A Note of the Ribet's Theorem

Li Anlun PB19010484

Abstract

This note is a reading report mainly based on [1] and [2]. And we will state Ribet's Theorem and follow its origin proof. First We will introduce modular curves and modular forms, and construct a Galois representation concerning a specific modular form. After that, we will state two stronger versions of Ribet's theorem and prove the latter one.

Contents

1 Introduction and Background

Let K/$\mathbb{Q}$ be a finite extension, and Cl_K be its ideal class group. In algebraic number theory, we know that Cl_K is a finite abelian group with order h_K, i.e. for any fractional ideal I, there exists n$\in \mathbb{Z}$, s.t. I^n is principal.

When $K = \mathbb{Q}(\mu_p)$, Kummer has found a powerful result relating to Fermat's Problem.

Proposition 1 (Kummer, in 1851)**.** *(cf. [4]) If $p \nmid h_{\mathbb{Q}(\mu_p)}$, i.e. the p-sylow subgroup of $Cl_{\mathbb{Q}(\mu_p)}$ is trivial, then $x^p + y^p = z^p$ has no solution in $\mathbb{Z}^3$.*

Proof. We sketch the proof. We may assume $p > 3$, $p \nmid (x - y)$ and x,y,z are coprime to each other in $\mathbb{Z}$. Let $\mu = \mu_p$, we have

$$x^p + y^p = (x + y)(x + \mu y) \cdots (x + \mu^{p-1} y) = z^p.$$

First we aim to prove that principal ideals $\{(x + \mu^i y)\}$ are coprime to each other in $\mathbb{Z}[\mu]$. Therefore, using the equation above, we conclude that $(x + \mu^i y) = \alpha_i^p$, for some fractional ideal I_i. Since the left hand side is principal, and $p \nmid h_K$, each I_i is principal, i.e. $I_i = (\alpha_i)$ where $\alpha_i \in \mathbb{Z}[\mu]$.

Then we claim that there exists $r \in \mathbb{Z}$, s.t. $x + \mu y - \mu^{2r} x - \mu^{2r-1} y \equiv 0$ (mod p). Through a little discussion, we are done. □

And if $p \nmid h_{\mathbb{Q}(\mu_p)}$ for all prime p, then Fermat's Last Theorem is done. But we have a counterexample indeed. For p=37, $Cl_{\mathbb{Q}(\mu_{37})} \cong \mathbb{Z}/37\mathbb{Z}$, h=37. Thus we may be interested in whether the order of the p-Sylow subgroup of $Cl_{\mathbb{Q}(\mu_p)}$ is divisible by p.

Henceforth, we denote $K = \mathbb{Q}(\mu_p)$, and Δ =Gal$(K/Q) \cong (\mathbb{Z}/p\mathbb{Z})^*$. Then Δ has a natural action on Cl_K, i.e., $\sigma[I] = [\sigma(I)]$. In addition, Cl_K has a $\mathbb{Z}$-module structure, i.e., $n.I = I^n$.

Let $C = Cl_K / Cl_K^p$ be an $\mathbb{F}_p$ -vector space. Then $p | h_K$ iff $C \neq 0$.

There is a decomposition lemma making C clear.

Lemma 1 (Decomposition Lemma)**.** *(cf. [5]) If R is a commutative ring containing $\{\langle \mu_n \rangle\}$ and $\frac{1}{n}$. G is an abelian group with order n, and $\widehat{G} = Hom(G, R^\times)$ be all group morphisms. Then for $R[G]$ -module M, we have*

$$M = \bigoplus_{\chi \in \widehat{G}} M(\chi),$$

where $M(\chi) = \{m \in M : \sigma m = \chi(\sigma) m$ for every $\sigma \in G\}$, χ is a Dirichlet character modulo n.

Proof. let $e_\chi = \frac{1}{n}\sum_{\sigma\in G}\chi(\sigma)\sigma^{-1}$, then we can see

$$\sum_{\chi\in\widehat{G}} e_\chi = 1, e_\chi e_{\chi'} = 0, e_\chi e_\chi = e_\chi.$$

Thus, for all $m \in M$, m can be uniquely written as $\sum_\chi e_\chi m$. □

View C as $\mathbb{F}_p[\Delta]$ -module, let $\chi : \Delta \cong (\mathbb{Z}/p\mathbb{Z})^* = \mathbb{F}_p^*$. Note that $\{\chi^i : 1 \leq i \leq p-1\} = Hom(\Delta, \mathbb{F}_p^*)$, we have:

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

and every $C(\chi^i)$ is an $\mathbb{F}_p[\Delta]$ -vector space, where $\sigma x = \chi^i(\sigma)x$ for $x \in C(\chi^i)$ and $\sigma \in \Delta$.

Let $\frac{t}{e^t-1} = \sum_{n=0}^{\infty} B_k \frac{t^n}{n!}$, where B_n are called Bernoulli numbers. In 1932, Herbrand found the following theorem.

Theorem 1 (Herbrand)**.** *(cf. [6]) Let $k \in [2, p-3]$ be an even integer. If $C(\chi^{1-k}) \neq 0$, then $p|B_k$.*

The proof is in [5]. What we concern is Ribet's result in 1970s:

Theorem 2 (Ribet)**.** *(cf. [1]) Let $k \in [2, p-3]$ be an even integer. If $p|B_k$, then $C(\chi^{1-k}) \neq 0$.*

This note will be organized as follows. In the following two chapters, we will state and prove several basic definitions and facts in Modular Curves and Modular Forms. And in the fourth chapter, we will follow Ribet's origin proof, which first claims two stronger propositions and proves the latter one.

