Iwasawa Theory and the Eisenstein Ideal

Romyar T. Sharifi

Max Planck Institute of Mathematics
Bonn, Germany

December 18, 2003

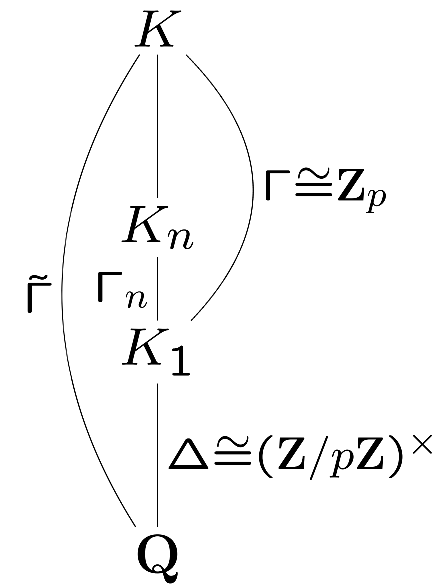
Iwasawa Theory for Cyclotomic Fields:

p odd prime, $n \geq 1$

μ_{p^n} group of p^nth roots of unity

$\mu_{p^\infty} = \cup_{n \geq 1} \mu_{p^n}$

$K_n = \mathbf{Q}(\mu_{p^n})$, $K = \mathbf{Q}(\mu_{p^\infty})$



$\chi\colon \tilde{\Gamma} \xrightarrow{\sim} \mathbf{Z}_p^\times$ cyclotomic character

$\sigma\zeta = \zeta^{\chi(\sigma)}$ for $\zeta \in \mu_{p^\infty}$, $\sigma \in \tilde{\Gamma}$

$\chi(\Gamma) = 1 + p\mathbf{Z}_p$

$\omega\colon \Delta \xrightarrow{\sim} (\mathbf{Z}/p\mathbf{Z})^\times \hookrightarrow \mathbf{Z}_p^\times$ Teichmüller character

χ and ω induce characters on $G_\mathbf{Q} = \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ by first projecting to $\tilde{\Gamma}$ and Δ, respectively

Iwasawa algebras:

$\Lambda = \mathbf{Z}_p[[\Gamma]] = \varprojlim \mathbf{Z}_p[\Gamma_n]$, $\tilde{\Lambda} = \mathbf{Z}_p[[\tilde{\Gamma}]]$

Let $\gamma \in \Gamma$ with $\chi(\gamma) = 1 + p$.

$\gamma - 1 \mapsto T$ defines $\Lambda \xrightarrow{\sim} \mathbf{Z}_p[[T]]$.

Iwasawa modules:

Any $\tilde{\Lambda}$-module A breaks up into "eigenspaces":

$$A = \bigoplus_{i=0}^{p-2} A^{(m)}$$

with

$$A^{(m)} = \langle a \in A \mid \delta a = \omega(\delta)^m a, \delta \in \Delta \rangle.$$

Also, $A = A^+ \oplus A^-$ via complex conjugation.

The Iwasawa module X_K:

H = maximal pro-p abelian unramified extension of K, $X_K = \text{Gal}(H/K)$

Action of $\tilde{\Gamma}$ on X_K by conjugation gives X_K the structure of a $\tilde{\Lambda}$-module.

$A_n = p$-part of ideal class group of K_n

$X_K \cong \varprojlim A_n$ (class field theory)

Let k be even with $2 \leq k \leq p-3$.

$B_k = k$th Bernoulli number

$X_K^{(1-k)} \neq 0 \Leftrightarrow A_1^{(1-k)} \neq 0 \Leftrightarrow p \mid B_k$ (Herbrand, Ribet)

We say that (p,k) is an irregular pair if $p \mid B_k$.

$X_K^{(k)} = 0 \Rightarrow X_K^{(1-k)}$ procyclic

Conjecture (Vandiver). $X_K^+ = 0$.

Vandiver's conjecture holds for $p <$ 12,000,000 (Buhler, et al).

