Ribet-Herbrand Theorem

Anlun Li

USTC

May 25, 2022

Plan

- A Short Review
- Two Stronger Versions of The Theorem
- Introduction to the Modular Forms
- Ribet's Idea of the proof

Notations

Let $A = Cl(\mathbb{Q}(\mu_p))$ finite ideal class group, $C = A/A^p$ is a $\mathbb{F}_p$ vector space.

$\Delta = Gal(\mathbb{Q}(\mu_p)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^*$

$G_{\mathbb{Q}} = Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ the absolute Galois group.

$\chi : G_{\mathbb{Q}} \to Gal(\mathbb{Q}(\mu_p)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^*$, sometimes it will also denote a Dirichlet character.

$H = \{z \in \mathbb{C} : Im(Z) > 0\}$, the upper half plane.

Decomposition

Lemma (Decomposition Lemma)

If R is a commutative ring containing $\{\langle \mu_n \rangle\}$ and $\frac{1}{n}$, G is an abelian group with order n, then for $R[G]$ -module M, we have

$$M = \bigoplus_{\chi} M(\chi),$$

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

View C as $\mathbb{F}_p[Gal(K/\mathbb{Q})]$ module, we have:

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

as a $\mathbb{F}_p$ vector space.

Decomposition

Lemma (Decomposition Lemma)

If R is a commutative ring containing $\{\langle\mu_n\rangle\}$ and $\frac{1}{n}$, G is an abelian group with order n, then for $R[G]$ -module M, we have

$$M = \bigoplus_{\chi} M(\chi),$$

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

View C as $\mathbb{F}_p[Gal(K/\mathbb{Q})]$ module, we have:

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

as a $\mathbb{F}_p$ vector space.

Statements of the Theorem

Let $\frac{t}{e^t-1} = \sum_{n=0}^{\infty} B_k \frac{t^n}{n!}$. B_n is called Bernoulli numbers. A fact states that $\zeta(1-n) = -\frac{B_n}{n}$ for $n \geq 1$.

In the 1930s, Herbrand found:

Proposition (Herbrand,1930s)

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

This is a consequence of the Stickelberger's Theorem.
Today, we mainly focus on the converse.

Theorem (Ribet,1970s)

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

Statements of the Theorem

Let $\frac{t}{e^t-1} = \sum_{n=0}^{\infty} B_k \frac{t^n}{n!}$. B_n is called Bernoulli numbers. A fact states that $\zeta(1-n) = -\frac{B_n}{n}$ for $n \geq 1$.

In the 1930s, Herbrand found:

Proposition (Herbrand,1930s)

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

This is a consequence of the Stickelberger's Theorem.
Today, we mainly focus on the converse.

Theorem (Ribet,1970s)

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

Version 2

We first introduce two stronger versions of the theorem.

Theorem

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

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

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

This theorem indeed implies Ribet's Theorem.

Version 3

Let $D \subset G_{\mathbb{Q}}$ denote one of the decomposition group at the prime p, i.e. $D = \{\sigma \in G_{\mathbb{Q}} : \wp^{\sigma} = \wp, p \subset \wp \subset \bar{\mathbb{Z}}\}$. $\chi : G_{\mathbb{Q}} \to Gal(\mathbb{Q}(\mu_p)/\mathbb{Q}) \xrightarrow{\sim} \mathbb{F}_p^*$.
The following theorem is stronger than the previous one.

Theorem

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

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

Note that in such case, a representation is semi-simple if and only if its image cannot be divided by p.

Definition (Congruence Group)

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

We will also need the following definitions.

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

Modular Forms

Definition (Modular Curves)

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

Fact: $X(\Gamma)$ is a compact Riemann Surface.

