Iwasawa Main Conjecture

For simplicity, we concentrate on the simplest case

$$K = \mathbb{Q}(\mu_p)$$

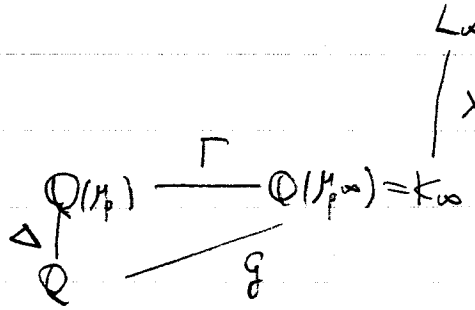
$$K_\infty = \mathbb{Q}(\mu_{p^\infty}) = \bigcup_{n>0} \mathbb{Q}(\mu_{p^n})$$

with p : odd prime.

$$G = \mathrm{Gal}(K_\infty/\mathbb{Q}) = \Delta \times \Gamma$$

$$\Delta = \mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/(p-1)\mathbb{Z}$$

$$\Gamma = \mathrm{Gal}(K_\infty/K) \simeq \mathbb{Z}_p$$



Let L_∞ be the maximal unramified abelian pro-p extension of K_∞ and put

$$X = \mathrm{Gal}(L_\infty/K_\infty)$$

By class field theory,

$$X \simeq \varprojlim_{\text{Norm}} A_{K_n} \qquad (\text{where } \underbrace{K \subset K_n}_{\deg = p^n} \subset K_\infty$$

A_{K_n} := p-primary component of the ideal class group of K_n)

$$\Lambda := \mathbb{Z}_p[[G]]$$

Our aim is to know the Λ-module X.

Since $\mathbb{Z}_p[\Delta] = \bigoplus_{i=0}^{p-2} \mathbb{Z}_p e_{\omega^i}$ $\left(e_{\omega^i} = \frac{1}{p-1}\sum_{\sigma\in\Delta} \omega^i(\sigma)\sigma^{-1}\right)$,

any $\mathbb{Z}_p[\Delta]$-module M is decomposed as

$$M = \bigoplus_{i=0}^{p-2} M^{[i]} \quad \text{with } M^{[i]} = \{x \in M \mid \sigma(x) = \omega^i(\sigma)x \text{ for all } \sigma \in \Delta\}$$

So $X = \bigoplus_{i=0}^{p-2} X^{[i]}$

$X^{[i]}$ is a $\Lambda^{[i]}$-module. $\left(\Lambda = \bigoplus \Lambda^{[i]} \simeq \bigoplus \mathbb{Z}_p[[T]]\right)$

We get easily $X^{[0]} = X^{[1]} = 0$. So in the following, suppose $i \neq 0, 1$.

Main Conjecture I $\quad \mathrm{char}\left(X^{[j]}\right) = \mathrm{char}\left(\left(\mathcal{E}_\infty / \mathcal{C}_\infty\right)^{[j]}\right)$

(char. ideal in $\Lambda^{[j]} \simeq \mathbb{Z}_p[[T]]$)

for even j s.t. $0 < j < p-2$

Main Conjecture II $\quad \mathrm{char}\left(\mathrm{Gal}(M_\infty/k_\infty)^{[j]}\right) = \left(\xi_p^{[j]}\right)$

(max. unramified outside p, pro-p abelian ext. ; p-adic L)

for even j s.t. $0 < j < p-2$.

Main Conjecture (Original form by Iwasawa)

For odd i s.t. $1 < i \leq p-2$,

$$\mathrm{char}\left(X^{[i]}\right) = \left(\theta_{k_\infty}^{[i]}\right)$$

$\theta_{k_\infty}^{[i]}$: a twist of ξ_p (we describe it explicitly later)

$$\text{MC I} \iff \text{MC II} \iff \text{MC}$$

(yesterday; duality (Kummer dual))

$$\mathrm{Hom}\left(\varinjlim A_{k_n}^{[i]}, \mu_{p^\infty}\right) \simeq \mathrm{Gal}(M_\infty/k_\infty)^{[p-i]}$$

for odd i s.t. $1 < i \leq p-2$.

θ_{k_n} : Stickelberger element

$$\theta_{k_n} = \sum_{\sigma \in \mathrm{Gal}(k_n/\mathbb{Q})} \zeta(0,\sigma)\sigma^{-1} = \sum_{\substack{a=1 \\ (a,p)=1}}^{p^{n+1}} \left(\frac{1}{2} - \frac{a}{p^{n+1}}\right)\sigma_a^{-1} \in \mathbb{Q}[\mathrm{Gal}(k_n/\mathbb{Q})]$$

partial zeta fct $\quad \zeta(s,\sigma_a) = \sum_{\substack{n=1 \\ n \equiv a \pmod{p^{n+1}}}}^{\infty} \frac{1}{n^s}$

$$\theta_{K_n} \in \mathbb{Q}[Gal(K_n/\mathbb{Q})] = \mathbb{Q}[\Delta \times Gal(K_n/k)] \xrightarrow{\omega^i} \mathbb{Q}_p[Gal(K_n/k)]$$

$$(\sigma, \tau) \longmapsto \omega^i(\sigma)\tau$$

$$\omega^i(\theta_{K_n}) \in \mathbb{Z}_p[Gal(K_n/k)] \quad \forall\ i \neq 1.$$

$(\omega^i(\theta_{K_n}))_{n \geq 0}$ is a projective system. (This follows easily from the definition of θ_{K_n}.)

$$\theta_{K_\infty}^{[i]} := (\omega^i(\theta_{K_n})) \in \varprojlim \mathbb{Z}_p[Gal(K_n/k)] = \Lambda^{[i]}$$

☆ $\mathrm{char}(X^{[i]}) \mid \theta_{K_\infty}^{[i]}$ can be proved by Euler system argument.

(The above divisibility implies the equality by using the analytic class number formula (Iwasawa))

☆☆ $\theta_{K_\infty}^{[i]} \mid \mathrm{char}(X^{[i]})$ can be proved by using modular forms. (modular curves)

(Again, the above divisibility implies the equality by using ACNF, and MC was first proved in this direction)

MC for Selmer groups over K_∞ for elliptic curves

☆ — Kato

☆☆ — Skinner, Urban ⟹ get the equality.

We identify $\Lambda^{[i]}$ with $\mathbb{Z}_p[[T]]$

★ $X^{[i]}/(\gamma-1)X^{[i]} = X^{[i]}/TX^{[i]} \simeq A_K^{[i]}$

★ $\theta_{K_\infty}^{[i]}(0) = \sum_{a=1}^{p-1} \left(\frac{1}{2} - \frac{a}{p}\right)\omega^{-i}(a) = -B_{1,\omega^{-i}} \equiv \frac{B_{p-i}}{p-i} \pmod p$

By Nakayama's lemma, MC $\Rightarrow$ $\left(A_K^{[i]} \neq 0 \iff p \mid B_{p-i}\right)$

Th (Herbrand Ribet) $A_K^{[i]} \neq 0 \iff p \mid B_{p-i}$

Rem. $(\exists i : \text{odd}\ A_K^{[i]} \neq 0) \iff (\exists i : \text{odd}\ p \mid B_{p-i})$
can be obtained only from ACNF.