More on Iwasawa modules:

If A is a finitely generated torsion Λ-module, then there exists a pseudo-isomorphism (finite kernel and cokernel),

$$A \to \oplus_{i=1}^{r} \Lambda/(f_i),$$

with $f_i \in \Lambda$, $f_i \neq 0$ (Iwasawa, Serre).

$\text{char}_\Lambda A = (\prod_{i=1}^{r} f_i)$ is an invariant of A.

More on X_K:

X_K is a f.g. torsion Λ-module (Iwasawa).

X_K^- has no p-torsion (Ferrero-Washington).

$L_p(s, \omega^k)$ p-adic L-function, interpolates special values of classical L-functions.

Iwasawa Main Conjecture (Mazur-Wiles).

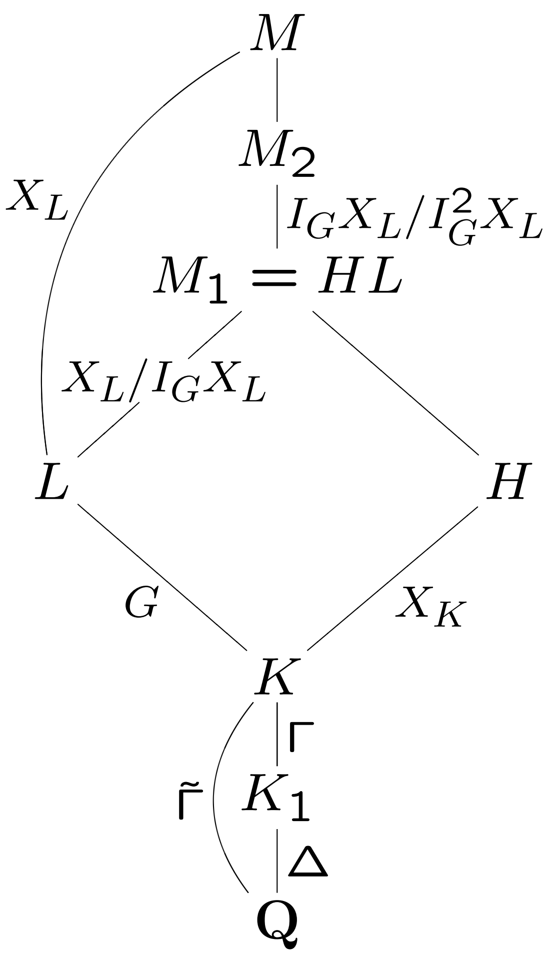
Let $g_k \in \Lambda$ with

$$g_k((1+p)^s - 1) = L_p(s, \omega^k)$$

for all $s \in \mathbf{Z}_p$. Then $(g_k) = \text{char}_\Lambda X_K^{(1-k)}$.

Iwasawa theory for Kummer extensions:

Let L be a $\mathbf{Z}_p$-extension of K unramified outside p, totally ramified at p, and Galois over $\mathbf{Q}$.
$G = \mathrm{Gal}(L/K)$, $\sigma \in G$ generator
$I_G = (\sigma - 1) \leq \mathbf{Z}_p[[G]]$ augmentation ideal
$M =$ max. unramified abelian pro-p ext. of L



X_L is not in general a $\tilde{\Lambda}$-module, but its quotients $I_G^t X_L / I_G^{t+1} X_L$ are.
E.g., restriction induces $X_L / I_G X_L \xrightarrow{\sim} X_K$.

Let Y_L denote the Galois group of the maximal unramified abelian pro-p extension of L in which the prime above p splits completely.
$X_L \to Y_L$ is a surjection with procyclic kernel.
Defining Y_K similarly, we have $Y_K = X_K$.
We also have $Y_L / I_G Y_L \xrightarrow{\sim} X_K$.