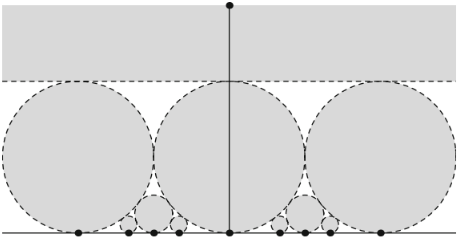

Figure 1: Neighborhoods of ∞ and of some rational points

An Example: $X(SL_2(\mathbb{Z})) \cong S^2$

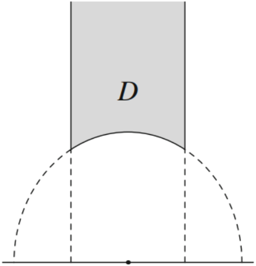

Figure 2: the fundamental domain for $SL_2(\mathbb{Z})$

Modular Forms

Definition (Modular Forms of weight k with respect to Γ)

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

- f is holomorphic in H
- $f[\gamma]_k = f$ for any $\gamma \in \Gamma$
- $f[\alpha]_k$ is holomorphic at ∞ for any $\alpha \in SL_2(\mathbb{Z})$

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**.

Modular Forms

Definition (Modular Forms of weight k with respect to Γ)

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

- f is holomorphic in H
- $f[\gamma]_k = f$ for any $\gamma \in \Gamma$
- $f[\alpha]_k$ is holomorphic at ∞ for any $\alpha \in SL_2(\mathbb{Z})$

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**.

Modular Forms

Definition (Modular Forms of weight k with respect to Γ)

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

- f is holomorphic in H
- $f[\gamma]_k = f$ for any $\gamma \in \Gamma$
- $f[\alpha]_k$ is holomorphic at ∞ for any $\alpha \in SL_2(\mathbb{Z})$

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**.

Modular Forms

Proposition (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 $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^*$. □

Pic^0 and Jacobi

Definition

$Pic^0(X) = Div^0(X)/Div^l(X)$

Definition

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

Note that the right side is a complex torus of dimension g.

Theorem (Abel Theorem)

For X a compact Riemann Surface, if $g > 0$, then

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

Pic^0 and Jacobi

Definition

$Pic^0(X) = Div^0(X)/Div^l(X)$

Definition

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

Note that the right side is a complex torus of dimension g.

Theorem (Abel Theorem)

For X a compact Riemann Surface, if $g > 0$, then

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

Pic^0 and Jacobi

Definition

$Pic^0(X) = Div^0(X)/Div^l(X)$

Definition

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

Note that the right side is a complex torus of dimension g.

Theorem (Abel Theorem)

For X a compact Riemann Surface, if $g > 0$, then

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

Maps induced by $\sigma : X \to Y$

Let $\sigma : X \to Y$ be a nonconstant holomorphic map between compact Riemann Surfaces, then we have forward map and reverse map of Pic^0.

$$\sigma_* : Pic^0(X) \to Pic^0(Y)$$

$$\sigma_*[\sum_x n_x x] = [\sum_x n_x \sigma(x)]$$

$$\sigma^* : Pic^0(Y) \to Pic^0(X)$$

$$\sigma^*[\sum_y n_y y] = [\sum_y n_y \sum_{x \in \sigma^{-1} y} e_x x]$$

Theorem

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 $\Omega^1_{hol}(X(\Gamma))$

Hecke Operators(1)

We can define two **Operators** 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. $f \in M_k(\Gamma_1(N))$.

Definition ($\langle n \rangle$)

For $(n, N) = 1$, define

$$\langle d \rangle f = f[\alpha]_k \text{ for an } \alpha = \begin{pmatrix} a & b \\ c & \delta \end{pmatrix} \in \Gamma_0(N), \text{where } \delta \equiv d \text{ mod(N)}.$$

For $(n, N) > 1$, $\langle d \rangle f = 0$.

Fact:

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

Hecke Operators(1)

We can define two **Operators** 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. $f \in M_k(\Gamma_1(N))$.

Definition ($\langle n \rangle$)

For $(n, N) = 1$, define

$$\langle d \rangle f = f[\alpha]_k \text{ for an } \alpha = \begin{pmatrix} a & b \\ c & \delta \end{pmatrix} \in \Gamma_0(N), \text{where } \delta \equiv d \bmod (\text{N}).$$

For $(n, N) > 1$, $\langle d \rangle f = 0$.

Fact:

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

Hecke Operators(1)

We can define two **Operators** 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. $f \in M_k(\Gamma_1(N))$.