$\Rightarrow$ Herbrand Stickelberger's th.

$\Leftarrow$ Ribet.

Remark 1. Why X ?

Iwasawa's idea : analogy with function fields

C : curve / $\mathbb{F}_\ell$ $(\ell \neq p)$

$$\begin{array}{ccc} C & \longrightarrow & C_{\overline{\mathbb{F}}_\ell} \\ \downarrow & & \downarrow \\ \mathbb{F}_\ell & \longrightarrow & \overline{\mathbb{F}}_\ell \end{array}$$

$\mathrm{Pic}^0(C_{\overline{\mathbb{F}}_\ell})[p^\infty] = (\mathbb{Q}_p/\mathbb{Z}_p)^{2g}$ (g : genus)

$\Big\}$ analogy ?

the action of the Frobenius on $\mathrm{Pic}^0(C_{\overline{\mathbb{F}}_\ell})[p^\infty]$ gives the zeta fct of C

$\Big\}$ analogy ?

MC $\longleftrightarrow$ X $\longleftrightarrow$ $\varprojlim A_{k_n}$

$\lambda = \dim(X \otimes \mathbb{Q}_p) \overset{?}{\sim} 2g$

$\mu = 0$?

2. Vandiver's conj says $X^{[j]} = 0$ for all even j.

(no theoretical evidence)

If you want to check $X^{[j]} = 0$, it is enough to check $A_k^{[j]} = 0$ for p dividing the Bernoulli number B_j.

So we can check $X^{[j]} = 0$ for small j.

We can also check $X^{[p-3]} = 0$ by using computation of a certain K-group.

Basic properties of modular forms (cf. Serre "Cours d'arithmétique")

$\mathcal{H} = \{ z \in \mathbb{C} \mid \mathrm{Im}\, z > 0 \}$

$k \in \mathbb{Z}_{>0}$

$f : \mathcal{H} \longrightarrow \mathbb{C}$ holomorphic fct is called a modular form of $SL_2(\mathbb{Z})$ (level 1) and weight k if

1) $f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$ for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$

In particular $f(z+1) = f(z)$, $q = e^{2\pi i z}$

2) $f(z) = \sum_{n=0}^{\infty} a_n q^n$ (holomorphic at $i\infty$)

$M_k(\mathbb{C}) = \{$ level 1, wt k modular forms $\}$

☆ $M_k(\mathbb{C})$ is a finite dimensional $\mathbb{C}$-vct sp, and

$$\dim M_k(\mathbb{C}) = \begin{cases} 0 & k: \text{odd} \\ \left[\frac{k}{12}\right] & k \equiv 2 \pmod{12} \\ \left[\frac{k}{12}\right] + 1 & k \not\equiv 2 \pmod{12} \quad k: \text{even} \end{cases}$$

Example : Eisenstein series

$$E_k = \sum_{\substack{(m,n) \neq (0,0) \\ \in \mathbb{Z}\times\mathbb{Z}}} \frac{1}{(mz+n)^k}$$

$$= 2 \cdot \frac{(2\pi i)^k}{(k-1)!} \cdot \underbrace{\left(\frac{1}{2} \zeta(1-k) + \sum_{n=1}^{\infty} \sigma_{k-1}(n)\, q^n \right)}_{\| \; G_k} \in M_k(\mathbb{C})$$

$$\zeta(1-k) = -\frac{B_k}{k} \qquad \sigma_{k-1}(n) = \sum_{d \mid n} d^{k-1}$$

$$\Delta = q \prod_{n=1}^{\infty} (1-q^n)^{24} = \sum_{n=1}^{\infty} \tau(n)\, q^n = q - 24 q^2 + 252 q^3 + \cdots$$

$\Delta \in M_{12}(\mathbb{C})$

$\star$ $\bigoplus M_k(\mathbb{C}) = \mathbb{C}[G_4, G_6]$

$M_k(\mathbb{Z}) = \{ \sum a_n q^n \mid a_n \in \mathbb{Z} \}$

For a ring R, $M_k(R) = M_k(\mathbb{Z}) \otimes R$.

$\Delta \in M_{12}(\mathbb{Z})$

$G_k \in M_k(\mathbb{Q})$

Hecke operator

For a prime number ℓ, $T_\ell : M_k(\mathbb{C}) \to M_k(\mathbb{C})$ is defined by

$$T_\ell\left(\sum a_n q^n\right) = \sum b_n q^n$$

$$b_n = \begin{cases} a_{n\ell} & \ell \nmid n \\ a_{n\ell} + \ell^{k-1} a_{\frac{n}{\ell}} & \ell \mid n \end{cases}$$

$f = \sum a_n q^n$ is a (normalized) eigenform if $a_1 = 1$ and $T_\ell \cdot f = a_\ell \cdot f$ for all ℓ.

- G_k, Δ are eigenforms
- $M_k(\mathbb{C})$ has a basis consisting of eigenforms.

$S_k(\mathbb{C}) = \{ \sum a_n q^n \in M_k(\mathbb{C}) \mid a_0 = 0 \}$ cusp forms

$M_k(\mathbb{C}) = \mathbb{C} \cdot G_k \oplus S_k(\mathbb{C})$

Th (Deligne) Suppose $f = \sum_{n=1}^{\infty} a_n q^n \in S_k(\mathbb{C})$ is a normalized eigenform

$F = \mathbb{Q}(\{a_n \mid n \geq 1\})$ finite over $\mathbb{Q}$

For any prime number p, there exists an irreducible p-adic representation

$$\rho_f : G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(F_{\mathfrak{p}}) \qquad (\mathfrak{p} \mid p)$$

s.t.

1) ρ_f is unramified outside p [ρ_f is crystalline at p]

2) For a prime $\ell \neq p$, $\mathrm{Tr}(\rho_f(\mathrm{Frob}_\ell)) = a_\ell$

$\det(\rho_f(\mathrm{Frob}_\ell)) = \ell^{k-1}$

Pf cohomology of Kuga-Sato variety

Th (Mazur Wiles) If f is ordinary at p (a_p is prime to p), the restriction of ρ_f to $G_{\mathbb{Q}_p} = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ satisfies

$$\rho_f|_{G_{\mathbb{Q}_p}} \sim \begin{pmatrix} \kappa^{k-1}\varepsilon_1 & * \\ 0 & \varepsilon_2 \end{pmatrix}$$

conjugate

κ : cyclotomic char $G_{\mathbb{Q}_p} \longrightarrow \mathbb{Z}_p^\times$

$\varepsilon_1, \varepsilon_2$: unram char.

Construction of unram ext.

$k = 12 \quad p = 691$

$\rho_\Delta : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{Z}_p)$

$$\sigma \longmapsto \begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix}$$

We take $\rho_\Delta|_{G_{\mathbb{Q}_p}}$ to be of the form above (especially $c|_{G_{\mathbb{Q}_p}} = 0$)

Since ρ_Δ is irreducible, $c \neq 0$, so changing the basis, we may assume $c \bmod p \neq 0$.