2 Modular Curves and Modular Forms

In this section, we will introduce modular curves, modular forms and use the algebraic structure of modular curves to construct a Galois representation.

2.1 Basic Definitions and Facts

2.1.1 Modular Curves and Modular Forms

First, let us explain the motivation. We want to construct a kind of Riemann Surface. Since simply-connected Riemann Surfaces have been classifed, i.e. they are $\mathbb{C}, \mathcal{H}$, and $\mathbb{CP}^1$, let's consider a group action on $\mathcal{H}$ and its induced quoient space, i.e. $\mathcal{H}/G$. To make it be a Riemann Surface, we consider $G \leq SL_2(\mathbb{Z})$.

Definition 1 (Congruence Group)**.** $\Gamma \leq SL_2(\mathbb{Z})$ *is called a congruence group if there exists N, s.t.* $\Gamma(N) \subset \Gamma$, *where* $\Gamma(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} (mod\ N)\}$.

In general,

$$\begin{aligned} \Gamma(N) &= \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} (mod\ N)\} \\ \triangle & \\ \Gamma_1(N) &= \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} (mod\ N)\} \\ \triangle & \\ \Gamma_0(N) &= \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} (mod\ N)\}. \end{aligned}$$

Definition 2 (Modular Curves)**.** $Y(\Gamma) := \mathcal{H}/\Gamma = \{\Gamma\tau : \tau \in \mathcal{H}\}$, *is the set of orbits.* $X(\Gamma) := \mathcal{H}^*/\Gamma$, *where* $\mathcal{H}^* = \mathcal{H} \cup P^1(\mathbb{Q})$.

Fact: $X(\Gamma)$ is a compact Riemann Surface. This requires careful discussion on its neighborhoods, elliptic points(we call $\Gamma\tau \in X(\Gamma)$ is an elliptic point(here $\tau \in \mathcal{H}$), if there exists non-trivial $\gamma \in \Gamma$, s.t. $\gamma\tau = \tau$) and cusps(the points equivalent to $P^1(\mathbb{Q})$).

Example 1. $X(SL_2(\mathbb{Z})) \cong S^2$. *(See the figure 1 below.)*

Note that the fundamental domain for $SL_2(\mathbb{Z})$ *is D below, and the cusp of* $X(SL_2(\mathbb{Z}))$ *is* ∞, *we think this point lying in the infinitely far up the imaginary axis. Thus we imagine two lines* $x = 1/2$ *and* $x = -1/2$ *intersect at the* ∞, *since these two lines and two arcs on the boundary are identified respectively, we get a Riemann sphere.*

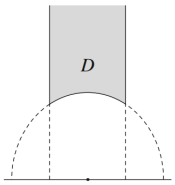


Figure 1: the fundamental domain for $SL_2(\mathbb{Z})$(This picture comes from [2])

Now we introduce modular forms, and its motivation is to analogize meromorphic forms. We will see later that Theorem 4 will tell us the relation.

Definition 3 (Modular Forms of weight k with respect to Γ)**.** *$f : \mathcal{H} \to \mathbb{C}$ is called modular forms of weight k with respect to Γ (i.e. $f \in M_k(\Gamma)$) if:*

- *f is holomorphic in $\mathcal{H}$,*
- *$f(\tau) = (c\tau + d)^{-k} f(\gamma(\tau)) =: (f[\gamma]_k)(\tau)$, for any $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$,*
- *$f[\alpha]_k$ is **holomorphic at** ∞ for any $\alpha \in SL_2(\mathbb{Z})$.*

Let me explain the meaning of "holomorphic at ∞". We know that since Γ is a congruence subgroup, so there exists N, $\Gamma(N) \subset \Gamma$, which implies that $\gamma = \begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} \in \Gamma$. Using property(2) above, $f[\gamma]_k = f$, we have $f(z + N) = f(z)$, so there is a natural fourier expansion, i.e.

$$f(z) = \sum_{n \in \mathbb{Z}} a_n e^{\frac{2\pi i n z}{N}} = \sum_{n \in \mathbb{Z}} a_n q_N^n.$$

Let's consider another function $g(q)$, which has a Laurent expansion $g(q) = \sum_n a_n q^n$. Thinking of ∞ as lying far in the imaginary direction, then $z \to \infty$ iff $q \to 0$. We say a function is **holomorphic at** ∞ iff $a_n = 0$ for all n<0.

Since $f[\alpha]_k$ is invariant under $\alpha^{-1}\Gamma\alpha$, which contains $\alpha^{-1}\Gamma(N)\alpha = \Gamma(N)$, therefore, (3) is well-defined.

Moreover, if $a_0 = 0$ in $f[\alpha]_k$'s fourier expansion for all $\alpha \in SL_2(\mathbb{Z})$, then f is called a **cusp form** of weight k respect to Γ, i.e. $f \in S_k(\Gamma)$.

If we replace **"holomorphic"** by **"meromorphic"**, then the set is $A_k(\Gamma)$, called **Automorphic form**.

Note that these function are NOT well-defined on $X(\Gamma)$.

Proposition 2 (Decomposition of $M_k(\Gamma_1(N))$)**.**

$$M_k(\Gamma_1(N)) = \bigoplus_{\chi} M_k(N, \chi),$$

where $M_k(N, \chi) = \{f : f[\gamma]_k = \chi(d_\gamma) f \text{ for all } \gamma \in \Gamma_0(N)\}$*, and* χ *is a Dirichlet character modulo N.*

Proof. Note that $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^*$. And f is invariant under $\Gamma_1(N)$, thus the action of $\Gamma_0(N)$ can be realized as $(\mathbb{Z}/N\mathbb{Z})^*$. □

In the theory of Compact Riemann Surface, there are two natural objects.