Multiplication defines a surjection

$$I_G / I_G^2 \otimes_{\mathbf{Z}_p} Y_L / I_G Y_L \to I_G Y_L / I_G^2 Y_L.$$

Since $I_G / I_G^2 \cong \mathbf{Z}_p$, there exists a canonical isomorphism of $\tilde{\Lambda}$-modules

$$I_G / I_G^2 \otimes_{\mathbf{Z}_p} X_K / \mathcal{P}_{L/K} \xrightarrow{\sim} I_G Y_L / I_G^2 Y_L$$

for some subgroup $\mathcal{P}_{L/K} \leq X_K$.
$\mathcal{P}_{L/K}$ can be described using cup products.

Cup products in Galois cohomology:

$\mathcal{G}_n =$ Galois group of the maximal unramified outside p extension of K_n
$\mathcal{E}_n = \mathbf{Z}_p[\mu_{p^n}, \frac{1}{p}]^\times$ group of p-units in K_n
$A_n = p$-part of the class group of K_n

$$\mathcal{E}_n/\mathcal{E}_n^{p^n} \hookrightarrow H^1(\mathcal{G}_n, \mu_{p^n})$$

$$H^2(\mathcal{G}_n, \mu_{p^n}) \cong A_n/p^n A_n$$

The cup products

$$H^1(\mathcal{G}_n, \mu_{p^n})^{\otimes 2} \to H^2(\mathcal{G}_n, \mu_{p^n}^{\otimes 2})$$

yield pairings

$$(\ ,\ )_n \colon \mathcal{E}_n \times \mathcal{E}_n \to A_n \otimes \mu_{p^n}.$$

$\mathcal{E}_K$ the pro-p completion of $\cup_n \mathcal{E}_n$
$\mathcal{U}_K = \varprojlim (\mathcal{E}_n \otimes \mathbf{Z}_p)$ universal norms
Inverse limit of the pairings yields

$$(\ ,\ )_K \colon \mathcal{E}_K \times \mathcal{U}_K \to X_K(1).$$

Conjecture 1 (McCallum-S.). *The image of* $(\ ,\ )_K$ *contains* $X_K^-(1)$.

Assume L/K is defined by (the p-power roots of) an element $a \in \mathcal{E}_K$.

Theorem 1. $\mathcal{P}_{L/K} = (a,\mathcal{U}_K)_K(-1)$. *That is,*

$$I_G/I_G^2 \otimes_{\mathbf{Z}_p} X_K/((a,\mathcal{U}_K)_K(-1)) \cong I_G Y_L/I_G^2 Y_L.$$

The goal of this talk will be:

Theorem 2. $(p,\mathcal{U}_K)_K = X_K(1)$ *for* $p < 1000$.

Corollary. *Conjecture 1 holds for* $p < 1000$.

Corollary. $X_L \cong Y_L \cong X_K$ *for* $L = K(p^{1/p^\infty})$ *and* $p < 1000$.

Ordinary Hecke algebras:

$\mathbf{T}_n =$ wt. 2 cuspidal Hecke algebra for $\Gamma_1(p^n)$
We consider Hida's ordinary Hecke algebra

$$\tilde{\mathbf{T}} = \varprojlim (\mathbf{T}_n \otimes \mathbf{Z}_p)^{\text{ord}}$$

where "ord" signifies the maximal subfactor in which U_p is a unit.

diamond operators $\langle i \rangle \in \tilde{\mathbf{T}}$ for $i \in \mathbf{Z}_p^\times$
$\mathbf{T}$ eigenspace of $\tilde{\mathbf{T}}$ upon which $\langle i \rangle$ for $i \in (\mathbf{Z}/p\mathbf{Z})^\times$ acts by multiplication by i^{k-2}.
$\mathbf{T}$ is a $\Lambda_{\mathbf{T}} = \mathbf{Z}_p[[T]]$-algebra, $T = \langle 1+p \rangle - 1$.
Eisenstein ideal $\mathcal{I}$ of $\mathbf{T}$:

$$\mathcal{I} = (U_p - 1) + (T_l - 1 - l\langle l \rangle \mid l \neq p).$$

We have $\mathbf{T}/\mathcal{I} \cong \mathbf{Z}_p[[T]]/h_k(T)$, with

$$h_k((1+p)^{-1-s} - 1) = L_p(s, \omega^k)$$

(Wiles).