Consider

$\rho_\Delta \bmod p : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{F}_p)$

Ramanujan's congruence

$$\tau(n) \equiv \sigma_{11}(n) \pmod{691}$$

Pf. $G_{12} - \left(\frac{G_6}{\frac{1}{2}\zeta(-5)}\right)^2 \cdot \frac{1}{2}\zeta(-11) \in S_{12}(\mathbb{C}) = \mathbb{C}\cdot\Delta$

$\left(\frac{G_6}{\frac{1}{2}\zeta(-5)}\right)^2 \cdot \frac{1}{2}\zeta(-11) = \alpha\cdot\Delta$

$p = 691 \nmid \zeta(-5)$ $\quad p \mid \zeta(-11) = \frac{B_{12}}{12}$

$\alpha \in \mathbb{Z}_{(p)}$ $\quad \alpha \equiv 1 \pmod{p}$ $\quad$ [determine α]

$G_{12} \equiv \Delta \pmod{p}$

This congruence implies

$$\mathrm{Tr}(\rho_\Delta(\mathrm{Frob}_\ell)) \equiv 1 + \ell^{11} \pmod{p}$$

$$\det(\rho_\Delta(\mathrm{Frob}_\ell)) \equiv \ell^{11} \pmod{p}$$

Namely, $\rho_\Delta \bmod p$ is reducible.

$$\rho_\Delta \bmod p \equiv \begin{pmatrix} \kappa^{11} & 0 \\ c & 1 \end{pmatrix} \bmod p$$

$c \neq 0$

Suppose L_0 is the field corresponding to $\ker(\rho_\Delta \bmod p)$.

$L_0 \supset \mathbb{Q}(\mu_p)$ $\quad$ (11 is prime to $69\cdots$)

and $L_0/\mathbb{Q}(\mu_p)$ is cyclic of deg p ($\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ is of order p)

Every prime above ℓ $(\neq p)$ is unramified in $L_0/\mathbb{Q}(\mu_p)$

(because of the construction, Th of Deligne)

and the prime above p is also unramified

(because $c|_{G_{\mathbb{Q}_p}} = 0$)

Hence, $L_0/\mathbb{Q}(\mu_p)$ is unramified everywhere.

Furthermore, $\Delta = Gal(\mathbb{Q}(\mu_p)/\mathbb{Q})$ acts on $Gal(L_0/\mathbb{Q}(\mu_p))$ via

$$k^{-11} \bmod p = \omega^{-11} = \omega^{p-12}$$

Hence, $A_k^{[p-12]} \neq 0$

Namely, using $p \mid \zeta(-11) = \frac{B_{12}}{12}$, we have got $A_k^{[p-12]} \neq 0$.

General case, suppose $p \mid B_k$.

Then, $G_k \bmod p \in S_k(\bar{\mathbb{F}}_p)$

There is a normalized eigenform f whose coefficients are in $\mathcal{O}_{\mathcal{F}_f}$ s.t. $f \bmod \pi = G_k \bmod p$

π : a prime element of $\mathcal{O}_{\mathcal{F}_p}$

$$\rho_f : G_{\mathbb{Q}} \longrightarrow GL_2(\mathcal{O}_{\mathcal{F}_p})$$

$$\downarrow \bmod \pi$$

$$\text{reducible} \nearrow \quad GL_2(\bar{\mathbb{F}}_q)$$

We can proceed as before.

Th (Herbrand Ribet) For odd i s.t. $1 < i < p-1$,

$$A_K^{[i]} \neq 0 \iff p \mid B_k \quad \text{where } k = p - i$$

What is the meaning of $\operatorname{ord}_p B_k$, or equivalently $\operatorname{ord}_p \zeta(1-k)$?

Theorem (Cor. of the MC)

$$\#\left(X^{[i]} / (\gamma - \kappa^{1-k}(\gamma))\, X^{[i]}\right) = \#\left(\mathbb{Z}_p / \zeta(1-k)\,\mathbb{Z}_p\right)$$

(γ: generator of $\Gamma = \mathrm{Gal}(K_\infty / K)$

$\kappa : \mathcal{G} \longrightarrow \mathbb{Z}_p^\times$ cyclotomic char)

Rem $LHS \simeq H^2_{\text{ét}}(\mathbb{Z}[\tfrac{1}{p}], \mathbb{Z}_p(k))$

For general even $k > 0$, $\dfrac{\#H^2(\mathbb{Z}[\frac{1}{p}],\ \mathbb{Z}_p(k))}{\#H^1(\mathbb{Z}[\frac{1}{p}],\ \mathbb{Z}_p(k))} = \operatorname{ord}_p \zeta(1-k)$

"We can construct sufficiently many unramified ext. from modular forms"

Hecke ring

$$T_\ell|_{S_k(\mathbb{Z})} \in \mathrm{End}(S_k(\mathbb{Z}))$$

$$\mathbb{T} = \mathbb{Z}[\,T_\ell \mid \ell : \text{prime number}\,] \subset \mathrm{End}(S_k(\mathbb{Z}))$$

Suppose $p^n \| B_k$ i.e. $p^n \| \prod(1-\ell^{k-1})$.

Then $G_k \bmod p^n \in S_k(\mathbb{Z}/p^n)$ and we have a ring hom

$$\mathbb{T} \longrightarrow \mathbb{Z}/p^n$$

$$T_\ell \longmapsto 1+\ell^{k-1}$$

Define I by $I = (\,T_\ell - (1+\ell^{k-1}) \mid \ell : \text{prime number}\,) \subset \mathbb{T}$

(Eisenstein ideal)

Prop. $\mathbb{T}/I \simeq \mathbb{Z}/p^n$.

Put $\mathfrak{m} = (p, I)$ which is the maximal ideal containing I.

$T_E := \mathbb{T}_{\mathfrak{m}}$ ($\mathfrak{m}$-adic completion of $\mathbb{T}$)

By using ρ_f, we have

$$\rho_{T_E} : G_{\mathbb{Q}} \longrightarrow GL_2(T_E \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$$

- unram outside p
- $\mathrm{Tr}(\rho_{T_E}(\mathrm{Frob}_\ell)) = T_\ell \quad (\ell \nmid p)$
- $\det(\quad) = \ell^{k-1}$
- $\rho_{T_E}|_{G_{\mathbb{Q}_p}} = \begin{pmatrix} \xi^{k-1}\varepsilon_1 & * \\ 0 & \varepsilon_2 \end{pmatrix}$

Rem We do not know whether $\rho_{T_E} : G_{\mathbb{Q}} \to GL_2(T_E)$ exists or no

It is better to consider $G_{\mathbb{Q}} \to \mathrm{Aut}$ (a certain $\mathbb{Z}_p$-coeff. cohomology) for further study.

Put $\mathfrak{I} = I \cdot T_E$

$\star$ $a(\sigma) \equiv k^{k-1}(\sigma)$ $\quad d(\sigma) \equiv 1 \pmod{\mathfrak{I}}$

Pf Take σ_c s.t $\rho(\sigma_c) \equiv \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. Then

$$a(\sigma) \equiv \frac{1}{2}(\mathrm{Tr}\,\rho(\sigma) - \mathrm{Tr}\,\rho(\sigma\sigma_c))$$
$$\equiv \frac{1}{2}(1 + k^{k-1}(\sigma) - (1 - k^{k-1}(\sigma)))$$
$$= k^{k-1}(\sigma)$$

For $d(\sigma)$, a similar computation.