Definition ($\langle n \rangle$)

For $(n, N) = 1$, define

$$\langle d \rangle f = f[\alpha]_k \text{ for an } \alpha = \begin{pmatrix} a & b \\ c & \delta \end{pmatrix} \in \Gamma_0(N), \text{where } \delta \equiv d \text{ mod(N)}.$$

For $(n, N) > 1$, $\langle d \rangle f = 0$.

Fact:

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

Hecke Operators(2)

Let $\Gamma_1(N)\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\Gamma_1(N)=\bigcup_j \Gamma_1(N)\beta_j$, for some $\beta_j(\in M_2(Z))\equiv \begin{pmatrix}1 & *\\ 0 & p\end{pmatrix}(mod\ N), det\ \beta=p.$

Definition (T_p)

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

In general, $T_1=Id$, and $T_{p^r}=T_pT_{p^{r-1}}-p^{k-1}\langle p\rangle T_{p^{r-2}}$, for $r\geq 2$. $T_{nm}=T_nT_m$ for $(n,m)=1$.

Facts of Hecke Operators

We list serveral facts we will use.

- $T_m\langle n\rangle = \langle n\rangle T_m$
- T defines a map from $J_1(N) = Jac(X(\Gamma_1(N)))$ to itself, where T is T_n or $\langle n\rangle$ for any $n \in \mathbb{Z}_{>0}$.

Eigenform

Definition

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, $f \in M_k(N, \chi)$.

Hecke algebra over $\mathbb{Z}$

Definition

$T_{\mathbb{Z}} = \mathbb{Z}[\{T_n, \langle n \rangle : n \in \mathbb{Z}^+\}]$, the algebra of $S_2(\Gamma_1(N))$ generated over $\mathbb{Z}$.

Proposition

$T_{\mathbb{Z}}$ 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

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

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

Hecke algebra over $\mathbb{Z}$

Definition

$T_{\mathbb{Z}} = \mathbb{Z}[\{T_n, \langle n \rangle : n \in \mathbb{Z}^+\}]$, the algebra of $S_2(\Gamma_1(N))$ generated over $\mathbb{Z}$.

Proposition

$T_{\mathbb{Z}}$ 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

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

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

Hecke algebra over $\mathbb{Z}$

Definition

$T_{\mathbb{Z}} = \mathbb{Z}[\{T_n, \langle n \rangle : n \in \mathbb{Z}^+\}]$, the algebra of $S_2(\Gamma_1(N))$ generated over $\mathbb{Z}$.

Proposition

$T_{\mathbb{Z}}$ 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

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

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

Abelian Variety constructed by Shimura

Let f $\in S_2(\Gamma_1(N))$ be a newform at the level N and an eigenform of the Hecke algebra $T_{\mathbb{Z}}$. $J_1(N) = Jac(X_1(N))$.

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

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

Definition

The Abelian Variety associated to f is defined to be

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

A Property of $A_f = J_1(N)/I_f J_1(N)$

Let $V_f = \text{Span}\left(\{f^\sigma | \sigma : K_f \to \mathbb{C} \text{ is an embedding}\}\right)$, 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

Let $f \in S_2(\Gamma_1(N))$ be an eigenform and newform with number field K_f, then

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

The right side is a complex torus of dimension $[K_f : \mathbb{Q}]$.

A Property of $A_f = J_1(N)/I_f J_1(N)$

Let $V_f = \text{Span}\left(\{f^\sigma | \sigma : K_f \to \mathbb{C} \text{ is an embedding}\}\right)$, 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

Let $f \in S_2(\Gamma_1(N))$ be an eigenform and newform with number field K_f, then

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

The right side is a complex torus of dimension $[K_f : \mathbb{Q}]$.

Igusa Theorem

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

Henceforce, $X_1(N)$ denotes the modular curve as a nonsingular algebraic curve over $\mathbb{Q}$. Let $\widetilde{X}_1(N)$ denote its reduction at $\mathbb{F}_p$.

Theorem (Igusa Theorem)

Let N be a positive number, and prime $p \nmid N$, then $X_1(N)$ acquires good reduction at p.

