ and $\mathrm{Dim}_k(\mathcal{S}_k)$ respectively.*

Proof. Take a basis $\{f_0, f_1, \ldots, f_n\}$ for $\mathcal{M}_k$ as in Proposition 1.3. We claim that the A-module generated by this basis is free and it is exactly $(\mathcal{M}_k)_A$. Clearly it is free and contained in $(\mathcal{M}_k)_A$. Let $f \in (\mathcal{M}_k)_A$ and write

$$f = \alpha_0 f_0 + \alpha_1 f_1 + \ldots + \alpha_n f_n,$$

with $\alpha_i \in \mathbb{C}$. We prove by induction on $k \leq n$ that $\alpha_i \in A$ for all $i \leq k$.
If $k = 0$, we apply ψ_0 obtaining

$$\alpha_0 = \psi_0(f) \in A.$$

Now assume that $\alpha_i \in A$ for all $i \leq k$ with $k < n$. By evaluating ψ_{k+1} we obtain

$$\alpha_{k+1} = \psi_{k+1}(f) - \alpha_0\psi_{k+1}(f_0) - \alpha_1\psi_{k+1}(f_1) - \ldots - \alpha_k\psi_{k+1}(f_k) \in A.$$

This proves the proposition for $(\mathcal{M}_k)_A$. The same argument works for the A-module $(\mathcal{S}_k)_A$ using the basis $\mathcal{B}'$ of Proposition 1.3. ∎

1.1.3 Hecke operators

Let $k \geq 0$ even fixed. For a natural number $n \geq 1$, there exits a Hecke operator

$$T_n : \mathcal{M}_k \to \mathcal{M}_k,$$

(see [DS05], Chapter 5 for a definition of Hecke operators). The following Proposition describes how these Hecke operators act on the q-coefficients of a modular form.

Proposition 1.5. *([DS05], Prop. 5.3.1) Let $f \in \mathcal{M}_k$ with Fourier expansion*

$$f(\tau) = \sum_{m \geq 0} a_m(f) q^m, \qquad q = e^{2\pi i \tau}.$$

Then for all $n \geq 1$ integer, $T_n f$ has Fourier expansion

$$T_n f(\tau) = \sum_{m \geq 0} a_m(T_n f) q^m,$$

where

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

Remark 1.5.1. From the formula for $a_m(T_n f)$, we see that T_n sends cusp forms to cusp forms. Moreover, if A is any subring of $\mathbb{C}$, then T_n restricts to an A-morphism on $(\mathcal{M}_k)_A$ and $(\mathcal{S}_k)_A$.

It is well known that Hecke operators commute, thus the Hecke algebra

$$\mathbb{T}_{\mathbb{Z}} \coloneqq \mathbb{Z}[\{T_n : n \geq 1\}] \subset \mathrm{End}_{\mathbb{C}}(\mathcal{M})$$

forms a commutative $\mathbb{Z}$-algebra. We will use this property repeatedly in this thesis. Another important property that we will use is the fact that the Eisenstein series E_k is an eigenvector for each Hecke operator T_n.

Proposition 1.6 ([DS05], Prop. 5.2.3)**.** *For each natural number $n \geq 1$, the Eisenstein series $E_k \in \mathcal{M}_k$ is an eigenvector of T_n with corresponding eigenvalue $\sigma_{k-1}(n)$.*

Note that the value of the eigenvalue of T_n with eigenvector E_k coincides with the q^n-coefficient of the Fourier expansion of E_k. The following Proposition tells us that this is always the case if the modular form f is normalized i.e. if f has a Fourier expansion of the form

$$f(\tau) = a_0(f) + q + \sum_{m \geq 2} a_m(f) q^m, \qquad q = e^{2\pi i \tau}.$$

Proposition 1.7. *Let $f = \sum_{m \geq 0} a_m(f) q^m \in \mathcal{M}_k$ be a normalized modular form which is an eigenvector for the operator T_n. If λ_n is the corresponding eigenvalue, then*

$$\lambda_n = a_n(f).$$

Proof. Taking $m = 1$ in the formula for $a_m(T_n f)$ of Proposition 1.5, we obtain

$$a_1(T_n f) = a_n(f).$$

Also, by hypothesis we have that $T_n f = \lambda_n f$. Therefore $a_1(T_n f) = \lambda_n a_1(f)$. Comparing both equalities and using $a_1(f) = 1$, we conclude that $\lambda_n = a_n(f)$. ∎

Definition 1.8. A modular form $f \in \mathcal{M}_k$ is called an eigenform if it is an eigenvector of T_n for each $n \geq 1$. If $f = \sum_{m \geq 1} a_m(f) q^m \in \mathcal{S}_k$ is a normalized cuspidal eigenform, we define

$$K_f = \mathbb{Q}(\{a_m(f) : m \geq 1\}) \subset \mathbb{C},$$

the Hecke field of f. This is smallest field L such that $f \in (\mathcal{S}_k)_L$.

Remark 1.8.1. Note that if $f = \sum_{m \geq 0} a_m(f) q^m \in \mathcal{M}_k$ is an eigenform with $a_1(f) = 0$, then the proof of Proposition 1.7 shows that f is constant. Thus, in weight $k > 0$ we may always normalize eigenforms.

Proposition 1.9. *Let $f = \sum_{m \geq 1} a_m(f) q^m \in \mathcal{S}_k$ be a normalized cuspidal eigenform. Then its Hecke field K_f is a finite extension of $\mathbb{Q}$.*

Proof. Let $\mathbb{K}$ be the field generated by the eigenvalues of each operator T_n. Since $a_n(f) = \lambda_n(f)$ is an eigenvalue of T_n for all $n \geq 1$, then $K_f \subset \mathbb{K}$. Thus it is enough to prove that $\mathbb{K}$ is a finite extension over $\mathbb{Q}$.
By Remark 1.5.1, the Hecke Algebra $\mathbb{T}_{\mathbb{Z}}$ restrict to $\mathbb{Z}$-morphisms on $(\mathcal{M}_k)_{\mathbb{Z}}$. Moreover, by Proposition 1.4, $(\mathcal{M}_k)_{\mathbb{Z}}$ is free $\mathbb{Z}$-module generated by some basis of $\mathcal{M}_k$. This implies that $\mathbb{T}_{\mathbb{Z}}$ is generated by a finite set of operators and the roots of their characteristic polynomials are algebraic integers. Thus a finite set of eigenvalues, which are algebraic integers, generates all the other eigenvalues. Therefore $\mathbb{K}$ is generated by finite a set of algebraic integers and so it is a finite extension of $\mathbb{Q}$. ■

Remark 1.9.1. From the proof, we see that in fact $f \in (\mathcal{S}_k)_{\mathcal{O}_{K_f}}$ where $\mathcal{O}_{K_f}$ its the ring of integers of K_f.

1.2 Deligne-Serre lifting Lemma

Let A be a discrete valuation ring (DVR) with maximal ideal $\mathfrak{m}_A$. We say that a DVR B with maximal ideal $\mathfrak{m}_B$ is an extension of A if $A \subset B$ and $\mathfrak{m}_A = A \cap \mathfrak{m}_B$. For an A-algebra B, an A-module M, an element $f \in M$ and a set of A-endomorphisms $\mathcal{T} \subset \mathrm{End}_A(M)$, we define

$$\begin{aligned} M_B &\coloneqq M \otimes_A B \\ f_B &\coloneqq f \otimes_A 1_B \in M_B \\ \mathcal{T}_B &\coloneqq \{T_B = T \otimes_A \mathrm{id}_B : T \in \mathcal{T}\} \subset \mathrm{End}_B(M_B). \end{aligned}$$

Note that if C is a B-algebra, then it has an induced structure of A-algebra and we may identify (under a canonical isomorphism)

$$M_C = M_B \otimes_B C, \quad f_C = f_B \otimes_B 1_C \qquad \text{etc ...}$$

The next Proposition will be fundamental for the construction of appropriate cuspidal eigenforms. We assume that $K = \mathrm{Frac}(A)$ is a perfect field.

Proposition 1.10 (D-S Lemma)**.** *Let M be a free A-module of finite rank and let $\mathcal{T} \subset \mathrm{End}_A(M)$ be a set of commuting A-endomorphisms. Suppose that $f \in M$ is such that $f_{A/\mathfrak{m}_A} \in M_{A/\mathfrak{m}_A}$ is an eigenvector for each operator $T_{A/\mathfrak{m}_A} \in \mathcal{T}_{A/\mathfrak{m}_A}$ with eigenvalue $a_T \in A/\mathfrak{m}_A$. Then, there exists a DVR B extending A with field of fractions L finite finite over K, and an element $f' \in M_B$ which is an eigenvector for each operator $T_B \in \mathcal{T}_B$ whose eigenvalue $b_T \in B$ satisfies $a_T = b_T + \mathfrak{m}_B$.*

Proof. Since M is free of finite rank, the field L generated by the eigenvalues of each operator $T \in \mathcal{T}$ is a finite extension of K (see the proof of Proposition 1.9). Let B be a DVR extending A with field of fraction L[1]. We may assume that the

[1]Since L/K is finite and separable, such ring exists (see [Sta22] Remark 15.110.6).