Definition 4. $Pic^0(X) = Div^0(X)/Div^l(X)$.

Definition 5. $Jac(X) = \Omega^1_{hol}(X)^\wedge / H_1(X, \mathbb{Z})$.

Using Riemann-Roch Theorem, the right hand side is a complex torus of dimension g, where g is the genus of the compact Riemann Surface X.

Abel Theorem states that the above two objects are isomorphic.

Theorem 3 (Abel Theorem)**.** *Let X be a compact Riemann Surface, if* $g > 0$*, then*

$$Pic^0(X) \cong Jac(X), \ [\sum_x n_x x] \mapsto \sum_x n_x \int_{x_0}^{x}$$

The next theorem states that automorphic forms and $k/2$ forms are bijective in the sense of complex vector space.

Theorem 4. *Let k be an even positive integer, and* Γ *be a congruence group of* $SL_2(\mathbb{Z})$*. The following map is an isomorphism of complex vector space.*

$$\omega : A_k(\Gamma) \to \Omega^{\otimes k/2}(X(\Gamma))$$

In particular, ω *induces an isomorphism from* $S_2(\Gamma)$ *to* $\Omega^1_{hol}(X(\Gamma))$.

Proof. We sketch the proof. We know that $\pi : \mathcal{H} \to X(\Gamma)$ induce the map $\pi^* : \Omega^{\otimes k/2}(X(\Gamma)) \to \Omega^{\otimes k/2}(\mathcal{H})$. Thus given a meromorphic differential ω on $X(\Gamma)$, we get a meromorphic differential $f(\tau)(d\tau)^{k/2}$. We can prove this f is what we want since it's invariant under Γ.

The converse is tricky. □

2.1.2 Hecke Operators

We can define two **Operators** T from $M_k(\Gamma_1(N))$ to $M_k(\Gamma_1(N))$. Let f be a modular form respect to $\Gamma_1(N)$, i.e. $f \in M_k(\Gamma_1(N))$.

Let $\alpha \in GL_2^+(\mathbb{Q})$, and $\Gamma_1(N)\alpha\Gamma_1(N) = \bigcup_{i\ finite} \Gamma_1(N)\beta_i$ for some $\beta_j (\in M_2(Z))$. We aim to define $Tf \in M_k(\Gamma_1(N))$ corresponding to α. It's necessarily invariant under $\Gamma_1(N)$. Therefore, it's natural to define as follows:

$$Tf = \sum_{i\ finite} f[\beta_j]_k.$$

Thus given an element in $GL_2^+(\mathbb{Q})$, we have what is called double coset operators.

Definition 6 ($\langle d \rangle$)**.** *For $(d, N) = 1$, let $\alpha_0 = \begin{pmatrix} a & b \\ c & \delta \end{pmatrix} \in \Gamma_0(N)$, where $\delta \equiv d$ mod(N). Since for any $\alpha = \begin{pmatrix} a' & b' \\ c' & \delta' \end{pmatrix} \in \Gamma_0(N)$, where $\delta' \equiv d$ mod(N), we have $\Gamma_1(N)\alpha\Gamma_1(N) = \Gamma_1(N)\alpha_0 (using \Gamma_1(N) \triangleleft \Gamma_0(N))$. So there is a unique operator $\langle d \rangle$.*

$$\langle d \rangle f = f[\alpha_0]_k.$$

For $(n, N) > 1$, $\langle d \rangle f$ is defined to be 0.

It's easy to see that:

- $\langle d \rangle \langle e \rangle = \langle e \rangle \langle d \rangle = \langle de \rangle$,
- $M_k(N, \chi) = \{f : \langle d \rangle f = \chi(d) f \text{ for all } d \in (\mathbb{Z}/N\mathbb{Z})^*\}$.

Definition 7 (T_n)**.** *Let p be a prime and $\Gamma_1(N) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_1(N) = \bigcup_j \Gamma_1(N)\beta_j$. Then we define:*

$$T_p f = f[\Gamma_1(N) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_1(N)]_k := \sum_j f[\beta_j]_k.$$

In general,

$$T_1 = Id \text{ and } T_{p^r} = T_p T_{p^{r-1}} - p^{k-1}\langle p \rangle T_{p^{r-2}}, for\ r \geq 2,$$
$$T_{nm} = T_n T_m \text{ for } (n, m) = 1.$$

We list several facts we will use.

- $T_m\langle n\rangle = \langle n\rangle T_m$,
- The above two Hecke operators T define a map from $J_1(N) = Jac(X(\Gamma_1(N)))$ to itself.

We sketch the proof of the fact(2). Since $S_2(\Gamma) \cong \Omega^1_{hol}(X(\Gamma))$, We have $T : S_2(\Gamma_1(N))^\wedge \to S_2(\Gamma_1(N))^\wedge$ and the following commutative diagram:

$$\begin{array}{ccc} S_2(\Gamma_1(N))^\wedge & \xrightarrow{T} & S_2(\Gamma_1(N))^\wedge \\ \downarrow & & \downarrow \\ \Omega^1_{hol}(X(\Gamma_1(N)))^\wedge & \xrightarrow{T} & \Omega^1_{hol}(X(\Gamma_1(N)))^\wedge \end{array}$$

And T will map a loop to another loop, so it induces $T : J_1(N) \to J_1(N)$.

Definition 8. *A non zero modular form $f \in M_k(\Gamma_1(N))$ is called an **eigenform** if it is an eigenform for the Hecke Operators T_n and $\langle n\rangle$ for all $n \in \mathbb{Z}^+$. Moreover, if $a_1(f) = 1$, then f is called a **normalized eigenform**.*

Since $M_k(N,\chi) = \{f : \langle d\rangle f = \chi(d)f \text{ for all } d \in (\mathbb{Z}/N\mathbb{Z})^*\}$, for every eigenform f, there exists a Dirichlet character χ, $f \in M_k(N,\chi)$.