Let I_B, I_C be the ideals of $T_E \otimes \mathbb{Q}_p$ generated by the image of b and c, respectively.

I_B and I_C depend on the choice of the basis, but

Lemma. $I_B \cdot I_C = \mathfrak{I}$

$\subset$ $a(\sigma\tau) = a(\sigma)a(\tau) + b(\sigma)c(\tau)$

$a(\sigma\tau) \equiv k^{k-1}(\sigma\tau) \equiv a(\sigma)a(\tau) \pmod{\mathfrak{I}}$,

so $b(\sigma)c(\tau) \equiv 0 \pmod{\mathfrak{I}}$

$\supset$ slightly complicated.

Suppose that $V = (T_E \otimes \mathbb{Q}_p)e_1 \oplus (T_E \otimes \mathbb{Q}_p)e_2$ is the module corresponding to the representation ρ_{T_E}.

Put $M = (T_E/\mathfrak{I})e_1 \oplus (I_C/\mathfrak{I}I_C)e_2$

which is a $G_{\mathbb{Q}}$-module.

$$\begin{pmatrix} c(\sigma) \in I_C \\ b(\sigma) I_C \subset \mathfrak{I} T_E \end{pmatrix}$$

$$0 \to (I_C/\mathfrak{I}I_C)e_2 \to M \to (T_E/\mathfrak{I})e_1 \to 0$$

exact as $G_{\mathbb{Q}}$-modules.

Let L' be the field corresponding to the kernel of the action of $G_{\mathbb{Q}}$ on M.

- $L'(\mu_{p^\infty}) / \mathbb{Q}(\mu_{p^\infty})$ is unramified everywhere
- $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ acts on $\mathrm{Gal}(L'(\mu_{p^\infty}) / \mathbb{Q}(\mu_{p^\infty}))$ via κ^{1-k}

($G_{\mathbb{Q}}$ acts on $(I_c/\mathfrak{d} I_c)\cdot e_2$ trivially $(d \equiv 1)$

and

$G_{\mathbb{Q}}$ acts on $(T_E/\mathfrak{d})\, e_1$ via κ^{k-1} $(a \equiv \kappa^{k-1})$)

Hence $X^{[i]}/(\gamma - \kappa^{1-k}(\gamma)) \longrightarrow \mathrm{Gal}(L'(\mu_{p^\infty}) / \mathbb{Q}(\mu_{p^\infty}))$

By construction, $\mathrm{Gal}(L'(\mu_{p^\infty}) / \mathbb{Q}(\mu_{p^\infty})) \simeq I_c/\mathfrak{d} I_c$.

By the Lemma below, $\# I_c/\mathfrak{d} I_c \geq p^n$, so we have constructed sufficiently many unramified p extensions

<u>Lemma.</u> Suppose J is a f.g. T_E module $\subset T_E \otimes_{\mathbb{Z}_l} \mathbb{Q}_p$ s.t.

$$T_E \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = T_E \otimes_{\mathbb{Z}_l} \mathbb{Q}_p$$

Then, $\# J/\mathfrak{d} J \geq \# T_E/\mathfrak{d} = p^n$.

<u>Fitting ideal</u>

R : comm ring

M : R-module with finite presentation

generator $e_1 \cdots e_n$

relation $\sum_{i=1}^{n} a_{ij} e_i \sim \quad j = 1, 2, \cdots$

The ideal generated by all $n \times n$ minors of $A = (a_{ij})$ is called the Fitting ideal of M, and denoted by $\mathrm{Fitt}_R(M)$.

(This does not depend on the choice of A.)

★ For an ideal I of R, $\mathrm{Fitt}_{R/I}(M/IM) = \mathrm{Fitt}_R(M)$ mod I.
from the definition of Fitt.

Proof of the Lemma $\mathrm{Fitt}_{T_E \otimes \mathbb{Q}_p}(J \otimes \mathbb{Q}_p) = 0$

$\Rightarrow \mathrm{Fitt}_{T_E}(J) = 0$

$\Rightarrow \mathrm{Fitt}_{T_E/\mathfrak{a}T_E}(J/\mathfrak{a}J) = 0$ ($T_E/\mathfrak{a}T_E \simeq \mathbb{Z}/p^n$)

$\Rightarrow \mathrm{Fitt}_{\mathbb{Z}_p}(J/\mathfrak{a}J) \subset (p^n)$

$\Rightarrow \# J/\mathfrak{a}J \geq p^n$

(For a f.g. torsion $\mathbb{Z}_p$-module M, $\mathrm{Fitt}_{\mathbb{Z}_p}(M) = (\#M)$) //

A proof of the Main Conjecture (Mazur-Wiles, Wiles)

A similar argument over $k_\infty = \mathbb{Q}(\mu_{p^\infty})$ as above using Hida theory (cf [W], [O]).

$\mathcal{O}$: the ring of integers of a local field over $\mathbb{Q}_p$.
$\Lambda_{\mathcal{O}} = \mathcal{O}[[T]]$
We call $f = \sum a_n q^n$ ($a_n \in \Lambda_{\mathcal{O}}$) a Λ-adic form if for any $k \in \mathbb{Z}_{\geq 2}$ and any $\zeta \in \mu_{p^\infty}$,
$f_{k,\zeta} = \sum c_{k,\zeta}(a_n) q^n$ is a modular form of level Np^r and of weight k
where $c_{k,\zeta} : \Lambda_{\mathcal{O}} \to \mathcal{O}[\zeta]$ is a ring hom $T \mapsto \zeta\kappa(\gamma)^{k-2} - 1$
and p^r: the order of ζ.

Suppose i : odd s.t. $1 < i < p-1$ and $k = p - i$.

We consider the Eisenstein series (Λ-adic form)

$$G_k = \frac{1}{2} g_k(T) + \sum_{n=1}^{\infty} \left(\sum_{d|n} \omega^{k-2}(d) (1+T)^{i(d)} d \right) q^n$$

where $g_k(T)$ is the power series s.t. $g_k((\kappa(\gamma)^s - 1)) = L_p(-1-s, \omega^k)$

and $i(d) \in \mathbb{Z}_p$ is defined by $\frac{d}{\omega(d)} = \kappa(\gamma)^{i(d)}$

We can define Hecke operators T_ℓ on Λ-adic forms,

and Hecke ring $\mathbb{T}$.

The Eisenstein ideal I is the ideal gen by $T_\ell - (1 + \langle \omega^{k-2} \rangle(\ell) \ell)$

Wiles proved $\mathbb{T}/I \simeq \mathbb{Z}_p[[T]]/(g_k(T))$.

Suppose that $f = \sum a_n q^n$ is an ordinary Λ-adic cusp form of level p-power which is an eigenform for Hecke operators ($a_n \in \Lambda_{\mathcal{O}}$).

Hida constructed a representation

$$\rho_f : G_{\mathbb{Q}} \longrightarrow GL_2(\mathrm{Frac}\,\Lambda_{\mathcal{O}})$$

which is unramified outside p and $\mathrm{Tr}(\rho_f(\mathrm{Frob}_\ell)) = a_\ell$ $(\ell \neq p)$.

whose restriction to $G_{\mathbb{Q}_p}$ is reducible as before.