B-module M_B is $\mathcal{T}_B$-indecomposable. Indeed, let

$$M_B = \bigoplus_{j=1}^{k} M^{(j)}$$

be a decomposition as $\mathcal{T}_B$-indecomposable modules. Since B is PID and M_B free B-module of finite rank, then each $M^{(j)}$ is also a free B-module of finite rank and

$$M_{B/\mathfrak{m}_B} = \bigoplus_{j=1}^{k} M^j_{B/\mathfrak{m}_B}$$

a decomposition as $\mathcal{T}_{B/\mathfrak{m}_B}$-modules. If we write the eigenvector $f_{B/\mathfrak{m}_B}$ as

$$f_{B/\mathfrak{m}_B} = \sum_{j=1}^{k} f^{(j)}_{B/\mathfrak{m}_B}, \qquad f^{(j)}_{B/\mathfrak{m}_B} \in M^j_{B/\mathfrak{m}B},$$

then each nonzero $f^{(j)}_{B/\mathfrak{m}_B}$ its an eigenvector with the same eigenvalue. Thus after choosing j with $f^{(j)}_{B/\mathfrak{m}_B} \neq 0$, we may assume that M_B is $\mathcal{T}_B$-indecomposable.
Let $T_B \in \mathcal{T}_B$. Since $\mathrm{End}_B(M_B)$ is free of finite rank, T_B has a minimal polynomial called p. Moreover B contains the eigenvalues of T_B (B contains the integral closure of A in L). Thus p has the form

$$p(x) = \left(x - b^{(1)}_{T_B}\right)^{e_1} \dots \left(x - b^{(n)}_{T_B}\right)^{e_n}, \qquad b^{(i)}_{T_B} \in B.$$

We claim that p has only one root. The factorization of p provides a decomposition for M_B as T_B-invariant spaces

$$M_B = \bigoplus_{j=1}^{n} M^j,$$

where M^j is the null space of $p_j(T)$ with p_j certain polynomial associated to $(x - b^{(j)}_{T_n})$(see [HK04], pag. 220). But since the elements of $\mathcal{T}_B$ commute, each M^j will be $\mathcal{T}_B$-invariant and so p has only one root because M_B is $\mathcal{T}_B$-indecomposable. Finally, the commutativity of $\mathcal{T}_B$ also implies that M_B has at least one simultaneous eigenvector f' and it is clear that its eigenvalues satisfy the required conditions. ■

1.3 Class field Theory

Let $L/F/\mathbb{Q}$ be a tower of finite field extensions. Through this section we assume that $F/\mathbb{Q}$ is Galois and L/F is unramified and abelian.
Since $F/\mathbb{Q}$ is Galois, we have $\mathrm{Gal}(L/F) \trianglelefteq \mathrm{Gal}(L/\mathbb{Q})$ and so $\mathrm{Gal}(L/\mathbb{Q})$ acts on

$\mathrm{Gal}(L/F)$ by conjugation. Moreover, since $\mathrm{Gal}(L/F)$ is abelian, $\mathrm{Gal}(L/F)$ acts trivially. Therefore we have a well defined action of $\mathrm{Gal}(F/\mathbb{Q})$ on $\mathrm{Gal}(L/F)$:

$$\sigma \cdot \tau := \sigma' \tau \sigma'^{-1},$$

where $\tau \in \mathrm{Gal}(L/F)$ and $\sigma' \in \mathrm{Gal}(L/\mathbb{Q})$ with $\sigma'|_F = \sigma \in \mathrm{Gal}(F/\mathbb{Q})$.

Let $\mathfrak{p}$ be a prime of F and $\mathfrak{B}$ a prime of L above $\mathfrak{p}$. Since L/F is unramified, there exists a unique element $\psi_{L/F}(\mathfrak{B}/\mathfrak{p}) \in \mathrm{Gal}(L/F)$ satisfying

$$\psi_{L/F}(\mathfrak{B}/\mathfrak{p})(x) \equiv x^q \mod \mathfrak{B} \quad \text{for all } x \in \mathcal{O}_L,$$

where $\mathcal{O}_L$ is the ring of integers of L and $q = N(\mathfrak{p})$ is the norm of $\mathfrak{p}$. We call $\psi_{L/F}(\mathfrak{B}/\mathfrak{p})$ the Frobenius element of $\mathfrak{B}$ over $\mathfrak{p}$. We have the following result.

Lemma 1.11. Let $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$. Then $\sigma(\mathfrak{B})$ and $\sigma(\mathfrak{p})$ are primes of L and F respectively and we have

$$\psi_{L/F}(\sigma(\mathfrak{B})/\sigma(\mathfrak{p})) = \sigma \psi_{L/F}(\mathfrak{B}/\mathfrak{p}) \sigma^{-1}. \tag{1.1}$$

Proof. The first claim follows from the fact that $L/\mathbb{Q}$ and $F/\mathbb{Q}$ are both Galois extensions. Now we calculate

$$\begin{aligned} & \psi_{L/F}(\mathfrak{B}/\mathfrak{p})(x) \equiv x^q \mod \mathfrak{B}, \quad \text{for all } x \in \mathcal{O}_L \\ \Rightarrow \quad & \sigma\psi_{L/F}(\mathfrak{B}/\mathfrak{p})(x) \equiv (\sigma(x))^q \mod \sigma(\mathfrak{B}), \quad \text{for all } x \in \mathcal{O}_L \\ \Rightarrow \quad & \sigma\psi_{L/F}(\mathfrak{B}/\mathfrak{p})\sigma^{-1}(u) \equiv (u)^q \mod \sigma(\mathfrak{B}), \quad \text{for all } u = \sigma(x) \in \sigma(\mathcal{O}_L) = \mathcal{O}_L, \end{aligned}$$

Since $N(\mathfrak{p}) = N(\sigma(\mathfrak{p})) = q$, the last relation corresponds to the definition of $\psi_{L/F}(\sigma(\mathfrak{B})/\sigma(\mathfrak{p}))$. This proves the lemma. ∎

Since every prime of L above $\mathfrak{p}$ is of the form $\sigma(\mathfrak{B})$ for $\sigma \in \mathrm{Gal}(L/F)$ and $\mathrm{Gal}(L/F)$ acts trivially on the right hand side of equation (1.1), we see that $\psi_{L/F}$ depends only on the prime $\mathfrak{p}$ of F. Henceforth we will write $\psi_{L/F}(\mathfrak{p}) = \psi_{L/F}(\mathfrak{B}/\mathfrak{p})$. Extending $\psi_{L/F}$ multiplicatively to the group of fractional ideals I_F of F, we get a group homomorphism

$$\psi_{L/F} : I_F \to \mathrm{Gal}(L/F).$$

Artin reciprocity asserts this map is surjective and factorizes through the class group A_F of F (see [Mil20] pag. 158 for example), thus obtaining a group homomorphism

$$\psi_{L/F} : A_F \to \mathrm{Gal}(L/F),$$

called the Artin map. We summarize our results in the following Proposition.

Proposition 1.12. *The Artin map $\psi_{L/F} : A_F \to \mathrm{Gal}(L/F)$ is surjective and satisfies*

$$\psi_{L/F}(\sigma \cdot a) = \sigma \cdot \psi_{L/F}(a)$$

for all $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$ and $a \in A_F$. Here $\sigma \cdot a$ is the natural action of $\mathrm{Gal}(F/\mathbb{Q})$ on A_F.

Proof. We only must prove the last claim. For a class $a \in A_F$, consider a representative fractional ideal I of F. If $I = \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}$ is its decomposition in prime ideals, then $\sigma(I) = \prod_{\mathfrak{p}} \sigma(\mathfrak{p})^{e_{\mathfrak{p}}}$. Thus it is enough to prove the case when I is a prime ideal but this is exactly what Lemma 1.11 states. ∎

1.4 Group representations

Let G be a pro-finite group (for the basic properties of these objects, see [Neu99] Chapter 4 Section 1,2). Let K be a topological field. By a representation of G of dimension n over K, or just a representation of G, we mean a continuous morphism of groups

$$\rho : G \to \mathrm{GL}_n(K),$$

where G is endowed with the Krull topology and $\mathrm{GL}_n(K)$ is endowed with the subspace topology of $M^{n\times n}(K) = K^{n^2}$.

1.4.1 Reduction of representations

We say that two representations $\rho_1, \rho_2 : G \to \mathrm{GL}_n(K)$ of G are equivalent over K if there exists matrix $M \in \mathrm{GL}_n(K)$ such that

$$\rho_1(g) = M\rho_2(g)M^{-1}, \qquad \forall g \in G.$$

Let p be a prime number. During this section K will denote a finite extension of $\mathbb{Q}_p$. We write $\mathcal{O}_K$ for its ring of integers, $\mathfrak{m}_K$ the maximal ideal and $\mathbb{F}_q = \mathcal{O}_K/\mathfrak{m}_K$ the residue field.