Definition 9. *$T_\mathbb{Z} = \mathbb{Z}[\{T_n, \langle n\rangle : n \in \mathbb{Z}^+\}]$, the Hecke algebra over $\mathbb{Z}$.*

Proposition 3. *$T_\mathbb{Z}$ is a finite generated $\mathbb{Z}$ module.*

Proof. $T_\mathbb{Z}$ can be viewed as a submodule of $End(H_1(X_1(N)), \mathbb{Z})$. □

Corollary 1. *Let f be a normalized eigenform, then $K_f = \mathbb{Q}(\{a_n(f)\})$ is a number field.*

Proof. For any normalized eigenform f, $f \in M_k(N,\chi)$, there is a surjective map from $T_\mathbb{Z}$ to $\mathbb{Z}[\{a_n(f), \chi(d) : n, d \in \mathbb{Z}_{>0}\}]$. Since

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

Let r=2 and take p, p' be two prime numbers, s.t. $p \equiv p' \pmod d$, then we have $\mathbb{Z}[\{a_n(f), \chi(d) : n, d \in \mathbb{Z}_{>0}\}]$=$\mathbb{Z}[\{a_n(f) : n \in \mathbb{Z}_{>0}\}]$. Thus $\mathbb{Z}[\{a_n(f) : n \in \mathbb{Z}_{>0}\}]$ is a finitely generated $\mathbb{Z}$ module, and $\mathbb{Q}(\{a_n(f) : n \in \mathbb{Z}_{>0}\})$ is a finite extension over $\mathbb{Q}$. □

Let d denote the dimension of K_f over $\mathbb{Q}$.

2.2 The Algebraic Structure

In this section, we introduce the algebraic structures of $X_1(N)$ and A_f, which have a $G_{\mathbb{Q}}$ action and induce an l-adic representation.

Henceforth, we assume f $\in S_2(\Gamma_1(N))$ be a newform at the level N and an eigenform of the Hecke algebra $T_{\mathbb{Z}}$. $J_1(N) = Jac(X_1(N))$, K_f is its number field. Here is a map:

$$\lambda_f : T_{\mathbb{Z}} \to \mathbb{C}, Tf = \lambda_f(T)f$$

and its kernel $I_f = ker(\lambda_f) = \{T \in T_{\mathbb{Z}} : Tf = 0\}$.

2.2.1 Abelian Variety associated to f

Definition 10. *The Abelian Variety associated to f is defined to be*

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

Let V_f = Span $(\{f^\sigma | \sigma : K_f \to \mathbb{C}$ is an embedding$\})$, a subspace of $S_2 = S_2(\Gamma_1(N))$, $V_f^\wedge$ is its dual space $\subset S_2^\wedge$. $\Lambda_f = H_1(X_1(N), \mathbb{Z})|_{V_f}$. It's natural to define

$$J_1(N) \to V_f^\wedge/\Lambda_f, \quad [\varphi] \mapsto \varphi|_{V_f} + \Lambda_f.$$

Proposition 4. *The above homomorphism induces an isomorphism:*

$$A_f \cong V_f^\wedge/\Lambda_f, \quad [\varphi] + I_f J_1(N) \mapsto \varphi|_{V_f} + \Lambda_f$$

And the right hand side is a complex torus of dimension $d = [K_f : \mathbb{Q}]$.

We omit the proof, and what we are concerned about is its complex torus structure of dimension d.

2.2.2 $X_1(N)$ is algebraic over $\mathbb{Q}$

Compact Riemann Surface is algebraic. But $X_0(N), X_1(N)$ can be taken as algebraic curves over $\mathbb{Q}$.

Henceforth, $X_1(N)$ denotes the modular curve as a nonsingular algebraic curve over $\mathbb{Q}$. Let $\widetilde{X_1}(N)$ denote its reduction at $\mathbb{F}_p$, and $X_1(N)_{\mathbb{C}}$ be our origin definition, i.e. $\mathbb{H}^*/\Gamma_1(N)$.

Theorem 5 (Eichler-Shimura Relation)**.** *Let $p \nmid N$. The following diagram commutes.*

$$\begin{array}{ccc} Pic^0(X_1(N)) & \xrightarrow{T_p} & Pic^0(X_1(N)) \\ \downarrow & & \downarrow \\ Pic^0(\widetilde{X}_1(N)) & \xrightarrow{\sigma_{p,*}+\widetilde{\langle p\rangle}_*\sigma_p^*} & Pic^0(\widetilde{X}_1(N)) \end{array}$$

Here

- $\sigma_p([x_0, x_1, \cdots, x_n]) = [x_0^p, x_1^p, \cdots, x_n^p]$,
- $\sigma_{p,*}([\sum Q]) = \sum[\sigma_p(Q)]$,
- $\sigma_p^*([\sum Q]) = p\sum[\sigma_p^{-1}(Q)]$.

Note that in $\mathbb{F}_p$, Frobenius is an isomorphism, thus the above map is well-defined.

2.2.3 l-adic Galois Representation

Since $X_1(N)$ is defined over $\mathbb{Q}$, there is a natural $G_{\mathbb{Q}}$ action on $Pic^0(X_1(N))$. For any $\sigma \in G_{\mathbb{Q}}$, any $x = (x_0 : x_1 : \cdots : x_n) \in X_1(N)$, $\sigma(x) = \big(\sigma(x_0) : \sigma(x : 1) : \cdots : \sigma(x_n)\big) \in X_1(N)$.