We get extension

$$0 \longrightarrow (I_C / \mathfrak{J} I_C) e_2 \longrightarrow M \longrightarrow (T_E / \mathfrak{J}) e_1 \longrightarrow 0$$

by a similar method as above. This extension gives a Galois extension L'_∞ / k_∞ which is unramified everywhere and on which Δ acts via ω^i.

Further, by the same method, we obtain

$$\mathrm{Fitt}_{\mathbb{Z}_p[[\mathrm{Gal}(k_\infty/\mathbb{Q})]]}^{[i]} (\mathrm{Gal}(L'/k_\infty)) \subset (\theta_{k_\infty}^{[i]})$$

Since we have surjective $X^{[i]} \longrightarrow \mathrm{Gal}(L'/k_\infty)$, the above implies

$$\mathrm{char}(X^{[i]}) = \mathrm{Fitt}(X^{[i]}) \subset \mathrm{Fitt}(\mathrm{Gal}(L'/k_\infty)) \subset (\theta_{k_\infty}^{[i]})$$

Thus, by the argument using the analytic class number formula, we get $\mathrm{char}(X^{[i]}) = (\theta_{K_\infty}^{[i]})$.

References

[MW] Mazur and Wiles, Class fields of abelian extensions of $\mathbb{Q}$, Invent math 76 (1984), 179–330.

[O] Ohta, Ordinary p-adic etale cohomology groups attached to towers of elliptic curves, Compos Math 115 (1999), 241–301, II Math. Ann. 318 (2000), 557–583

[W] Wiles, The Iwasawa conjecture for totally real fields, Ann of Math 131 (1990), 493–540.

Euler system of Gauss sums

✡ Euler system of cyclotomic units is easier. [CR1]

(cf. Rubin Appendix to "Cyclotomic Fields" by S. Lang
Rubin "Euler systems")

Stickelberger element

For a positive integer $N>0$,

$$\theta_{\mathbb{Q}(\mu_N)} = \sum_{a=1}^{N} \left(\frac{1}{2} - \frac{a}{N}\right) \sigma_a^{-1} \in \mathbb{Q}[\mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})]$$

$$\mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \simeq (\mathbb{Z}/N\mathbb{Z})^\times$$

$$\sigma_a \longleftrightarrow a.$$

For a finite abelian extension $F/\mathbb{Q}$ with conductor N, we define $\theta_F \in \mathbb{Q}[\mathrm{Gal}(F/\mathbb{Q})]$ to be the image of $\theta_{\mathbb{Q}(\mu_N)}$ by the restriction map.

$$\left(\theta_F = \sum_{\sigma \in \mathrm{Gal}(F/\mathbb{Q})} \zeta(0,\sigma)\sigma^{-1} \qquad \zeta(s,\sigma) = \sum_{(n,F/\mathbb{Q})=\sigma} \frac{1}{n^s} \right)$$

Stickelberger's theorem (1890)

If $\alpha \in \mathrm{Ann}_{\mathbb{Z}[\mathrm{Gal}(F/\mathbb{Q})]}(\mu_F)$, then $\alpha\theta_F \in \mathbb{Z}[\mathrm{Gal}(F/\mathbb{Q})]$ and

$$(\alpha\theta_F) \cdot Cl_F = 0$$

Pf. Prime factorization of Gauss sums.

(cf. Washington "Cyclotomic Fields" Chap. 6)

We fix $r \geq 0$ and consider $k_r = \mathbb{Q}(\mu_{p^{r+1}})$

$\mathcal{M} = \{ F' \mid F'/\mathbb{Q}$ is a finite abelian p-extension and the conductor of F' is prime to $p \}$

$\mathcal{M}_{k_r} = \{ F' \cdot k_r \mid F' \in \mathcal{M} \}$.

We fix an odd i s.t. $1 < i < p-1$, and for a $\mathbb{Z}_p[\Delta]$-module M, if no confusion arises, we simply write M for the ω^i-component $M^{[i]}$.
For $x \in M$, $e_{\omega^i} x \in M^{[i]}$ $\left(e_{\omega^i} = \frac{1}{p-1} \sum_{\sigma \in \Delta} \omega^i(\sigma)\sigma^{-1}\right)$ is abbreviated as x.

For example, for $F \in \mathcal{M}_{k_r}$, $A_F^{[i]} = (Cl_F \otimes \mathbb{Z}_p)^{[i]}$ is a $\mathbb{Z}_p[\mathrm{Gal}(F/k_r)]$-module, and $e_{\omega^i} \theta_F$ is in $\mathbb{Z}_p[\mathrm{Gal}(F/k_r)]$ because we assumed $i \neq 1$. Stickelberger's theorem says $(e_{\omega^i} \theta_F) \cdot A_F^{[i]} = 0$. We write this relation just as

$$\theta_F \cdot A_F = 0 \qquad \text{if no confusion arises.}$$

Suppose that $F \in \mathcal{M}_{k_r}$ and ℓ is a prime number which splits completely in F, and $\mathfrak{l}_F$ is a prime of F above ℓ.
Let Div_F be the divisor group, namely the group of fractional ideals (we write the group law additively). The prime factorization of elements in F gives a map $\mathrm{div} : F^\times \longrightarrow \mathrm{Div}_F$, and we have an exact sequence $0 \longrightarrow E_F \longrightarrow F^\times \xrightarrow{\mathrm{div}} \mathrm{Div}_F \longrightarrow Cl_F \longrightarrow 0$ where E_F is the unit group.
We consider an exact sequence

$$0 \longrightarrow (E_F \otimes \mathbb{Z}_p)^{[i]} \longrightarrow (F^\times \otimes \mathbb{Z}_p)^{[i]} \xrightarrow{\mathrm{div}} (\mathrm{Div}_F \otimes \mathbb{Z}_p)^{[i]} \longrightarrow A_F^{[i]} \longrightarrow 0.$$

Since i is odd and $i \neq 1$, $(E_F \otimes \mathbb{Z}_p)^{[i]} = 0$, hence there is a unique element $g_{F,\mathfrak{l}_F} \in (F^\times \otimes \mathbb{Z}_p)^{[i]}$ s.t. $\mathrm{div}(g_{F,\mathfrak{l}_F}) = (e_{\omega^i} \theta_F) \cdot \mathfrak{l}_F$.

ϑ_{F,ρ_F} is essentially the Gauss sum.

Note We can define this element for a CM field F over an arbitrary totally real field (cf. [K])

Suppose M is a subfield of F. Then, we have

$$N_{F/M}(\vartheta_{F,\rho_F}) = \prod_{\substack{\ell \mid \mathrm{cond}(F) \\ \ell \nmid \mathrm{cond}(M)}} (1 - \mathrm{Frob}_\ell^{-1}) \cdot \vartheta_{M,\rho_M}$$

where $\mathrm{Frob}_\ell \in \mathrm{Gal}(M/\mathbb{Q})$ is the Frobenius of ℓ, ρ_M is the prime below ρ_F, $\mathrm{cond}(F)$ and $\mathrm{cond}(M)$ are the conductors of F and M.

This is the norm property of Euler systems.