Proposition 1.13. *Let $\rho : G \to \mathrm{GL}_n(K)$ be a representation of G. Then ρ is equivalent to a representation $\rho' : G \to \mathrm{GL}_n(\mathcal{O}_K) \subset \mathrm{GL}_n(K)$.*

Proof. Let $V = K^n$ be the vector space of columns of dimension n over K. Note that G acts via ρ on V by multiplication on the left. For a basis $\mathcal{B}$ of V, define $\Lambda_{\mathcal{B}} \subset V$ as the $\mathcal{O}_K$-module generated by $\mathcal{B}$. Then the Proposition is equivalent to find a basis $\mathcal{B}$ such that $\Lambda_{\mathcal{B}}$ is $\rho(G)$-invariant.
Since $\mathrm{GL}_n(\mathcal{O}_K)$ is open and ρ is continuous, $H = \rho^{-1}(\mathrm{GL}_n(\mathcal{O}_K))$ is open and so it has finite index in G. Take $\{g_1, \dots, g_\ell\}$ a set of representatives for the cosets $\{Hg : g \in G\}$. If $\Lambda_0 = \mathcal{O}_K^n \subset V$ is the $\mathcal{O}_K$-module generated by the canonical basis, then Λ_0 is $\rho(H)$-invariant and so

$$\Lambda = \sum_{i=1}^{\ell} \rho(g_i)\,(\Lambda_0)$$

is a $\rho(G)$-invariant finite generated $\mathcal{O}_K$-module. Since $\mathcal{O}_K$ is PID we have that $\Lambda = \Lambda_{\mathcal{B}}$ for some basis $\mathcal{B}$ of V. ∎

Let $\rho : G \to \mathrm{GL}_n(K)$ be a representation of G and $\rho' : G \to \mathrm{GL}_n(\mathcal{O}_K)$ an equivalent representation over K with matrix coefficients in $\mathcal{O}_K$. After composing

with the projection map $\mathrm{GL}_n(\mathcal{O}_K) \to \mathrm{GL}_n(\mathbb{F}_q)$ we obtain a representation of G of dimension n over $\mathbb{F}_q$

$$\overline{\rho}' : G \to \mathrm{GL}_n(\mathbb{F}_q).$$

We called $\overline{\rho}'$ the reduction of ρ associated to ρ' or a reduction of ρ to simplify. Although equivalent representations over K

$$\rho_1, \rho_2 : G \to \mathrm{GL}_2(\mathcal{O}_K) \subset \mathrm{GL}_n(K),$$

could give us non-equivalent representation over $\mathbb{F}_q$

$$\overline{\rho}_1, \overline{\rho}_2 : G \to \mathrm{GL}_n(\mathbb{F}_q),$$

it can be proved that they share the same blocks in their Jordan form. To be specific we make the following definition.

Let $\overline{\rho} : G \to \mathrm{GL}_n(\mathbb{F}_q)$ be a representation over $\mathbb{F}_q$. Just as in the proof of Proposition 1.13, we consider the $\mathbb{F}_q$-vector space $V = \mathbb{F}_q^n$ with the action of G via $\overline{\rho}$ on it. Since V is finite dimensional, there exists a descending chain of vector spaces

$$V = V_1 \supsetneq V_2 \supsetneq \ldots \supsetneq V_{k-1} \supsetneq V_{k+1} = 0,$$

such that each V_i is G-invariant and the quotient representation

$$\overline{\rho}^{(i)} : G \to \mathrm{GL}(V_i/V_{i+1}) = \mathrm{GL}_{n_i}(\mathbb{F}_q), \quad n_i = \dim V_i - \dim V_{i+1},$$

is irreducible for all $1 \leq i \leq k$. Now consider the representation

$$\overline{\rho}' = \bigoplus_{i=1}^{k} \overline{\rho}^{(i)}.$$

The Jordan-Holder Theorem (see [CR06] pag. 79) asserts that up to equivalence, the representation $\overline{\rho}'$ is the same for every descending chain. We call this representation the semi-simplification of $\overline{\rho}$.

Theorem 1.14 (Brauer-Nesbitt)**.** *([CR06] Pag. 215) Let L be a perfect field and A a L-algebra. Let M, N be two A-modules finite-dimensional as L-vector spaces. If for all a in A, the characteristic polynomials of M and N are equal, then their semi-simplifications are equivalent.*

For a matrix $T \in \mathrm{GL}_n(K)$, we write $\operatorname{char} T$ for its characteristic polynomial. If $M \in \mathrm{GL}_n(K)$, then we have the relation $\operatorname{char} T = \operatorname{char} MTM^{-1}$.

Proposition 1.15. *Let $\rho_1, \rho_2 : G \to \mathrm{GL}_n(\mathcal{O}_K) \subset \mathrm{GL}_n(K)$ be two equivalent group representations. Then the semi-simplifications of $\overline{\rho}_1$ and $\overline{\rho}_2$ are equivalent.*

Proof. Take $M \in \mathrm{GL}_n(K)$ such that $\rho_1(g) = M\rho_2(g)M^{-1}$ for all $g \in G$. Then

$$\begin{aligned}
\operatorname{char}[\overline{\rho}_2(g)] &= \operatorname{char}[\rho_2(g)] \mod \mathfrak{m}_K \\
&= \operatorname{char}[M\rho_2(g)M^{-1}] \mod \mathfrak{m}_K \\
&= \operatorname{char}[\rho_1(g)] \mod \mathfrak{m}_K \\
&= \operatorname{char}[\overline{\rho}_1(g)]
\end{aligned}$$

After taking $L = \mathbb{F}_q$, $A = \mathbb{F}_q G$ and $M = \mathbb{F}_q^n$, $N = \mathbb{F}_q^n$ with the structure of $\mathbb{F}_q G$-module induced by $\overline{\rho}_1, \overline{\rho}_2$ respectively, we see that Proposition follows from Theorem 1.14. ■

In conclusion, the semi-simplification of a reduction $\overline{\rho}_1$ of ρ does not depend on the chosen equivalent representation ρ_1.

1.4.2 Ribet's Lemma

Now consider a two dimensional representation $\rho : G \to \mathrm{GL}_2(K)$ of G. By Proposition 1.13, ρ is equivalent to a representation ρ_0 with matrix coefficients in $\mathcal{O}_K$. Let us assume that its reduction $\overline{\rho}_0$ is reducible. Then there exist two characters $\varphi_1, \varphi_2 : G \to \mathbb{F}_q$ such that $\overline{\rho}_0$ is equivalent over $\mathbb{F}_q$ to a representation of one of the forms

$$\begin{pmatrix} \varphi_1 & * \\ 0 & \varphi_2 \end{pmatrix}, \qquad \begin{pmatrix} \varphi_1 & 0 \\ * & \varphi_2 \end{pmatrix}. \tag{1.2}$$

Its semi-simplification is the representation $\varphi_1 \oplus \varphi_2$. Note that Proposition 1.15 implies this will be the case for every reduction of ρ. In particular we see that all its reductions are reducible.
The next Proposition will be used in the construction of the special reduction mentioned in the proof of Theorem A.

Proposition 1.16 (Ribet's Lemma)**.** *Let $\rho : G \to \mathrm{GL}_2(K)$ be an irreducible representation of G such that its reductions are reducible. Then ρ is equivalent to a representation $\rho_0 : G \to \mathrm{GL}_2(\mathcal{O}_K) \subset \mathrm{GL}_2(K)$ such that its reduction is of the form*

$$\overline{\rho}_0 = \begin{pmatrix} \varphi_1 & * \\ 0 & \varphi_2 \end{pmatrix},$$

and it is not diagonalizable.