The representation space:

We begin by describing work of Ohta, which provides a generalization of results of Harder-Pink and Kurihara for level 1.

Let Y denote the eigenspace of

$$\varprojlim H^1_{\text{ét}}(X_1(p^n), \mathbf{Z}_p)^{\text{ord}}.$$

upon which $\langle i \rangle$ acts as i^{k-2} for $i \in (\mathbf{Z}/p\mathbf{Z})^\times$.

Fix a decomposition group D_p in $G_\mathbf{Q}$ at p.
Let I_p be the inertia subgroup of D_p.
Fix $\Delta_p \le I_p$ with $\omega\colon \Delta_p \xrightarrow{\sim} (\mathbf{Z}/p\mathbf{Z})^\times$.
Under Δ_p, we have $Y = Y^+ \oplus Y^-$.

Y^+ is a free $\mathbf{T}$-module of rank 1.

$\mathcal{L}_\mathbf{T}$ = quotient field of $\Lambda_\mathbf{T}$
$Y^- \otimes_{\Lambda_T} \mathcal{L}_T$ is a free $\mathbf{T} \otimes_{\Lambda_\mathbf{T}} \mathcal{L}_\mathbf{T}$-module of rank 1.

The modular representation:
The action of $G_{\mathbf{Q}}$ on Y provides

$$\rho\colon G_{\mathbf{Q}} \to \mathrm{Aut}_{\mathbf{T}}(Y).$$

For $\sigma \in G_{\mathbf{Q}}$, we write

$$\rho(\sigma) = \begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix},$$

$a(\sigma) \in \mathrm{End}_{\mathbf{T}}(Y^-)$, $b(\sigma) \in \mathrm{Hom}_{\mathbf{T}}(Y^+, Y^-)$, ...
We remark that $\mathrm{End}_{\mathbf{T}}(Y^\pm) \hookrightarrow \mathbf{T} \otimes_{\Lambda_{\mathbf{T}}} \mathcal{L}_{\mathbf{T}}$.
For $\sigma \in I_p$, we have

$$\rho(\sigma) = \begin{pmatrix} a(\sigma) & 0 \\ c(\sigma) & 1 \end{pmatrix}.$$

For $\sigma, \tau \in G_{\mathbf{Q}}$, we have

$$\begin{aligned} d(\sigma) &\equiv 1 \bmod \mathcal{I}, \\ b(\sigma)c(\tau) &\equiv 0 \bmod \mathcal{I}. \end{aligned}$$

In fact, let B (resp., C) denote the $\mathbf{T}$-module generated by all $b(\sigma)$ (resp., $c(\sigma)$) with $\sigma \in G_{\mathbf{Q}}$. Then $BC = \mathcal{I}$.

Classical Iwasawa Theory:

Let (p,k) be an irregular pair.

Consider the maps

$$\bar{a}\colon G_{\mathbf{Q}} \to (\mathbf{T}/\mathcal{I})^{\times} \quad \text{and} \quad \bar{b}\colon G_{\mathbf{Q}} \to B/\mathcal{I}B.$$

We have a homomorphism on $G_{\mathbf{Q}}$:

$$\phi_B(\sigma) = \begin{pmatrix} \bar{a}(\sigma) & \bar{b}(\sigma) \\ 0 & 1 \end{pmatrix}.$$

Let H be the fixed field of the kernel of ϕ_B. H is an unramified abelian pro-p extension of K with $\mathrm{Gal}(H/K) \cong B/\mathcal{I}B$ having an ω^{1-k}-action of Δ.

By an argument on characteristic ideals, Ohta shows:

Theorem (Ohta). $\mathrm{Gal}(H/K) = X_K^{(1-k)}$.

This yields another proof of Iwasawa's Main Conjecure.

Iwasawa theory for Kummer extensions:

Let (p,k) be an irregular pair with $p \nmid B_{p+1-k}$.