This follows from the distribution property of Gauss sums,

or follows from that of Stickelberger elements

$$c_{F/M}(\theta_F) = \prod_{\substack{\ell \mid \mathrm{cond}(F) \\ \ell \nmid \mathrm{cond}(M)}} (1 - \mathrm{Frob}_\ell^{-1}) \cdot \theta_M$$

We fix sufficiently large $N > 0$ (especially $N > r+1$, $N > 2\,\mathrm{ord}_p(\#A_{K_r}^{[i]})$).

$\mathcal{S} = \{ \ell : \text{prime number} \mid \ell \equiv 1 \pmod{p^N} \}$

$\mathcal{T} = \{ n : \text{square free integer} > 0 \mid \ell \mid n \Rightarrow \ell \in \mathcal{S} \}$.

For $\ell \in \mathcal{S}$, define ℓ_p to be the maximal p-power dividing $\ell - 1$, namely

$\ell - 1 = \ell_p \cdot u$ s.t. ℓ_p is a power of p and $p \nmid u$.

We denote by k_ℓ the subfield of $\mathbb{Q}(\mu_\ell)$ s.t. $[k_\ell : \mathbb{Q}] = \ell_p$.

We fix a generator σ_ℓ of $\mathrm{Gal}(k_\ell/\mathbb{Q})$, and put

$$N_\ell = \sum_{i=0}^{\ell_p - 1} \sigma_\ell^{\,i}, \qquad D_\ell = \sum_{i=0}^{\ell_p - 1} i \cdot \sigma_\ell^{\,i} \in \mathbb{Z}[\mathrm{Gal}(k_\ell/\mathbb{Q})].$$

The fundamental equation is

$$(\sigma_\ell - 1) D_\ell = \ell_p - N_\ell .$$

For $n \in \mathcal{J}$, define $k_n = k_{\ell_1} \cdots k_{\ell_s}$ where $n = \ell_1 \cdots \ell_s$.

Put $N_n = N_{\ell_1} \cdots N_{\ell_s}$ and $D_n = D_{\ell_1} \cdots D_{\ell_s} \in \mathbb{Z}[\mathrm{Gal}(k_n/\mathbb{Q})]$.

For $n \in \mathcal{J}$, define $F_n = k_r \cdot k_n$. Then $F_n \in \mathcal{M}_{k_r}$.

Suppose ℓ is a prime number which splits in F_n. We take a prime $\mathfrak{l}_{F_n}$ above ℓ.

<u>Lemma.</u> $D_n \, g_{F_n, \mathfrak{l}_{F_n}} \in \left(\left(F_n^\times / (F_n^\times)^{p^N} \right)^{[i]} \right)^{\mathrm{Gal}(F_n/k_r)}$

<u>Pf</u>. Induction on s. Suppose $\ell \mid n$.

$$\begin{aligned}
(\sigma_\ell - 1) D_n \, g_{F_n, \mathfrak{l}_{F_n}} &\equiv - N_\ell \cdot D_{\frac{n}{\ell}} \cdot g_{F_n, \mathfrak{l}_{F_n}} \\
&= - \frac{D_n}{\ell} \left(1 - \varphi_\ell^{-1} \right) g_{F_{\frac{n}{\ell}}, \mathfrak{l}_{F_{\frac{n}{\ell}}}} \\
&\equiv 0 \pmod{p^N} \quad \text{(by induction)}
\end{aligned}$$

Since σ_ℓ's generate $\mathrm{Gal}(F_n/k_r)$, we get the conclusion.

From the isomorphism $\left(k_r^\times / (k_r^\times)^{p^N} \right)^{[i]} \xrightarrow{\sim} \left(\left(F_n^\times / (F_n^\times)^{p^N} \right)^{[i]} \right)^{\mathrm{Gal}(F_n/k_r)}$,

there is a unique element $k_{n, \mathfrak{l}_{F_n}}$ s.t. $k_{n, \mathfrak{l}_{F_n}} \mapsto D_n \, g_{F_n, \mathfrak{l}_{F_n}}$.

If no confusion arises, we simply write $k_{n, \mathfrak{l}}$ for $k_{n, \mathfrak{l}_{F_n}}$.

By the same method, we can show that $\exists!\ \delta(n) \in \mathbb{Z}_p[\mathrm{Gal}(K_n/K)]$ s.t.

$$D_n \theta_{F_n}^{[i]} = N_n \cdot \delta(n).$$

Lemma $\mathrm{div}(\kappa_{n,p}) = \delta(n) \mathfrak{p}_{K_n} + (\text{a divisor whose support is primes dividing } n)$ mod P^N

where $\mathfrak{p}_{K_n}$ is the prime of K_n below $\mathfrak{p}_{F_n}$.

Pf From definition.

Let $\ell \in \mathcal{L}$. Define $W_\ell = \ker\left((K_r^\times \otimes \mathbb{Z}_p)^{[i]} \xrightarrow{\mathrm{div}_\ell} \bigoplus_{\mathfrak{p}\mid\ell} \mathbb{Z}_p\right)$, and

$$\varphi_\ell : W_\ell \longrightarrow \left(\bigoplus_{\mathfrak{p}\mid\ell} k(\mathfrak{p})^\times / (k(\mathfrak{p})^\times)^{p^N}\right)^{[i]} \quad (k(\mathfrak{p}) : \text{the residue field of } \mathfrak{p} = \mathcal{O}_{K_r}/\mathfrak{p})$$

by $\quad x \longmapsto (x \bmod \mathfrak{p})$

Since ℓ splits in K_r, $\left(\bigoplus_{\mathfrak{p}\mid\ell} k(\mathfrak{p})^\times / (k(\mathfrak{p})^\times)^{p^N}\right)^{[i]} \underset{(*)}{\simeq} \mathbb{Z}/p^N[\mathrm{Gal}(K_r/K)]$.

Prop. Assume that ℓ splits in F_n, and a prime $\mathfrak{l}_{K_r}$ of K_r above ℓ is in the same class as $\mathfrak{p}_{K_r}$ in $Cl_{K_r}(\mathfrak{p}_{F_n} \mid \mathfrak{p}_{K_r})$.

Then, taking isomorphism $(*)$ suitably,

$$\varphi_\ell(\kappa_{n,p}) \equiv \delta_{n\ell} \pmod{\delta_n}.$$

cf. [R2] Th 2.4, [K] Prop. 8.7.

Stickelberger's congruence.

The case $r=0$, namely $k_r = k = \mathbb{Q}(\mu_p)$.

Suppose that $A_k^{[i]} \simeq \mathbb{Z}/p^{n_1} \oplus \cdots \oplus \mathbb{Z}/p^{n_r}$.

and $C_1, \cdots C_r$ are generators.