Proof. Let $\rho_I : G \to \mathrm{GL}_2(\mathcal{O}_K) \subset \mathrm{GL}_2(K)$ be an equivalent representation to ρ with matrix coefficients in $\mathcal{O}_K$. Then its reduction is equivalent to one of the two forms in (1.2). Note that since $\mathcal{O}_K^* = \mathcal{O}_K - \mathfrak{m}_K$, the natural map

$$Pr : M_{2\times 2}(\mathcal{O}_K) \to M_{2\times 2}(\mathbb{F}_q),$$

satisfies $Pr^{-1}(\mathrm{GL}_2(\mathbb{F}_q)) = \mathrm{GL}_2(\mathcal{O}_K)$, and so the restriction

$$P_r|_{\mathrm{GL}_2(\mathcal{O}_K)} : \mathrm{GL}_2(\mathcal{O}_K) \to \mathrm{GL}_2(\mathbb{F}_q),$$

is surjective. Thus after lifting a matrix from $\mathrm{GL}_2(\mathbb{F}_q)$ to $\mathrm{GL}_2(\mathcal{O}_K)$, we may assume that $\overline{\rho}_I$ is equal to one of the two forms in (1.2). Moreover, if π denotes a generator for $\mathfrak{m}_K$, the identity

$$P \begin{pmatrix} a & \pi b \\ c & d \end{pmatrix} P^{-1} = \begin{pmatrix} a & b \\ \pi c & d \end{pmatrix}, \qquad P = \begin{pmatrix} 1 & 0 \\ 0 & \pi \end{pmatrix}, \tag{1.3}$$

shows that we may assume that $\overline{\rho}_I$ takes exactly the left form in (1.2).
For a matrix $M \in \mathrm{GL}_2(K)$, we denote by $\rho_M : G \to \mathrm{GL}_n(K)$ the representation defined by $\rho_M(g) = M\rho_I(g)M^{-1}$ for all $g \in G$. Suppose for a contradiction that for every matrix satisfying:

- The representation $\rho_M : G \to \mathrm{GL}(K)$ has coefficients in $\mathcal{O}_K$.
- Its reduction is
$$\overline{\rho}_M = \begin{pmatrix} \varphi_1 & * \\ 0 & \varphi_2 \end{pmatrix}.$$

We have that $\overline{\rho}_M$ is diagonalizable.
We are going to construct by induction a convergent sequence of matrices $\{T_n\}_{n\geq 1}$ with the properties

$$\rho_{T_n}(g) = T_n\rho_I(g)T_n^{-1} \in \begin{pmatrix} \mathcal{O}_K & \mathfrak{m}_K^n \\ \mathcal{O}_K & \mathcal{O}_K \end{pmatrix}, \qquad \overline{\rho}_{T_n} = \begin{pmatrix} \varphi_1 & 0 \\ * & \varphi_2 \end{pmatrix}. \tag{1.4}$$

This will prove the Proposition. Indeed, if $T_n \to T$ is the limit, then the group representation $\rho_T : G \to \mathrm{GL}_2(K)$ has upper-right entry zero, but this is impossible since it is equivalent to ρ and so it is irreducible.

For $n = 1$ we take $T_1 = P^{-1}$ and use identity (1.3). Suppose that for $n \geq 1$, we have matrix T_n satisfying (1.4). Then

$$\rho_{P^nT_n}(g) = P^n\rho_{T_n}(g)P^{-n} \in P^n \begin{pmatrix} \mathcal{O}_K & \mathfrak{m}_K^n \\ \mathcal{O}_K & \mathcal{O}_K \end{pmatrix} P^{-n} = \begin{pmatrix} \mathcal{O}_K & \mathcal{O}_K \\ \mathfrak{m}_K^n & \mathcal{O}_K \end{pmatrix}.$$

Since conjugating by P does not change upper-left and lower-right entries, its reduction is of the form $\overline{\rho}_{P^nT_n} = \begin{pmatrix} \varphi_1 & * \\ 0 & \varphi_2 \end{pmatrix}$. Thus, by assumption of contradiction, we have that $\overline{\rho}_{P^nT_n}$ is diagonalizable. By using $Pr^{-1}(\mathrm{GL}_2(\mathbb{F}_q)) = \mathrm{GL}_2(\mathcal{O}_K)$, we find a matrix $U \in \mathrm{GL}_2(\mathcal{O}_K)$ of the form $U = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$ such that

$$\overline{\rho}_{UP^nT_n}(g) = \begin{pmatrix} 1 & \overline{u} \\ 0 & 1 \end{pmatrix} \overline{\rho}_{P^nT_n}(g) \begin{pmatrix} 1 & \overline{u} \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} \varphi_1(g) & 0 \\ 0 & \varphi_2(g) \end{pmatrix}.$$

Moreover, conjugation by U does not change the lower-left entry, then

$$\rho_{UP^nT_n}(g) = U\rho_{P^nT_n}(g)U^{-1} \in \begin{pmatrix} \mathcal{O}_K & \mathfrak{m}_K \\ \mathfrak{m}_K^n & \mathcal{O}_K \end{pmatrix}.$$

Conjugating by P^{-n} we obtain

$$\rho_{P^{-n}UP^nT_n} = (P^{-n})\rho_{UP^nT_n}(g)(P^{-n})^{-1} \in \begin{pmatrix} \mathcal{O}_K & \mathfrak{m}_K^{n+1} \\ \mathcal{O}_K & \mathcal{O}_K \end{pmatrix}$$

and $\overline{\rho}_{P^{-n}UP^nT_n} = \begin{pmatrix} \varphi_1 & 0 \\ * & \varphi_2 \end{pmatrix}$ since $\overline{\rho}_{UP^nT_n} = \begin{pmatrix} \varphi_1 & 0 \\ * & \varphi_2 \end{pmatrix}$ and conjugation by P does not change upper-left and lower-right entries. Thus taking

$$T_{n+1} = P^{-n}UP^nT_n = \begin{pmatrix} 1 & u\pi^n \\ 0 & 1 \end{pmatrix} T_n,$$

we complete the induction and the formula shows that $\{T_n\}_{n\geq 1}$ is convergent. ■

Remark 1.16.1. Since $\overline{\rho}_0$ is not diagonalizable, Maschke Theorem (see [CR06] pag. 40) implies that the characteristic of $\mathbb{F}_q$ must divide the order of $\overline{\rho}_0(G)$. This is the arithmetic information that we shall use in the proof Theorem A.

1.4.3 Galois representations induced by a modular form

Let $k > 2$ be a fixed even integer. Let $f \in \mathcal{S}_k$ be a normalized eigenform. Consider a prime $\mathfrak{p}$ of K_f above a rational prime p. We denote $K_{f,\mathfrak{p}}$, the completion of K_f at the place $\mathfrak{p}$, $\mathcal{O}_{f,\mathfrak{p}}$ its ring of integers and $\mathfrak{m} = \mathfrak{p}\mathcal{O}_{f,\mathfrak{p}}$ the maximal ideal. By Proposition 1.9 we see that that $K_{f,\mathfrak{p}}$ is a finite extension of $\mathbb{Q}_p$. Let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$ and write $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. A representation of $G_{\mathbb{Q}}$ is called a Galois representation.
The following Theorem, due to Deligne, associates to a normalized eigenform a Galois representation over $K_{f,\mathfrak{p}}$. This will be the analogous to Eichler–Shimura construction used by Ribet.

Theorem 1.17 ([DS05], Thm. 9.6.5)**.** *Let $f = \sum_{n\geq 1} a_n(f)q^n \in S_k$ be a normalized cuspidal eigenform with Hecke field K_f. Let p be a prime. For each prime ideal $\mathfrak{p}$ of K_f lying over p, there is an irreducible group representation of dimension 2 over $K_{f,\mathfrak{p}}$*

$$\rho_{f,\mathfrak{p}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(K_{f,\mathfrak{p}}).$$

This representation is unramified at all primes $\ell \nmid p$. If $\mathrm{Frob}_\ell \in G_{\mathbb{Q}}$ is an absolute Frobenius at the prime ℓ, then the characteristic polynomial of $\rho(\mathrm{Frob}_\ell)$ depends only on ℓ and it is

$$x^2 - a_\ell(f)x + \ell^{k-1}.$$

1.4.4 $\mathfrak{p}$-ordinary modular forms

Definition 1.18. Let $f = \sum_{n\geq 1} a_n(f)q^n$ be a normalized eigenform. Let $\mathfrak{p}$ be a prime of K_f above a rational prime p. We say that f is $\mathfrak{p}$-ordinary if $a_p(f) \not\equiv 0 \mod \mathfrak{p}$.

To finalize this chapter, we quote a result due to Mazur and Wiles, which will be used during the passage from cuspidal forms to Galois representations (see part (iv) of Theorem 2.4). We denote by D_p an absolute decomposition group at the prime p.

Theorem 1.19 ([Wil88] Thm. 2)**.** *If f is $\mathfrak{p}$-ordinary, then the representation $\rho_{f,\mathfrak{p}}|_{D_p}$ of D_p is equivalent to a representation $\rho_{(0)} : D_p \to \mathrm{GL}_2(K_{f,\mathfrak{p}})$ of the form*

$$\rho_{(0)} = \begin{pmatrix} \varepsilon_1 & \nu \\ 0 & \varepsilon_2 \end{pmatrix},$$

where ε_2 is unramified and $\varepsilon_2(\mathrm{Frob}_p) = \alpha_{\mathfrak{p}}$ where $\alpha_{\mathfrak{p}}$ is the unit root of the polynomial $x^2 - a_p(f)x - p^{k-1}$.

Remark 1.19.1. We may assume that $\rho_{(0)}(g) \in \mathcal{O}_{f,\mathfrak{p}}$ for every $g \in D_p$. Indeed, the characters $\varepsilon_1(g), \varepsilon_2(g)$ are both integral since those are the roots of $\mathrm{char}\, \rho_f(g)$ which by Proposition 1.13 has integral coefficients. By the compactness of D_p, we have that $\nu(D_p) \subset \mathfrak{m}^r\mathcal{O}$ for some $r \in \mathbb{Z}$. Thus, after conjugating several times by a matrix P as in the proof of Ribet lemma, we obtain an equivalent representation with the same form and integral upper-right entry.