Eichler-Shimura Relation

Theorem (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

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

l-adic Galois Representation

Since $X_1(N)$ is defined over $\mathbb{Q}$, we can define a $G_{\mathbb{Q}}$ action on $Pic^0(X_1(N))$.
For each n, there is a commutative diagram.

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

We state without proof that the inclusion below is an isomorphism.

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

So these induce a homomorphism

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

l-adic Galois Representation

Since $X_1(N)$ is defined over $\mathbb{Q}$, we can define a $G_{\mathbb{Q}}$ action on $Pic^0(X_1(N))$.
For each n, there is a commutative diagram.

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

We state without proof that the inclusion below is an isomorphism.

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

So these induce a homomorphism

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

l-adic Galois Representation

Since $X_1(N)$ is defined over $\mathbb{Q}$, we can define a $G_{\mathbb{Q}}$ action on $Pic^0(X_1(N))$.
For each n, there is a commutative diagram.

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

We state without proof that the inclusion below is an isomorphism.

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

So these induce a homomorphism

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

l-adic Galois Representation

Theorem

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 $\wp \subset \bar{\mathbb{Z}}$ be any maximal ideal over p. Then $\rho_{X_1(N),l}(Frob_{\wp})$ satisfies the polynomial equation.*

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

l-adic Galois Representation

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.

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

And

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

As a corollary of the previous theorem, we have:

Theorem

Let f be a normalized, newform and eigenform in $S_2(N, \chi)$, $\rho_{A_f,l} : G_{\mathbb{Q}} \to GL_{2d}(\mathbb{Q}_l)$, is unramified at every prime $p \nmid lN$. And $\rho(Frob_{\wp})$ satisfies

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

l-adic Galois Representation

Let $V_l(A_f) := Ta_l(A_f) \otimes \mathbb{Q} \cong \mathbb{Q}_l^{2d}$

Lemma

$V_l(A_f)$ is a free $K_f \otimes_{\mathbb{Q}} \mathbb{Q}_l$-module of rank 2.

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

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

l-adic Galois Representation

Let f $\in S_2(N, \chi)$ be a normalized eigenform with number field K_f. Let l be a prime, for each maximal ideal λ of $\mathcal{O}_{K_f}$ lying over l, there is a 2-dimensional Galois representation

$$\rho_{f,\lambda} : G_{\mathbb{Q}} \to GL_2(K_{f,\lambda}).$$

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

Theorem

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

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

Reduction

Let $L/\mathbb{Q}_p$ be a finite extension, $\mathcal{O}$ the ring of intergers of L, π 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. Then there exists a $\mathcal{O}$-lattice $\Lambda \subset V$, which is $G_{\mathbb{Q}}$ stable.

And ρ induces a representation $\rho_\Lambda : G_{\mathbb{Q}} \to GL(\Lambda) \to GL(\Lambda/\pi\Lambda)$

ρ_Λ is called the reduction of ρ attached to Λ.

Semi-Simplification

Definition (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.

We will use the following result.

Proposition

The semi-simplification of the representation of $G_{\mathbb{Q}}$ on $\Lambda / \pi \Lambda$ does not depend on the choice of Λ. Denote this unique representation by $\bar{\rho}$.

Ribet's Lemma

We have a criteria to determine whether a representation is semi-simple or not. Let $L/\mathbb{Q}_p$ be a finite extension.

Proposition (Ribet's Lemma)

Suppose that L-representation ρ is simple but $\bar{\rho}$ 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 $\begin{pmatrix} \varphi_1 & * \\ & \varphi_2 \end{pmatrix}$ but is not semi-simple.

A Nice Eigenform constructed by Ribet

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

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 that for $\lambda | l$:

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

Proposition

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

Ribet's Idea

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

Proposition

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

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

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 omit the proof that $\rho|_D$ is semi-simple.

Reference

- Kenneth A. Ribet. A modular construction of unramifiedp-extensions of $Q(\mu_p)$
- Fred Diamond, Jerry Shurman. A First Course in Modular Forms
- Chandan Singh Dalawat. Ribet's modular construction of unramified p-extensions of $Q(\mu_p)$

Thank You!