$\mathcal{Q}_i := \{ \ell \in \mathcal{Q} \mid$ a prime ℓ_k above ℓ is in the class $C_i \}$

$\mathcal{Q} := \bigcup_{i=1}^{r} \mathcal{Q}_i$.

$$(\mathrm{Div}_k)' = \bigoplus_{\ell \in \mathcal{Q}} \left(\mathbb{Z}_p[\mathrm{Gal}(k/\mathbb{Q})] \cdot \ell_k\right)^{[i]} \subset \left(\mathrm{Div}_k \otimes \mathbb{Z}_p\right)^{[i]}$$

$$\mathcal{K} = \{ x \in (k^\times \otimes \mathbb{Z}_p)^{[i]} \mid \mathrm{div}(x) \in (\mathrm{Div}_k)' \} \subset (k^\times \otimes \mathbb{Z}_p)^{[i]}$$

We have a commutative diagram of exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{K} & \longrightarrow & (\mathrm{Div}_k)' & \longrightarrow & A_k^{[i]} & \longrightarrow & 0 \\ & & f \downarrow & & \downarrow g & & \| & & \\ 0 & \longrightarrow & \mathbb{Z}_p^r & \xrightarrow{h} & \mathbb{Z}_p^r & \longrightarrow & A_k^{[i]} & \longrightarrow & 0 \end{array}$$

where g is the map defined by $\ell_k \longmapsto (0 \cdots 0 \overset{i}{1} 0 \cdots 0)$ $\forall \ell \in \mathcal{Q}_i$,

f is induced by g, and h corresponds to

$$\begin{pmatrix} p^{n_1} & & 0 \\ & \ddots & \\ 0 & & p^{n_r} \end{pmatrix}.$$

Take $\wp_1 \in \mathcal{Q}_1$, and consider $g_{k,\wp_1,k} \in \mathcal{K}$.

Take $\ell_1 \in \mathcal{Q}_1$ s.t. $\mathrm{pr}_1 \circ f = u\, g_{\ell_1}$ with $u \in \mathbb{Z}_p^\times$.

This is possible by Chebotarev density.

Then, $f(g_{k,\wp_1,k}) = \begin{pmatrix} u\delta_{\ell_1} + c\theta_k^{[i]} \\ * \\ \vdots \\ * \end{pmatrix}$, $g(\mathrm{div}(g_{k,\wp_1,k})) = \begin{pmatrix} \theta_k^{[i]} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$

for some $c \in \mathbb{Z}_p$.

Therefore, $u\delta_{\ell_1} \cdot p^{n_1} = (1 - p^{n_1} c)\theta_k^{[i]}$, and $\mathrm{ord}_p(\delta_{\ell_1}) + n_1 = \mathrm{ord}_p(\theta_k^{[i]})$

Next, we take $\mathfrak{p}_2 \in \mathfrak{Q}_2$ which splits in $F_{\mathfrak{l}_1}$, and consider $\kappa_{\mathfrak{l}_1,\mathfrak{p}_2}$. We take a (good) lifting $\widetilde{\kappa}_{\mathfrak{l}_1\mathfrak{p}_2} \in \mathcal{K}$.

Take $\mathfrak{l}_2 \in \mathfrak{Q}_2$ which splits in $F_{\mathfrak{l}_1}$ s.t. $\mathrm{pr}_2 \circ f = u' \varphi_{\mathfrak{l}_2}$ with $u' \in \mathbb{Z}_p^\times$

(This is possible by Chebotarev density.)

Then, $f(\widetilde{\kappa}_{\mathfrak{l}_1,\mathfrak{p}_2}) = \begin{pmatrix} * \\ u'\delta_{\mathfrak{l}_1\mathfrak{l}_2} + c'\delta_{\mathfrak{l}_1} \\ * \\ \vdots \\ * \end{pmatrix}$, $g(\mathrm{div}(\widetilde{\kappa}_{\mathfrak{l}_1,\mathfrak{p}_2})) = \begin{pmatrix} * \\ \delta_{\mathfrak{l}_1} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$

for some $c' \in \mathbb{Z}_p$.

Therefore, $u' \delta_{\mathfrak{l}_1\mathfrak{l}_2} \cdot p^{n_2} = (1 - p^{n_2} c') \delta_{\mathfrak{l}_1}$

and $\mathrm{ord}_p(\delta_{\mathfrak{l}_1\mathfrak{l}_2}) + n_2 = \mathrm{ord}_p(\delta_{\mathfrak{l}_1})$

$\vdots$

$$\mathrm{ord}_p(\delta_{\mathfrak{l}_1 \cdots \mathfrak{l}_r}) + n_1 + \cdots + n_r = \mathrm{ord}_p(\theta_k^{[i]})$$

Thus, $n_1 + \cdots + n_r \leq \mathrm{ord}_p(\theta_k^{[i]})$

$$\# A_k^{[i]} \leq \#(\mathbb{Z}_p / \theta_k^{[i]}) = \# \mathbb{Z}_p / \beta_{1,\omega^{-i}}$$

References

[R1] Rubin, The main conjecture, Appendix to "Cyclotomic Fields" by S. Lang, GTM 121, Springer, 397–419.

[R2] Rubin, Kolyvagin's system of Gauss sums in "Arith. Alg. Geometry" van der Geer eds, Progress in Math 89, Birkhäuser, 309–324.

[K] Kurihara, On the structure of ideal class groups of CM fields, Documenta Math Kato Volume, 537–563.

Application of Chebotarev

$K_r = \mathbb{Q}(\mu_{p^{r+1}})$

$\Lambda_r = \mathbb{Z}_p[\mathrm{Gal}(K_r/\mathbb{Q})]^{[i]} = \mathbb{Z}_p[\mathrm{Gal}(K_r/K)]$

Prop (Rubin) M: f.g. Λ_r submodule $\subset (K_r^\times \otimes \mathbb{Z}_p)^{[i]}$, $\mathfrak{q} \in A_{K_r}^{[i]}$, $\psi: M \to \Lambda_r/p^N$ Λ_r-hom. } given

Then, there exists infinitely many $\ell \in \mathcal{L}$ s.t.

1) $\exists \ell_{K_r}$ a prime of K_r above ℓ s.t. $[\ell_{K_r}] = \mathfrak{q}$
2) $\psi = u\, \varphi_\ell|_M$ for some $u \in \Lambda_r^\times$.

∵) Consider $F(\mu_N, \sqrt[p^N]{M})$ where F is the unramified extension of K_r s.t. $\mathrm{Gal}(F/K_r) \simeq A_{K_r}^{[i]}$.

Proof of the MC

Suppose $X^{[i]} \sim \bigoplus_{j=1}^{s} \Lambda/(f_j)$ (pseudo isom) $\Lambda = \mathbb{Z}_p[[\mathrm{Gal}(K_\infty/\mathbb{Q})]]^{[i]} = \mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]]$

Take an exact sequence

$$0 \to X^{[i]} \xrightarrow{\varphi} \bigoplus \Lambda/(f_j) \to F \to 0$$

where $\#F = \eta < \infty$.

Take $\mathfrak{q}_j \in X^{[i]}$ s.t. $\varphi(\mathfrak{q}_j) = (0 \cdots 0 \overset{j}{\eta} 0 \cdots 0)$ $(1 \le j \le s)$, and the image of $\mathfrak{q}_j$ in $A_{K_r}^{[i]} = (X^{[i]})_{\mathrm{Gal}(K_\infty/K_r)}$ is also denoted by $\mathfrak{q}_j$.