Chapter 2

Proof of Ribet's Theorem in weight k

Let p be an irregular prime and choose $2 \leq k \leq p-3$ even such that $p|B_k$. In this chapter we focus on proving Theorem A. We divide the proof in four sections following the mind scheme mentioned in the Introduction.

2.1 From Bernoulli numbers to Cusp forms

Let $A = \mathbb{Z}_{(p)}$ be the localization of $\mathbb{Z}$ at p and $\mathfrak{m}_A = \mathbb{Z}_{(p)}$ its maximal ideal. Let

$$f = \sum_{n \geq 0} a_n(f) q^n, \quad g = \sum_{n \geq 0} a_n(g) q^n,$$

be two modular forms in $(\mathcal{M}_k)_A$. Following the notation of Section 1.2, we see that

$$f_{A/\mathfrak{m}_A} = g_{A/\mathfrak{m}_A} \iff a_n(f) \equiv a_n(g) \mod \mathfrak{m}_A \quad \forall n \geq 0.$$

We shall write $f \equiv g \mod \mathfrak{m}_A$ in this case.

Lemma 2.1. If $p|B_k$, then there exists a cuspidal form $f \in (\mathcal{S}_k)_A$ such that

$$f \equiv E_k \mod \mathfrak{m}_A.$$

Proof. Write E_k in the basis $\mathcal{B} = \{f_0, f_1, \ldots, f_n\}$ of Proposition 1.3

$$E_k = \alpha_0 f_0 + \alpha_1 f_1 + \ldots + \alpha_n f_n.$$

Since $E_k \in (\mathcal{M}_k)_A$ and $(\mathcal{M}_k)_A$ is generated as A-module by $\mathcal{B}$, we deduce that $\alpha_i \in A$. Define

$$f = E_k - \alpha_0 f_0 = \alpha_1 f_1 + \ldots + \alpha_n f_n \in (S_k)_A.$$

By evaluating the linear operator ψ_0, we obtain that

$$-\frac{B_k}{2k} + \alpha_0 = 0,$$

and so $\alpha_0 \in \mathfrak{m}_A$ because $p|B_k$. Therefore

$$f = E_k - \alpha_0 f_0 \equiv E_k \mod \mathfrak{m}_A.$$

■

Proposition 2.2. *If $p|B_k$, then there exists a normalized cuspidal eigenform $f = \sum_{n\geq 1} a_n(f)q^n \in (\mathcal{S}_k)_{(\mathcal{O}_{K_f})_\mathfrak{p}}$ such that for each prime ℓ, we have*

$$a_\ell(f) \equiv 1 + \ell^{k-1} \mod \mathfrak{p}(\mathcal{O}_{K_f})_\mathfrak{p},$$

where $\mathfrak{p}$ is a prime of the Hecke field K_f above p, and $(\mathcal{O}_{K_f})_\mathfrak{p}$ is the localization of the ring of integers of K_f at $\mathfrak{p}$.

Proof. Write $M = (S_k)_A$ and let $f \in M$ be a cuspidal form as in Lemma 2.1. Since E_k is an eigenvector for the Hecke operator T_n with eigenvalue $\sigma(n)$, then $f_{A/\mathfrak{m}_A} \in M_{A/\mathfrak{m}_A}$ is an eigenvector for $(T_n)_{A/\mathfrak{m}_A}$ with eigenvalue $\sigma(n) + \mathfrak{m}_A$. Since M is free of finite rank and the Hecke operators commute, we may apply the Deligne-Serre lemma to obtain a discrete valuation ring B extending A with field of fraction L finite over $\mathbb{Q}$, and an eigenform $f' \in M_B = (S_k)_B$ such that its eigenvalue λ_{T_n} for the operator T_n satisfies

$$\lambda_{T_n} \equiv \sigma_{k-1}(n) \mod \mathfrak{m}_B.$$

If we normalise the cusp form $f' = q + \sum_{n\geq 2} a_n(f')q^n$, then by Proposition 1.7 we obtain that

$$a_n(f') \equiv \sigma_{k-1}(n) \mod \mathfrak{m}_B, \qquad \forall n.$$

Thus the Proposition follows by changing the field L by $K_{f'}$ and noticing that B must be the localization of its ring of integer $\mathcal{O}_{K_{f'}}$ at some prime $\mathfrak{p}$ above p. ■

2.2 From cusp forms to Galois representations

Let f be a cuspidal eigenform as in Proposition 2.2. Using the prime $\mathfrak{p}$ above p, we obtain an irreducible Galois representation $\rho_{f,\mathfrak{p}} : G_\mathbb{Q} \to \mathrm{GL}_2(K_{f,\mathfrak{p}})$. Let $\mathcal{O}_{K,\mathfrak{p}}$ be its ring of integers, $\mathfrak{m}$ the maximal ideal and $\mathbb{F}_q$ the residual field. Let $\zeta \in \overline{\mathbb{Q}}$ be a primitive pth-root of unity. We write $\chi : G_\mathbb{Q} \to \mathbb{F}_p^*$ for the Galois character satisfying

$$\sigma(\zeta) = \zeta^{\chi(\sigma)}, \qquad \forall \sigma \in G_\mathbb{Q}.$$

Proposition 2.3. *The representation $\rho_{f,\mathfrak{p}}$ is equivalent to a representation $\rho : G_\mathbb{Q} \to \mathrm{GL}_2(\mathcal{O}_{K,\mathfrak{p}})$ with reduction $\overline{\rho}$ of the form*

$$\begin{pmatrix} 1 & \gamma \\ 0 & \chi^{k-1} \end{pmatrix},$$

which is not diagonalizable.

Proof. By Ribet's lemma (Proposition 1.16), it is enough to show that $\rho_{f,\mathfrak{p}}$ has an equivalent representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O}_{K,\mathfrak{p}}) \subset \mathrm{GL}_2(K_{f,\mathfrak{p}})$ such that its reduction $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_q)$ has semi-simplification $1 \oplus \chi^{k-1}$.
Let $\ell \neq p$ be a prime and Frob_ℓ an absolute Frobenius element at the prime ℓ. The semi-simple representation $1 \oplus \chi^{k-1}$ has characteristic polynomial at Frob_ℓ equal to

$$x^2 - (1 + \chi^{k-1}(\mathrm{Frob}_\ell))x + \chi^{k-1}(\mathrm{Frob}_\ell) = x^2 - (1 + \ell^{k-1})x + \ell^{k-1}.$$

Now let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O}_{K,\mathfrak{p}}) \subset \mathrm{GL}_2(K_{f,\mathfrak{p}})$ be an equivalent representation to $\rho_{f,\mathfrak{p}}$. By Theorem 1.17 and Proposition 2.2, its reduction $\overline{\rho}$ has characteristic polynomial at Frob_ℓ equal to

$$x^2 - a_\ell(f)x + \ell^{k-1} \equiv x^2 - (1 + \ell^{k-1})x + \ell^{k-1} \mod \mathfrak{m},$$

By the Ceboratev Density Theorem, we conclude that the representation $1 \oplus \chi^{k-1}$ and $\overline{\rho}_{f,\mathfrak{p}}$ have equal characteristic polynomials. Then the Proposition follows from Brauer-Nesbitt Theorem 1.14. ∎

Remark 2.3.1. Note that we may have proved the existence of similar equivalent representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O}_{K,\mathfrak{p}})$ with non diagonalizable reduction $\overline{\rho}$ but of the form

$$\begin{pmatrix} \chi^{k-1} & \gamma \\ 0 & 1 \end{pmatrix}.$$

A reason of this choice is to prove that $\overline{\rho}|_{D_p}$ is diagonalizable using Theorem 1.19 (see the proof of part (iv) of Theorem 2.4). If we use this form instead, there is not guarantee that this crucial property is satisfied.

Theorem 2.4. *Suppose $p \mid B_k$. Then there exists a finite extension $\mathbb{F}_q/\mathbb{F}_p$ and a representation*

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

with the properties:

(i) $\overline{\rho}$ is unramified at all primes $\ell \neq p$.

(ii) The representation $\overline{\rho}$ is equivalent (over $\mathbb{F}_q$) to a representation of the form

$$\begin{pmatrix} 1 & \gamma \\ 0 & \chi^{k-1} \end{pmatrix},$$

for some function $\gamma : G_{\mathbb{Q}} \to \mathbb{F}_q$.

(iii) The image of $\overline{\rho}$ has order divisible by p.

(iv) Let D_p be a decomposition group for p in $G_{\mathbb{Q}}$. Then $\overline{\rho}|D_p$ is diagonalizable and $\overline{\rho}(D_p)$ has order co-prime to p.