Now let $\bar{c}\colon G_{\mathbf{Q}} \to C/\mathcal{I}C$ and define

$$\phi_C(\sigma) = \begin{pmatrix} \bar{a}(\sigma) & 0 \\ \bar{c}(\sigma) & 1 \end{pmatrix}.$$

The fixed field L of the kernel of ϕ_C is an abelian pro-p extension of K which is unramified outside p and totally ramified at p.

Let $G = \mathrm{Gal}(L/K)$.

Remark. If $X_K^{(1-k)}$ is procyclic (e.g., if $p <$ 12,000,000), then $G = G^{(k-1)} \cong \mathbf{Z}_p$ as a pro-p group.

Now define $\bar{d}\colon G_{\mathbf{Q}} \to (\mathbf{T}/\mathcal{I}^2)^\times$ and consider the homomorphism

$$\phi_D(\sigma) = \begin{pmatrix} \bar{a}(\sigma) & \bar{b}(\sigma) \\ \bar{c}(\sigma) & \bar{d}(\sigma) \end{pmatrix}.$$

We also have a homomorphism

$$\psi(\sigma) = \begin{pmatrix} 1 & \bar{c}(\sigma) & \bar{d}(\sigma) - 1 \\ 0 & \bar{a}(\sigma) & \bar{b}(\sigma) \\ 0 & 0 & 1 \end{pmatrix}$$

defining the same extension as ϕ_D.

Fact: $\bar{d}([\sigma, \tau]) - 1 = \bar{c}(\sigma)\bar{b}(\tau)$ for $\sigma, \tau \in G_K$.

The map $\bar{d} - 1$ yields a surjection

$$I_G/I_G^2 \otimes_{\mathbf{Z}_p} X_K^{(1-k)} \to \mathcal{I}/\mathcal{I}^2$$

This leads to the following.

Theorem 3. *Assume that $p \mid B_k$ and $p \nmid B_{p+1-k}$. Then there is a canonical isomorphism*

$$(I_G X_L / I_G^2 X_L)_{\tilde{\Gamma}} \cong \mathcal{I}/\mathcal{I}^2.$$

Remark. If $X_K^{(1-k)}$ is procyclic, then

$$(I_G X_L / I_G^2 X_L)_{\tilde{\Gamma}} = (I_G X_L / I_G^2 X_L)^{(0)}.$$

$\bar{d}(\varphi_p^{-1}) = U_p$ for a Frobenius $\varphi_p \in D_p$
$\mathcal{U} = \mathbf{Z}_p$-submodule of $\mathbf{T}$ generated by $U_p - 1$

Theorem 4. *Assume that $p \mid B_k$ and $p \nmid B_{p+1-k}$. There is canonical a isomorphism*

$$(I_G Y_L / I_G^2 Y_L)_{\tilde{\Gamma}} \cong \mathcal{I}/(\mathcal{U} + \mathcal{I}^2).$$

The following was verified computationally:

Theorem 5. *For any irregular pair (p, k) with $p < 1000$, we have $\mathcal{I} = \mathcal{U} + \mathcal{I}^2$.*

We conclude from this that $(p, \mathcal{U}_K)_K = X_K(1)$ for $p < 1000$.

Remark: Actually, our L is not the Kummer extension defined by p, but rather by an element which pairs nontrivially with it at the level of K_1.

Some applications:

We obtain results on the structure of many different objects (for $p < 1000$).

1. complete determination of the pairing $(\, , \,)_1$

2. determination of X_L for "most" L

3. relations in the Galois group of the maximal pro-p unramified outside p extension of $\mathbf{Q}(\mu_p)$

4. Greenberg's pseudo-nullity conj. for $\mathbf{Q}(\mu_p)$

5. pro-p Galois Lie algebra of $\mathbf{P}^1_{\mathbf{Q}} - \{0, 1, \infty\}$ (e.g., Ihara's $p = 691$ conjecture)

6. products on p-parts of K-groups of $\mathbf{Z}$ and other cyclotomic integer rings

7. Selmer groups of modular representations