$\mathcal{L}_j := \{\, \ell \in \mathcal{L} \mid$ a prime of ℓ_{K_r} above ℓ satisfies $[\ell_{K_r}] = \mathfrak{q}_j \,\}$

$\mathcal{L} := \bigcup_{j=1}^{s} \mathcal{L}_j$

$$(\mathrm{Div}_{K_r})' = \bigoplus_{\mathfrak{l}\in\Omega} \left(\mathbb{Z}_p[\mathrm{Gal}(K_r/\mathbb{Q})]\,\mathfrak{l}_{K_r}\right)^{[i]} \subset \left(\mathrm{Div}_{K_r}\otimes\mathbb{Z}_p\right)^{[i]}$$

$$\mathcal{K} = \left\{ x\in (K_r^\times\otimes\mathbb{Z}_p)^{[i]} \mid \mathrm{div}(x)\in (\mathrm{Div}_{K_r})' \right\} \subset (K_r^\times\otimes\mathbb{Z}_p)^{[i]}$$

We have a commutative diagram of exact sequences

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathcal{K} & \longrightarrow & (\mathrm{Div}_{K_r})' & \longrightarrow & A_{K_r}^{[i]} \\ & & \downarrow f & & \downarrow g & & \downarrow \\ 0 & \longrightarrow & \Lambda_r^{\oplus s} & \xrightarrow{h} & \Lambda_r^{\oplus s} & \longrightarrow & \bigoplus_{j=1}^{s} \Lambda_r/(f_j) \longrightarrow 0 \end{array}$$

where g is the map defined by $\mathfrak{l}_{K_r} \mapsto (0\cdots 0\ \overset{j}{\eta}\ ,0\cdots 0)$ if $\mathfrak{l}\in\Omega_j$

f is induced by g, and h corresponds to

$$\begin{pmatrix} f_1 & & 0 \\ & \ddots & \\ 0 & & f_s \end{pmatrix}.$$

Take $\mathfrak{l}_1\in\Omega_1$ and consider $g_{K_r,\mathfrak{l}_1}\in\mathcal{K}$. (some $u\in\Lambda_r^\times$.)

Using Chebotarev (Prop. in Page 1), take $\mathfrak{l}_1\in\Omega_1$ s.t. $\mathrm{pr}_1\circ f = u\,\varphi_{\mathfrak{l}_1} \pmod{p^N}$ for

Then, $f_1\cdot u\,\varphi_{\mathfrak{l}_1}(g_{K_r,\mathfrak{l}_1}) = \eta\,\theta_{K_r}^{[i]}$ from the above commutative diagram.

So $f_1\cdot u(\delta_{\mathfrak{l}_1} + c\,\theta_{K_r}^{[i]}) = \eta\,\theta_{K_r}^{[i]}$ for some $c\in\Lambda_r$.

Since $\mu=0$ and $\mathrm{char}(X^{[i]}) = (f_1\cdots f_s)$, f_1 is prime to p,

so is prime to η. Hence, by taking $r\to\infty$, the above equality implies $f_1 \mid \theta_{K_\infty}^{[i]}$.

In order to prove $\mathrm{char}(X^{[i]}) \mid \theta_{K_\infty}^{[i]}$, we have to show

$$f_2\cdots f_r \mid \delta_{\mathfrak{l}_1}\,\theta_{K_\infty}^{[r]}$$

We consider $\delta_{\mathfrak{l}_1}$.

Take $\mathfrak{l}_2 \in \mathcal{Q}_2$ which splits in $F_{\mathfrak{l}_1}$, and consider $\widetilde{K}_{\mathfrak{l}_1,\mathfrak{l}_2} \in \mathcal{K}$ like yesterday.

Take $\mathfrak{l}_2 \in \mathcal{Q}_2$ which splits in $F_{\mathfrak{l}_1}$, s.t. $pr_2 \circ f = u' \varphi_{\mathfrak{l}_2}$ with $u' \in \Lambda_r^{\times}$. using Chebotarev density (Proposition in Page 1).

Then, $f_2 \cdot u' \varphi_{\mathfrak{l}_2}(\widetilde{K}_{\mathfrak{l}_1,\mathfrak{l}_2}) = \eta\, \delta_{\mathfrak{l}_1}$, so

$$f_2\, u' (\delta_{\mathfrak{l}_1\mathfrak{l}_2} + c' \delta_{\mathfrak{l}_1}) = \eta\, \delta_{\mathfrak{l}_1}.$$

Since f_2 is prime to η, by $r \to \infty$, this implies $f_2 \mid \delta_{\mathfrak{l}_1}$.

$f_2 \mid \theta_{k_\infty}^{[r]}$ can be proved by the same method.

Next, we have to prove $f_3 \cdots f_r \mid \delta_{\mathfrak{l}_1\mathfrak{l}_2}, \delta_{\mathfrak{l}_1}, \cdots$.

We continue this procedure, and get $f_1 \cdots f_r \mid \theta_{k_\infty}^{[r]}$, namely

$$\mathrm{char}(X^{(i)}) \mid \theta_{k_\infty}^{(i)}.$$

cf. M. Aoki, J. Number Theory (2002?)

By the argument using the analytic class number formula, we obtain

$$\mathrm{char}(X^{(i)}) = (\theta_{k_\infty}^{(i)}).$$

//

Higher Fitting ideal

R: comm. ring

M: R-module s.t. $R^m \xrightarrow{\varphi} R^n \longrightarrow M \longrightarrow 0$ (*) exact as R-modules

Let A be the matrix corresponding to φ.

Then for $i \geq 0$, the i-th Fitting ideal $\mathrm{Fitt}_{i,R}(M)$ is defined to be the ide generated by all $(n-i)\times(n-i)$-minors of A.

For $i \geq n$, it is defined to be R.

This does not depend on the choice of the exact sequence (*).

The Fitting ideal we defined in the second lecture is the 0-th (initial) Fitting ideal.

We take $g_1, \cdots g_s$ generators of $X^{[i]}$.

Since $X^{[i]}$ has no nontrivial finite sub Λ-module,

$\ker(\Lambda^{\oplus S} \longrightarrow X^{[i]})$ is a free Λ-module of rank S,

$$(j)\begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \longmapsto g_j$$

and we have an exact sequence

$$0 \longrightarrow \Lambda^{\oplus S} \xrightarrow{h} \Lambda^{\oplus S} \longrightarrow X^{[i]} \longrightarrow 0 \quad \text{of } \Lambda\text{-modules.}$$

Let $A \in M_S(\Lambda)$ be the matrix corresponding to h.

Since $\mathrm{char}(X^{[i]}) = (\det A)$, the main conjecture tells you

$$(\det A) = (\theta_{k_\infty}^{[i]})$$

We can show that not only $\det A$, but also minors of A are described by δ_n's.

In particular, we can get the following.

Define $\textcircled{H}_{k_r, i, N}$ to be the ideal of $\mathbb{Z}/p^N[\mathrm{Gal}(k_r/k)]$ generated by all $\delta_{l_1 \cdots l_j}$ with $l_1 \cdots l_j \in J$ and $j \leq i$.

(take $N = N_r$ s.t. $N_r \to \infty$ $(r \to \infty)$)

Define $\textcircled{H}_i := \varprojlim \textcircled{H}_{k_r, i, N} \subset \Lambda$.

For $i = 0$, $\textcircled{H}_0 = (\theta_{k_\infty}^{[i]})$.

Then, beyond the main conjecture, we have

Theorem. $\mathrm{Fitt}_{i,\Lambda}(X^{[i]}) = \textcircled{H}_i$ for all $i \geq 0$.

This is a more finer relation between algebraic side and analytic side.