Thus for each n, there is a commutative diagram.

$$\begin{array}{ccc} & & G_{\mathbb{Q}} \\ & \swarrow & \downarrow \\ Aut(Pic^0(X_1(N))[l^n]) & \longleftarrow & Aut(Pic^0(X_1(N))[l^{n+1}]) \end{array}$$

We state without proof that the following two maps are isomorphisms.

$$i_n : Pic^0(X_1(N))[l^n] \hookrightarrow Pic^0(X_1(N)_{\mathbb{C}})[l^n](\cong Jac[l^n] \cong (\mathbb{Z}/l^n\mathbb{Z})^{2g})$$

$$\pi_n : Pic^0(X_1(N))[l^n] \twoheadrightarrow Pic^0(\widetilde{X}_1(N))[l^n], \text{if } p \nmid lN.$$

So these induce a homomorphism

$$\rho_{X_1(N),l} : G_{\mathbb{Q}} \to GL_{2g}(\mathbb{Z}_l) \subset GL_{2g}(\mathbb{Q}_l).$$

Theorem 6. *Let l be prime and let N be a positive integer. The Galois representation $\rho_{X_1(N),l}$ is* ***unramified*** *at every prime $p \nmid lN$. For any such p, let $\wp \subset \overline{\mathbb{Z}}$ be any maximal ideal lying over p. Then $\rho_{X_1(N),l}(Frob_\wp)$ satisfies the polynomial equation.*

$$x^2 - T_p x + \langle p \rangle p = 0.$$

We say ρ is unramified at prime number p, if for all $\wp$ lying over p, $I_\wp$, the inertia group, is contained in $\ker \rho$.

Proof. First note that $D_\wp / I_\wp \cong G_{\mathbb{F}_p}$, and there is a commutative diagram:

$$\begin{array}{ccc} D_\wp & \longrightarrow & Aut(Pic^0(X_1(N))[l^n]) \\ \downarrow \pi & & \downarrow \\ G_{\mathbb{F}_p} & \longrightarrow & Aut(Pic^0(\widetilde{X}_1(N))[l^n]) \end{array}$$

Since $I_\wp$ is the kernel of π, and right vertical arrow is isomorphic, $I_\wp$ is contained in the kernel of the map across the top. Since n is arbitrary, this means $I_\wp$ is contained in the kernel of ρ as desired.

By Eichler-Shimura Relation, we have the following commutative diagram:

$$\begin{array}{ccc} Pic^0(X_1(N))[l^n] & \xrightarrow{T_p} & Pic^0(X_1(N))[l^n] \\ \downarrow \pi_n & & \downarrow \pi_n \\ Pic^0(\widetilde{X}_1(N))[l^n] & \xrightarrow{\sigma_{p,*} + \widetilde{\langle p \rangle}_* \sigma_p^*} & Pic^0(\widetilde{X}_1(N))[l^n] \end{array}$$

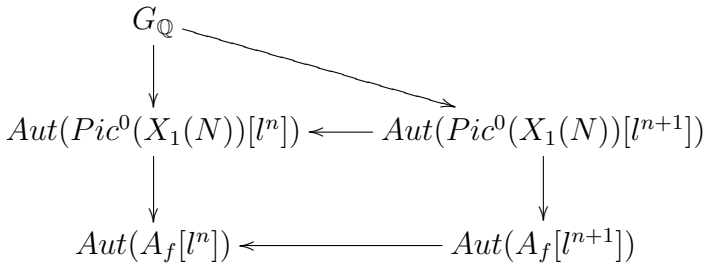
If we replace T_p by $Frob_p + \langle p \rangle p Frob_p^{-1}$, this makes the diagram commutes too, since two vertical arrows are isomorphisms, this shows

$$T_p = Frob_p + \langle p \rangle p Frob_p^{-1}.$$

The result then follows directly. □

Since $\ker(Pic^0(X_1(N))[l^n] \twoheadrightarrow A_f[l^n])$ is stable unber $G_{\mathbb{Q}}$(we omit the

proof), the following diagram commutes.



And

$$Ta_l(A_f) := \lim_{\leftarrow} A_f[l^n] \cong \lim_{\leftarrow} (\mathbb{Z}/l^n\mathbb{Z})^{2d} \cong (\mathbb{Z}_l)^{2d}.$$

As a corollary of the previous theorem, we have:

Theorem 7. *$\rho_{A_f,l} : G_{\mathbb{Q}} \to GL_{2d}(\mathbb{Q}_l)$ is unramified at every prime $p \nmid lN$. And $\rho(Frob_{\wp})$ satisfies*

$$x^2 - a_p(f)x + \chi(p)p = 0.$$

Lemma 2. *Let $V_l(A_f) := Ta_l(A_f) \otimes \mathbb{Q} \cong \mathbb{Q}_l^{2d}$. Then $V_l(A_f)$ is a free $K_f \otimes_{\mathbb{Q}} \mathbb{Q}_l$-module of rank 2.*

We omit the proof.

Using the canonical isomorphism $K_f \otimes \mathbb{Q}_l \cong \prod_{\lambda|l} K_{f,\lambda}$, we get

$$\rho_{f,\lambda} : G_{\mathbb{Q}} \to GL(V_l(A_f) \otimes_{K_f \otimes \mathbb{Q}_l} K_{f,\lambda}) \to GL_2(K_{f,\lambda}).$$

As a corollary to the previous theorem, we get the following:

Theorem 8. *This representation is unramified at every prime $p \nmid lN$. For any such p, let $\wp \subset \overline{\mathbb{Z}}$ be any maximal ideal lying over p. Then $\rho_{f,\lambda}(Frob_{\wp})$ satisfies the polynomial equation:*

$$x^2 - a_p(f)x + \chi(p)p = 0.$$

3 Several Methods in Representation Theory

In this section, we introduce several facts in representation theory.