Proof. Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O}_{K,\mathfrak{p}})$ be the representation of Proposition 2.3. Let us see that its associated reduction

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

satisfies the Theorem. Since $\overline{\rho}$ is the resulting composition

$$G_{\mathbb{Q}} \xrightarrow{\ \rho\ } \mathrm{GL}_2(\mathcal{O}_{f,\mathfrak{p}}) \xrightarrow{\ (\cdot)+\mathfrak{m}\ } \mathrm{GL}_2(\mathbb{F}_q),$$

by Theorem 1.17 we see that $\overline{\rho}$ is unramified at all primes $\ell \neq p$. This proves (i). Properties (ii) and (iii) are satisfied by construction (see also Remark 1.16.1). Thus it only remains to prove (iv). Since

$$a_p(f) \equiv 1 + p^{k-1} \equiv 1 \not\equiv 0 \mod \mathfrak{m},$$

the modular form f is $\mathfrak{p}$-ordinary and so by Theorem 1.19, $\rho|_{D_p}$ is equivalent to a representation $\rho_{(0)}$ of the form

$$\rho_{(0)} = \begin{pmatrix} \varepsilon_1 & \nu \\ 0 & \varepsilon_2 \end{pmatrix}, \tag{2.1}$$

with ε_2 unramified. Since $\rho|_{D_p}$ and $\rho_{(0)}$ are equivalent, Proposition 1.15 tell us that their reduction have the same semi-simplification.[1] Furthermore, if we denote ω_1, ω_2 the reduction of $\varepsilon_1, \varepsilon_2$ respectively, the semi-simplification of $\rho_{(0)}$ is $\omega_1 \oplus \omega_2$, and since ω_2 its unramified, we have that

$$\omega_1 = \chi^{k-1}, \qquad \omega_2 = 1.$$

Now write $\rho = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$. Then

$$A + \mathfrak{m} = 1, \qquad B + \mathfrak{m} = \gamma, \qquad D + \mathfrak{m} = \chi^{k-1}.$$

Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(K)$ be a matrix such that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \varepsilon_1 & \nu \\ 0 & \varepsilon_2 \end{pmatrix} = \begin{pmatrix} A|_{D_p} & B|_{D_p} \\ C|_{D_p} & D|_{D_p} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{2.2}$$

Note that if we change M by $\pi^r M$ with π a prime element and $r \in \mathbb{Z}$, the equality still holds and so we may assume that $a, c \in \mathcal{O}_{f,\mathfrak{p}}$ and either a or c is a unit.
By looking at the upper-left entry in the equation (2.2) , we see that

$$a(\varepsilon_1 - A|_{D_p}) = cB|_{D_p}. \tag{2.3}$$

If $\pi | c$, then $\pi | (\varepsilon_1 - A|_{D_p})$ since $a \in \mathcal{O}^*_{f,\mathfrak{p}}$. But on the other hand

$$\varepsilon_1 + \mathfrak{m} = \omega_1 = \chi^{k-1} \neq 1 = A|_{D_p} + \mathfrak{m}.$$

[1] Here we use that $\rho_{(0)}$ has integer matrix coefficients (see Remark 1.19.1).

Therefore $\pi \nmid c$ and so c is a unit. Thus, if we denote $s = -a/c + \mathfrak{m} \in \mathbb{F}_q$, then by reducing the equation (2.3), we have that

$$\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} \overline{\rho} \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1|_{D_p} & \gamma + s(\chi^{k-1}|_{D_p} - 1|_{D_p}) \\ 0 & \chi^{k-1}|_{D_p} \end{pmatrix} = \begin{pmatrix} 1|_{D_p} & 0 \\ 0 & \chi^{k-1}|_{D_p} \end{pmatrix}.$$

This proves the first claim in (iv). For the second claim, note that using the diagonal form of $\overline{\rho}$, we may see the group $\overline{\rho}(D_p)$ as a subgroup of $\mathbb{F}_p^*$. Since $|\mathbb{F}_p^*| = p - 1$, this shows that $\overline{\rho}(D_p)$ has order co-prime to p. ■

2.3 From Galois representation to extension E/K

Theorem 2.5. *Suppose that $p \mid B_k$. Then there exists a Galois extension $E/\mathbb{Q}$ containing K with the following properties.*

(a) The extension E/K is everywhere unramified.

(b) The group $H = \mathrm{Gal}(E/K)$ is a finite non-zero p-elementary abelian group i.e. $\mathbb{F}_p$-vector space of positive dimension.

(c) The natural action of $\Delta = \mathrm{Gal}(K/\mathbb{Q})$ on H satisfies the relation

$$\sigma \cdot \tau = \tau^{\chi(\sigma)^{1-k}}, \qquad \sigma \in \Delta, \tau \in H.$$

Proof. Let $\overline{\rho}$ a representation as in Theorem 2.4. We may assume that

$$\overline{\rho}(g) = \begin{pmatrix} 1 & \gamma(g) \\ 0 & \chi^{k-1}(g) \end{pmatrix}, \qquad \forall g \in G_{\mathbb{Q}}.$$

We denote K' and E' the fixed field of $\mathrm{Ker}(\chi^{k-1})$ and $\mathrm{Ker}(\overline{\rho})$ respectively. We first prove the Theorem for the fields K' and E' instead of K and E.
By Galois correspondence, we have

$$G' = \mathrm{Gal}(E'/\mathbb{Q}) \simeq G_{\mathbb{Q}}/\mathrm{Ker}(\overline{\rho}) \simeq \mathrm{Im}(\overline{\rho}),$$
$$\Delta' = \mathrm{Gal}(K'/\mathbb{Q}) \simeq G_{\mathbb{Q}}/\mathrm{Ker}(\chi^{1-k}) \simeq \mathrm{Im}(\chi^{1-k}).$$

Write $H' = \mathrm{Gal}(E'/K') \trianglelefteq G$. Then

$$G'/H' \simeq \Delta'. \tag{2.4}$$

By the matrix identity

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix},$$

we see that γ induces an injective morphism from H' into the additive group $\mathbb{F}_q$. In particularly H' is a finite p-elementary abelian group. On the other hand we have $p \nmid |\Delta'|$ since $\Delta' \simeq \mathrm{Im}(\chi^{1-k}) \leqslant \mathbb{F}_q^*$. Using equation (2.4) and part (iii) of

Theorem 2.4 we obtain that p divides $|H'|$ and so it is not trivial. This proves (b) for the extension E'/K'.
By part (i) of Theorem 2.4, the extension $E'/\mathbb{Q}$ is unramified at all primes $\ell \neq p$. So E'/K' is unramified for all primes $\mathfrak{p}$ of K' such that $\mathfrak{p} \cap \mathbb{Q} \neq p$. Now let $\mathfrak{B}/\mathfrak{p}/p$ be primes in the extension $E'/K'/\mathbb{Q}$. The image of the decomposition D_p under $\overline{\rho}$ is equal (up to conjugation) to the decomposition group $D(\mathfrak{B}, p)$ and by part (iv) of Theorem 2.4, its order is coprime to p. Since

$$D(\mathfrak{B}, \mathfrak{p}) = D(\mathfrak{B}, p) \cap H',$$

and H' is a p-group, we conclude that $D(\mathfrak{B}, \mathfrak{p})$ is trivial. In particularly its inertia group $I(\mathfrak{B}, \mathfrak{p})$ is trivial and p is unramified. This proves (a) for the extension E'/K'. (Note that E'/K' is unramified at the infinite primes since the extension is odd).
Now take elements $\sigma \in G'$, $\tau \in H'$, and $g, h \in G_{\mathbb{Q}}$ such that $g|_{E'} = \sigma$ and $h|_{K'} = \tau$. Using the identity

$$\begin{pmatrix} 1 & \gamma(g) \\ 0 & \chi(g)^{k-1} \end{pmatrix} \begin{pmatrix} 1 & \gamma(h) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \gamma(g) \\ 0 & \chi(g)^{k-1} \end{pmatrix}^{-1} = \begin{pmatrix} 1 & \gamma(h) \\ 0 & 1 \end{pmatrix}^{\chi(g)^{1-k}},$$

and the isomorphism described for G' and H' above, we obtain that $\sigma\tau\sigma^{-1} = \tau^{\chi(g)^{1-k}}$. This proves (c) for the extension E'/K'.
Now, we define $E = E'K$, $G = \mathrm{Gal}(E/\mathbb{Q})$ and $H = \mathrm{Gal}(E/K)$. The restriction map $H \to H'$ is injective and has image $\mathrm{Gal}(E'/K \cap E')$. Thus H is an abelian p-group. If H were trivial, then $E' \subset K$ and

$$G' \simeq \Delta/\mathrm{Gal}(K/E'),$$

but this is impossible since $p||G'|$ and $p \nmid |\Delta|$. This proves (b).
Since the restriction morphism sends inertia elements to inertia elements and $E'/(E' \cap K')$ is unramified, we have that E/K is unramified. This proves (a).
For (c), we note the restriction map $H \to H'$ is a Δ-morphism. Therefore $H = H(\chi^{1-k})$ because it is injective. This concludes the proof. ∎

2.4 From Extensions E/K to the class group of K

Theorem A. *If $p|B_k$ for some $2 \leq k \leq p-3$ even, then $C(\chi^{1-k}) \neq 0$.*

Proof. By Proposition 1.12, the Artin map $\psi_{L/K} : A_K \to H$ is a surjective Δ-morphism. Since H is annihilated by p, this morphism factorizes through C_K and so one obtains a surjective Δ-morphism $\psi_{L/K} : C_K \to H$. Let

$$H = \bigoplus_{i \mod p-1} H(\chi^i), \qquad H(\chi^i) = \{\tau \in H : \sigma \cdot \tau = \tau^{\chi(\sigma)^i} \quad \forall \sigma \in \Delta\},$$

the decomposition of H as χ^i-eigenspaces. By parts (b) and (c) of Theorem 2.5, we have

$$H(\chi^{1-k}) = H \neq 1.$$

Since $\varphi_{L/K}$ is surjective, then

$$\psi_{L/K}(C(\chi^{1-k})) = H(\chi^{1-k}) = H \neq 0,$$

and so $C(\chi^{1-k}) \neq 0$.