Definition 11 (Semi-Simplification)**.** *Let V be a finite dimensional representation of G. $0 = V_0 \subset V_1 \subset \cdots \subset V_n = V$ is its Jordan-Holder series, i.e. V_i/V_{i-1} is simple. Then*

$$V^{ss} := \bigoplus_{j=1}^{n} V_j/V_{j-1}$$

is its semi-simplification.

Let $L/\mathbb{Q}_p$ be a finite extension, $\mathcal{O}$ the ring of intergers of L, π the uniformizer of the unique maximal ideal of $\mathcal{O}$, and $\mathbb{F} = \mathcal{O}/\pi$ the residue field. Let $\rho : G_{\mathbb{Q}} \to GL(V)$ be a continuous representation.

Proposition 5. *There exists a $\mathcal{O}$-lattice $\Lambda \subset V$, which is $G_{\mathbb{Q}}$ stable. And ρ induces a representation $\rho_\Lambda : G_{\mathbb{Q}} \to GL(\Lambda) \to GL(\Lambda/\pi\Lambda)$, which is called the reduction of ρ attached to Λ. The semi-simplification of ρ_Λ does not depend on the choice of Λ. Denote this unique representation by $\overline{\rho}$, which is called the residual representation of ρ.*

Proof. We just prove the first claim. For any lattice Λ', $H = \{g \in GL_n(L) : g(\Lambda') = \Lambda'\}$ is an open subgroup of $GL_n(L)$(here we actually use its non-Achimedian property). Hence its intersection with $G = \rho(G_{\mathbb{Q}})$, is open in G. Since $G_{\mathbb{Q}}$ is profinite, thus G is compact, we have $G = \bigcup_{i,finite} g_i(H \cap G)$.

Let $\Lambda = \sum_{i,finite} g(\Lambda')$, then we have a G-stable $\mathcal{O}$-lattice, hence is $G_{\mathbb{Q}}$-stable. □

We have a criterion to determine whether a representation is semi-simple or not.

Lemma 3 (Ribet's Lemma)**.** *Suppose that L-representation ρ is simple but $\overline{\rho}$ is NOT simple.. Let φ_1 and φ_2 be the characters associated to the reductions of ρ. Then G leaves stable some lattice $\Lambda \subset V$ for which the associated reductions is of the form $\begin{pmatrix} \varphi_1 & * \\ 0 & \varphi_2 \end{pmatrix}$ but is not semi-simple.*

Proof. We sketch the proof. First, we need to show that at least one of these reductions is of the desired type $\begin{pmatrix} \varphi_1 & * \\ 0 & \varphi_2 \end{pmatrix}$. Next, if all reductions of this type are semi-simple, then ρ cannot be simple, which is a contradiction.

□

4 Proof of the Ribet's Theorem

In this section, we follow Ribet's origin proof. First, we introduce two stronger versions of the theorem.

Theorem 9. *Let $k \in [2, p-3]$ be an even integer, and suppose that $p|B_k$. Then there exists a galoisian extension $E/\mathbb{Q}$ containing $K = \mathbb{Q}(\mu_p)$ such that*

- *(a)The extension E/K is everywhere unramified,*
- *(b)The group $H = Gal(E/K)$ is a non-trivial p-elementary commutative group, i.e. $H \cong (\mathbb{Z}/p\mathbb{Z})^n$,*
- *(c)For every $\sigma \in$G=Gal(E/$\mathbb{Q}$), $\overline{\sigma} \in \Delta = Gal(K/\mathbb{Q})$, and every $\tau \in H$,*

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

Here H has a natural $\mathbb{F}_p^*$ structure, i.e., for $a \in Im(\chi) = \mathbb{F}_p^*$, and $\tau \in H$, $a \cdot \tau = \tau^a$.

Proposition 6. *This theorem implies Ribet's Theorem 2.*

Proof. Let M be the Hilbert class field of $K = \mathbb{Q}(\mu_p)$, then E is contained in M. Using Artin map, we have $Gal(M/K) \cong Cl_K$ as $\mathbb{Z}[\Delta]$ -module.

Note that for any $\sigma \in \Delta$, any $\tau \in Gal(M/k)$ and any $[I] \in Cl_K$,

$$\sigma(\tau) = \sigma\tau\sigma^{-1}, \text{and } \sigma([I]) = [\sigma(I)]$$

We have $Gal(M/K)/Gal(M/K)^p \cong Cl_K/Cl_K^p = C$ as $\mathbb{F}_p[\Delta]$ -module, and is the biggest p-elementary group which is a quoient of $Gal(M/K)$. Since H is a p-elementary group and the quoient of $Gal(M/K)$, this implies that $H \hookrightarrow C$.

Using (c) of the theorem, $H = H(\chi^{1-k}) \neq \emptyset$, then $C(\chi^{1-k}) \neq \emptyset$. □

Let $D_\wp \subset G_\mathbb{Q}$ denote one of the decomposition group at the prime p, i.e. $D_\wp = \{\sigma \in G_\mathbb{Q} : \wp^\sigma = \wp, p \subset \wp \subset \overline{\mathbb{Z}}\}$. Let $\chi : G_\mathbb{Q} \to Gal(\mathbb{Q}(\mu_p)/\mathbb{Q}) \xrightarrow{\sim} \mathbb{F}_p^*$.