■

Chapter 3

Class field Theory encoded by the representation $\overline{\rho}$

Let p be an irregular prime and choose $2 \leq k \leq p-3$ even with $p|B_k$. Let E be the unramified abelian extension of K constructed in the proof of Theorem 2.5. In this Chapter we use the representation $\overline{\rho}$ of Theorem 2.4 to prove Theorem B and Theorem C mentioned in the Introduction. We finish the Chapter by describing the field E as the unique extension of K satisfying certain explicit properties (see Proposition 3.4 and Proposition 3.5). Thus obtaining a general statement for each Theorem.

3.1 Class field Theory of the extension E/K

Before proving Theorem B and Theorem C, we recall some previous notation. Let E' and K' be the field fixed by $\operatorname{Ker}\overline{\rho}$ and χ^{k-1} respectively. By the proof of Theorem 2.5 we have that $E = E'K$. For a prime $\mathfrak{B}$ of E above a prime $\mathfrak{q}$ of K, we write

$$\mathfrak{B}' = E' \cap \mathfrak{B}, \qquad \mathfrak{q}' = K' \cap \mathfrak{B}.$$

If $\psi_{E/K}(\mathfrak{B}/\mathfrak{q})$ and $\psi_{E'/\mathbb{Q}}(\mathfrak{B}'/q)$ denote the Frobenius element of $\mathfrak{B}$ over $\mathfrak{q}$ and $\mathfrak{B}'$ over q respectively, then

$$\psi_{E/K}(\mathfrak{B}/\mathfrak{q})|_{E'} = \psi_{E'/\mathbb{Q}}(\mathfrak{B}'/q)^{f(\mathfrak{q}/q)} \in \operatorname{Gal}(E'/K').$$

Note that since $E = E'K$, we have that

$$\psi_{E/K}(\mathfrak{B}/\mathfrak{q}) = 1 \iff \psi_{E/K}(\mathfrak{B}/\mathfrak{q})|_{E'} = 1.$$

Thus the prime $\mathfrak{q}$ splits completely if and only if $\psi_{E'/\mathbb{Q}}(\mathfrak{B}'/q)^{f(\mathfrak{q}/q)} = 1$.
We also use the following result.

Proposition 3.1 ([Was97], Thm 2.17)**.** *Let $f(\mathfrak{q}/q)$ be the residual degree of $\mathfrak{q}$ over q. Then $f(\mathfrak{q}/q)$ is the minimal integer f such that $q^f \equiv 1 \mod p$.*

Now we are ready to prove the Theorem B and Theorem C.

Theorem B. Assume that $p|B_k$. Let $\mathfrak{q}$ be a prime of K above a rational prime $q \neq p$. If $q^{k-1} \not\equiv 1 \mod p$, then $\mathfrak{q}$ splits completely in the extension E.

Proof. Since E' is the field fixed by $\operatorname{Ker}\overline{\rho}$, we have the following commutative diagram

$$\begin{array}{ccc} \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & \twoheadrightarrow & \mathrm{Gal}(L/\mathbb{Q}) \\ & \searrow^{\rho} & \downarrow \wr \\ & & \rho(\mathrm{Gal}_{\mathbb{Q}}) \end{array}$$

Let Frob_q be an absolute Frobenius element at the prime q. Then (up to conjugation) we have that $\psi_{E'/\mathbb{Q}}(\mathfrak{B}'/q) = \mathrm{Frob}_q\,|_{E'}$, and so

$$\psi_{E'/\mathbb{Q}}(\mathfrak{B}'/q)^{f(\mathfrak{q}/q)} = 1 \iff \mathrm{Frob}_q^{f(\mathfrak{q}/q)} \in \operatorname{Ker}\overline{\rho}.$$

We compute

$$\overline{\rho}(\mathrm{Frob}_q^{f(\mathfrak{q}/q)}) = \begin{pmatrix} 1 & \gamma(\mathrm{Frob}_q) \\ 0 & q^{k-1} \end{pmatrix}^{f(\mathfrak{q}/q)} = \begin{pmatrix} 1 & \gamma(\mathrm{Frob}_q)\sum_{i=0}^{f(\mathfrak{q}/q)-1}(q^{k-1})^i \\ 0 & 1 \end{pmatrix}.$$

By Proposition 3.1, $q^{f(\mathfrak{q}/q)} \equiv 1 \mod p$. Thus

$$\sum_{i=0}^{f(\mathfrak{q}/q)-1}(q^{k-1})^i \equiv \begin{cases} 0 \mod p & \text{if } q^{k-1} \not\equiv 1 \mod p \\ f(\mathfrak{q}/q) \mod p & \text{if } q^{k-1} \equiv 1 \mod p \end{cases}.$$

Then the Theorem follows from the first case. Note that $f(\mathfrak{q}/q)|p-1$, so $f(\mathfrak{q}/q) \not\equiv 0 \mod p$. ∎

Theorem C. There exist (infinitely many) primes $\mathfrak{q}$ in K above a prime q satisfying $q^{k-1} \equiv 1 \mod p$ which do not split completely in the extension E/K.

Proof. Let $\sigma \in \mathrm{Gal}(E'/K') \subset \mathrm{Gal}(E'/\mathbb{Q})$ be a non-trivial element. By applying the Chebotarev's density theorem, we found (infinitely many) primes $\mathfrak{B}'$ in the extension E' above a rational prime q such that $\psi_{E'/\mathbb{Q}}(\mathfrak{B}'/q) = \sigma$. Choose a prime $\mathfrak{B}$ of E above $\mathfrak{B}'$ and write $\mathfrak{q} = \mathfrak{B} \cap K$ and $\mathfrak{q}' = \mathfrak{B} \cap K'$. Since σ fixes K', we have

$$\psi_{K'/\mathbb{Q}}(\mathfrak{q}'/q) = \psi_{E'/\mathbb{Q}}(\mathfrak{B}'/q)|_{K'} = 1,$$

or equivalently $q^{k-1} \equiv 1 \mod p$. Also, since $\mathrm{Gal}(E'/K')$ is a p-group and $f(\mathfrak{q}/q)$ divides $p-1$, then

$$\psi_{E/K}(\mathfrak{B}/\mathfrak{q})|_{E'} = \psi_{E'/\mathbb{Q}}(\mathfrak{B}'/q)^{f(\mathfrak{q}/q)} = \sigma^{f(\mathfrak{q}/q)} \neq 1.$$

Therefore $\mathfrak{q}$ does not split completely in the extension E. ∎

Note that in this proof we only used the fact that the extension E/K is induced by a lower unramified abelian extension E'/K' with K' the fixed field of χ^{k-1}. This fact can be proven using only Class field Theory. First we prove a more general result.

Proposition 3.2. *Let $F/\mathbb{Q}$ be a finite Galois extension and L/F an unramified abelian extension such that the natural action of $\mathrm{Gal}(F/\mathbb{Q})$ on $\mathrm{Gal}(L/F)$ factorizes through a quotient $\mathrm{Gal}(F'/\mathbb{Q})$. Assume that $([F : F'], |\mathrm{Gal}(L/F)|) = 1$. Then there exists an unramified abelian extension E'/K' such that $E = E'K$ and the restriction map $\mathrm{Gal}(L/F) \to \mathrm{Gal}(L'/F')$ is a $\mathrm{Gal}(F'/\mathbb{Q})$-isomorphism.*

Proof. Let $\mathfrak{p}'$ be a prime of F' and $\mathfrak{p}$ any prime of F above $\mathfrak{p}'$. We define

$$\varphi(\mathfrak{p}') = \psi_{L/F}(\mathfrak{p})^{\frac{[F:F']}{f(\mathfrak{p}/\mathfrak{p}')}}.$$

Note that the element $\frac{[F:F']}{f(\mathfrak{p}/\mathfrak{p}')}$ is always an integer since the extension F/F' is Galois. Since the action of $\mathrm{Gal}(F/\mathbb{Q})$ on $\mathrm{Gal}(L/F)$ factorizes through $\mathrm{Gal}(F'/\mathbb{Q})$, Lemma 1.11 implies

$$\psi_{L/F}(\sigma(\mathfrak{p})) = \psi_{L/F}(\mathfrak{p}), \qquad \forall \sigma \in \mathrm{Gal}(F/F'). \tag{3.1}$$

Thus $\varphi(\mathfrak{p}')$ does not depend on the chosen prime. We extend φ multiplicatively to a morphism $\varphi : I_{F'} \to \mathrm{Gal}(L/F)$ defined on the group of fractional ideals of F'. We claim that φ is surjective and its kernel contains the group of principal ideals.
Since $(|\mathrm{Gal}(L/F)|, [F : F']) = 1$ we have

$$\langle \psi_{L/F}(\mathfrak{p}) \rangle = \langle \psi_{L/F}(\mathfrak{p})^{\frac{[F:F']}{f(\mathfrak{p}/\mathfrak{p}')}} \rangle = \langle \varphi(\mathfrak{p}') \rangle. \tag{3.2}$$

Therefore φ is surjective because so is the Artin morphism. Now let $\alpha \in F'$. Write

$$(\alpha) = \prod_i (\mathfrak{p}_i')^{\mathrm{ord}_{\mathfrak{p}_i'}(\alpha)}$$

as product of primes of F'. By definition we have

$$\varphi((\alpha)) = \prod_i \psi_{L/F}(\mathfrak{p}_\mathfrak{i})^{\frac{[F:F']}{f(\mathfrak{p}/\mathfrak{p}')} \cdot \mathrm{ord}_{\mathfrak{p}_i'}(\alpha)}, \qquad \mathfrak{p}_i' = \mathfrak{p}_i \cap F'.$$

On the other hand we have

$$\alpha \mathcal{O}_F = \prod_i \left[(\mathfrak{p}_i') \mathcal{O}_F \right]^{\mathrm{ord}_{\mathfrak{p}_i'}(\alpha)} = \prod_i \left[\prod_{\mathfrak{p}_j^{(i)} | \mathfrak{p}_i'} \psi_{L/F}(\mathfrak{p}_j^{(i)})^{e(\mathfrak{p}_j^{(i)}/\mathfrak{p}_i')} \right]^{\mathrm{ord}_{\mathfrak{p}_i'}(\alpha)},$$

and using (3.1) and Artin reciprocity, we obtain

$$\varphi((\alpha)) = \psi_{L/F}(\alpha \mathcal{O}_F) = 1.$$

This proves the claim. Now the Existence Theorem of Class Field Theory (see [Mil20] pag. 158), implies that there exists an unramified abelian extension L'/F' with Galois group $\mathrm{Gal}(L'/F') \simeq \mathrm{Gal}(L/F)$ and whose primes $\mathfrak{p}'$ which split are

those satisfying $\varphi(\mathfrak{p}') = 1$. Now we prove that $L = L'F$.
Let $\tilde{L} = L'F$. Then $\tilde{L}$ is a unramified extension of F. Let $\mathfrak{p}$ a prime of F and write $\mathfrak{p}' = \mathfrak{p} \cap F'$. By the formula

$$\psi_{\tilde{L}/F}(\mathfrak{p})|_{E'} = \psi_{L'/F'}(\mathfrak{p}')^{f(\mathfrak{p}/\mathfrak{p}')} \in \mathrm{Gal}(L'/F), \tag{3.3}$$

and the fact that $f(\mathfrak{p}/\mathfrak{p}')$ is coprime with $|\mathrm{Gal}(L'/F')|$, we see that $\mathfrak{p}'$ splits in L'/F' if and only if $\mathfrak{p}$ splits in $\tilde{L}/F$. Moreover, by equation (3.2), we have that $\mathfrak{p}'$ splits in in L'/F' if and only if $\mathfrak{p}$ splits in L/F. Therefore $L = \tilde{L} = L'F$ since the set of primes that split determines the extension (see [Mil20], Theorem 3.25 Chaper V).
Finally, the restriction map $\mathrm{Gal}(L/F) \to \mathrm{Gal}(L'/F')$ agrees with the action of $\mathrm{Gal}(F/\mathbb{Q})$, it is clearly injective and it is surjective by equation (3.3) and the fact that the Artin map $\psi_{L'/F'} : I_{F'} \to \mathrm{Gal}(L'/F')$ is surjective. ■

Proposition 3.3. *Let E/K be a p-elementary unramified extension such that $\mathrm{Gal}(E/K) = H = H(\chi^j)$ in his decomposition as χ^i-eigenspaces. Then the fixed field K' by $\operatorname{Ker}\chi^j$ has an unramified abelian extension E'/K' such that $E'K = E$ and the restriction $\mathrm{Gal}(E/K) \to \mathrm{Gal}(E'/K')$ is a χ^j-isomorphism.*

Proof. This follows from the previous Proposition since $[K : \mathbb{Q}] = p-1$ is co-prime with $|H|$. ■

3.2 E as a canonical extension of K

Let $\alpha : A_k \to C(\chi^{k-1})$ be the morphism defined by the commutative diagram

$$\begin{array}{ccc} A_K & \twoheadrightarrow & A_K/A_K^p = C \\ & \searrow^{\alpha} & \downarrow \mathrm{Pr} \\ & & C(\chi^{1-k}) \end{array}$$

Let L be the field fixed by $\operatorname{Ker}\alpha$ and $\mathbb{H}$ the Hilbert Class field of K. Since the restriction map $\mathrm{Gal}(\mathbb{H}/K) \to \mathrm{Gal}(L/K)$ agrees with the action of $\Delta = \mathrm{Gal}(K/\mathbb{Q})$, we obtain a Δ-isomorphism

$$\mathrm{Gal}(L/K) \simeq C(\chi^{1-k}).$$

Proposition 3.4. *The field L is the maximal p-elementary unramified abelian extension of K such that $\mathrm{Gal}(L/K) = H = H(\chi^{1-k})$ in its decomposition as χ^i-eigenspaces.*

Proof. Clearly L is a p-elementary unramified abelian extension of K. It also satisfies the condition about its Galois group by the comment made above.
Let L' be an extension of K satisfying the Proposition. Since $p\,\mathrm{Gal}(L'/K) = 0$,

the restriction map $\varphi : \mathrm{Gal}(\mathbb{H}/K) \to \mathrm{Gal}(L'/K)$ factorizes through π. Moreover, since φ is a Δ-morphism and

$$\mathrm{Gal}(L'/K) = H' = H'(\chi^{1-k}),$$

φ also factorizes through Pr. Therefore $\mathrm{Ker}\,\alpha$ is contained in the kernel of φ and so $L' \subset L$. ■

Now let E be the extension constructed in the proof of Theorem A. We have that following.

Proposition 3.5. *$L = E$.*

Proof. By the previous Proposition we have that $E \subset L$. The fact that $E = L$ is a consequence of Iwasawa main conjecture (see the comment made below in [Eri08] pag. 4) which implies that $C(\chi^{1-k})$ are one dimension $\mathbb{F}_p$-spaces and so L/K has degree p. ■

Bibliography

[CR06] Charles W. Curtis and Irving Reiner. *Representation theory of finite groups and associative algebras*. AMS Chelsea Publishing, Providence, RI, 2006. Reprint of the 1962 original.

[Dal09] Chandan Singh Dalawat. Ribet's modular construction of unramified p-extensions of $\mathbb{Q}(_p)$. 2009. 10.48550/ARXIV.0903.2617.

[DS05] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[Eri08] C. W. Erickson. Ribet's converse to herbrand's theorem. 2008.

[HK04] Kenneth Hoffman and Ray A. Kunze. *Linear Algebra*. PHI Learning, second edition, 2004.

[LW21] Jaclyn Lang and Preston Wake. A modular construction of unramified p-extensions of $\mathbb{Q}(n^{1/p})$, 2021. 10.48550/ARXIV.2109.04308.

[Maz11] Barry Mazur. How can we construct abelian galois extensions of basic number fields? *Bulletin (New Series) of the American Mathematical Society*, 48, 05 2011.

[Mil20] J.S. Milne. Class field theory (v4.03), 2020. Available at www.jmilne.org/math/.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Rib76] Kenneth A. Ribet. A modular construction of unramified p-extension of $\mathbb{Q}(\mu_p)$. *Inventiones mathematicae*, 34:151–162, 1976.

[Ser73] J.-P. Serre. *A course in arithmetic*. Graduate Texts in Mathematics, No. 7. Springer-Verlag, New York-Heidelberg, 1973. Translated from the French.

[Sta22] The Stacks project authors. The stacks project. https://stacks.math.columbia.edu, 2022.

[Was97] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

[Wil88] A. Wiles. On ordinary λ-adic representations associated to modular forms. *Invent. Math.*, 94(3):529–573, 1988.