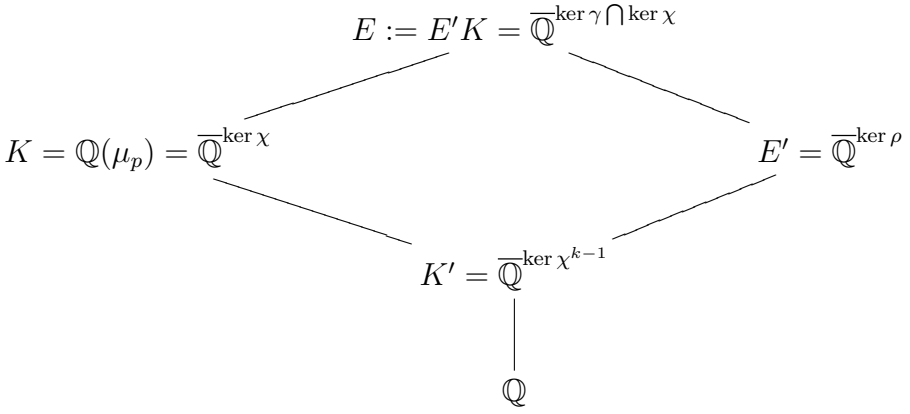
The following theorem is stronger than the previous one.

Theorem 10. *Let $k \in [2, p-3]$ be an even integer, and suppose that $p|B_k$. There exists a finite extension $\mathbb{F}/\mathbb{F}_p$, and a continuous representation $\rho : G_\mathbb{Q} \to GL_2(\mathbb{F})$, such that*

- *(1) ρ is unramified at every prime $l \neq p$,*
- *(2)$\rho \sim \begin{pmatrix} 1 & \gamma \\ & \chi^{k-1} \end{pmatrix}, \gamma : G_{\mathbb{Q}} \to \mathbb{F}$ is non-trivial,*
- *(3)$\rho|_{D_\wp}$ is semi-simple.*

Proposition 7. *The theorem 10 is stronger than the theorem 9.*

Proof. Using the theorem 10, we have the following diagram:



Let $H' = Gal(E'/K')$, then $H' \cong \ker\chi^{k-1}/\ker\rho = \ker\chi^{k-1}/\ker\chi^{k-1} \bigcap \ker\gamma$. Since $\gamma : \ker\chi^{k-1} \to \mathbb{F}$, this induces $\gamma : H \hookrightarrow \mathbb{F}$. Thus $H = Gal(E/K) \cong H'$ is p-elementary group.

For any prime $l \neq p$, any λ lying over l, we have $I_\lambda \subset \ker\rho$, this implies that $\overline{\mathbb{Q}}^{\ker\rho} \subset \overline{\mathbb{Q}}^{I_\lambda}$. Therefore, for any prime $l \neq p$, E'/K' is unramified.

Choose $\mathbf{p} = \wp \bigcap \mathcal{O}_{E'}$ in E', we claim $\mathbf{p}$ over the unique $\mathfrak{p}$ in K' lying over p, is unramified. If we prove this claim, since E'/K' is galois, then (a) of the theorem 9 is done.

Note that $\rho|_{D_\wp}$ is semi-simple, it's equivalent to say that the order of $\rho(D_\wp)$ can not be divided by p, i.e. $p \nmid \#\rho(D_\wp)$. Since

$$\rho(D_\wp) \cong D_\wp/\ker\rho \cap D_\wp, \text{and } I_{\mathbf{p}} \leq D_{\mathbf{p}} \leq G_{\mathbb{Q}}/\ker\rho$$

we conclude that $p \nmid e = \#I_{\mathbf{p}}$. On the other hand, $I_{\mathbf{p}} \leq H'$, which is a p-elementary group, thus $e = 1$, i.e. E'/K' is everywhere unramified. And this implies that E/K is everywhere unramified.

It remains to prove (c) of the theorem 9, i.e. $\sigma\tau\sigma^{-1} = \chi(\overline{\sigma})^{1-k} \cdot \tau$. Since the above elements are in $Gal(E/K) \cong \ker \chi^{k-1} / \ker \rho$, so only need to verify

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

and this is because:

$$\begin{pmatrix} 1 & \gamma(\sigma) \\ 0 & \chi^{k-1}(\sigma) \end{pmatrix} \begin{pmatrix} 1 & \gamma(\tau) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \gamma(\sigma) \\ 0 & \chi^{k-1}(\sigma) \end{pmatrix}^{-1} = \begin{pmatrix} 1 & \chi^{1-k}(\sigma) \cdot \gamma(\tau) \\ 0 & 1 \end{pmatrix}.$$

□

Let $\mathbb{F}_p^* \to \mathbb{Z}_p^*$ be the Teichmuller lift, $\omega : \mathbb{F}_p \to \mu_{p-1}$ such that

$$\begin{array}{ccc} \mathbb{F}_p^* & \xrightarrow{\omega} & \mu_{p-1} \\ {\scriptstyle lift}\downarrow & \swarrow & \\ \mathbb{Z}_p^* & & \end{array}$$

commutes. $\epsilon = \omega^{k-2}$. We state without proof that there exists a nice eigenform.

Theorem 11. *Suppose $p|B_k$, there exists a normalized cusp eigenform $f \in S_2(p, \epsilon)$, $f = \sum_{n>0} a_n q^n$, and a prime ideal $\wp|p$ of the number field K_f, such that for every prime $l \neq p$, the number a_l is $\wp$-integral and*

$$a_l \equiv 1 + l^{k-1} \equiv 1 + \epsilon(l)l \ (mod\ p).$$

Recall in the previous section we have proved theorem 8 which states that $\rho_{f,\wp}$ is unramified at $l \nmid p^2$, and for maximal ideal $\lambda \subset \overline{\mathbb{Z}}$, lying over prime number $l \nmid p^2$:

$$Tr(\rho_{f,\wp}(Frob_\lambda)) = a_l(f), det(\rho_{f,\wp}(Frob_\lambda)) = \epsilon(l)l.$$

Proposition 8. *The representation $\rho_{f,\wp}$ is simple.*

Proof. Suppose not, then its semi-simplification is $\rho_1 \oplus \rho_2$, where $\rho_i : G_{\mathbb{Q}} \to K_{f,\wp}^*$. We state without proof that each ρ_i can be written as $\rho_i = \epsilon_i \widetilde{\chi}^{n_i}$, where $\widetilde{\chi} : G_{\mathbb{Q}} \to Gal(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \cong \mathbb{Z}_p^*$, the p-adic cyclotomic character, and $\epsilon_i : G_{\mathbb{Q}} \to K_{f,\wp}^*$ is of finite order. Since

$$\epsilon_i(Frob_\lambda) = \epsilon_i(l),\ \widetilde{\chi}(Frob_\lambda) = l,$$

We have

$$\begin{cases} \epsilon_1(l)l^{n_1} + \epsilon_2(l)l^{n_2} = a_l \\ \epsilon_1(l)\epsilon_2(l)l^{n_1+n_2} = l\epsilon(l). \end{cases}$$

Thus $n_1 + n_2 = 1$, W.L.O.G, $\begin{cases} n_1 \geq 1 \\ n_2 \leq 0 \end{cases}$, and this implies that $|a_l| \geq l - 1$.

Due to the Ramanujan Bounds, which states that for almost all prime l, $a_l(f) \leq 2\sqrt{l}$, we conclude a contradiction. □

Denote the ring of integer of $K_{f,\wp}$ by $\mathcal{O}_{f,\wp}$.

Proposition 9. *There exists a $G_{\mathbb{Q}}$ -stable $\mathcal{O}_{f,\wp}$ -lattice $\Lambda \subset V_{\wp}(A_f)$ such that*

$$\rho_{f,\wp,\Lambda} \sim \begin{pmatrix} 1 & * \\ 0 & \chi^{k-1} \end{pmatrix}, \rho_{f,\wp,\Lambda} \nsim \begin{pmatrix} 1 & 0 \\ 0 & \chi^{k-1} \end{pmatrix}.$$

Proof. Due to the lemma 3 and the proposition above, it's sufficient to prove that $\overline{\rho}_{f,\wp}$ is NOT simple, i.e. $\overline{\rho}_{f,\wp} \sim 1 \oplus \chi^{k-1}$. Here $\overline{\rho}_{f,\wp}$ is the unique semi-simplification of the reduction of $\rho_{f,\wp}$.

For any prime $l \neq p$, since ρ is unramified at l, so is $\overline{\rho}$.

$$\begin{cases} tr(\rho(Frob_l)) = & a_l \equiv & 1 + l^{k-1} \bmod (\mathrm{p}), \\ det(\rho(Frob_l)) = & l\epsilon(l) \equiv & l^{k-1} \bmod (\mathrm{p}). \end{cases}$$

Consider another representation $\rho' : G_{\mathbb{Q}} \to GL_2(\mathbb{F})$, $\rho' \sim 1 \oplus \chi^{k-1}$, then $\overline{\rho}(Frob_l) \sim \rho'(Frob_l)$ for any $l \neq p$. By Prop 5 and Cebotarev density theorem, which states that $F = \{Frob_\lambda\}_{\{l \ prime, \lambda | l\}}$ is dense in $G_{\mathbb{Q}}$, we have $\overline{\rho} \sim \rho' \sim 1 \oplus \chi^{k-1}$.

□

To sum up, $\rho_{f,\wp,\Lambda}$ has the properties that

- It's unramified at every prime $l \neq p$.
- It's NOT semi-simple.

We claim $\rho_{f,\wp,\Lambda}$ is what we want in the theorem 10. We omit the proof that $\rho|_D$ is semi-simple since it's beyond the scope here.

Acknowledgement

First of all, I would like to give my heartfelt thanks to all the people who have ever helped me with this paper.

My sincere and hearty thanks and appreciations go firstly to my supervisor, Prof. Xu Jinxing, and Prof. Liu Zheng(at UCSB), who gave me the

idea of the Iwasawa Theory and recommended several books and papers to me. When I had difficulty reading the paper, they also lend me a helping hand. Their kindly help runs through my writing.

I am also extremely grateful to Zhou Keshu and You Lei who explained to me several ideas and theorems in Riemann Surface. In addition, many thanks go to my classmates who gave wonderful talks at Hua Loo-Keng Seminar, which encouraged me to be better.

5 Reference

References

[1] Kenneth A. Ribet, A modular construction of unramified p-extensions of Q(µ p), Invent. Math. 34 (1976), no. 3, 151–162. MR MR0419403 (54 #7424)

[2] Fred Diamond and Jerry Shurman, A first course in modular forms, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005. MR MR2112196 (2006f:11045)

[3] Chandan Singh Dalawat. Ribet's modular construction of unramified p-extensions of $Q(\mu_p)$, arXiv:0903.2617

[4] Keqin Feng, Algebraic Number Theory(in Chinese), HARBIN INSTITUTE OF TECHNOLOGY PRESS, 2018

[5] Lawrence C. Washington, Introduction to cyclotomic fields, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997. MR MR1421575 (97h:11130)

[6] Jacques Herbrand, Sur les classes des corps circulaires, J. Math. Pures et Appliqu´ ees (9) 11 (1932), 417–441.