FALL 2022 LEARNING SEMINAR: INTRODUCTION TO IWASAWA THEORY

MURILO CORATO ZANARELLA

November 21, 2022

1. What is Iwasawa theory?

1.1. **Inspiration from function fields.** Let X be a smooth projective variety over $\mathbb{F}_p$. Its *zeta function* was originally defined as

$$\zeta(X,s) = \exp\left(\sum_{m\geq 1} \frac{\#X(\mathbb{F}_{p^m})}{m} p^{-ms}\right).$$

To prove the easy parts of the Weil conjecture, one writes $X(\mathbb{F}_{p^m}) = X(\overline{\mathbb{F}}_p)^{\mathrm{Frob}^m=1}$, and rewrites this using Grothendieck–Lefschetz as

$$\#X(\mathbb{F}_{p^m}) = \sum_{k\geq 0}(-1)^k \mathrm{tr}\left(\mathrm{Frob}^{m,*} \mid H^k_{\text{èt}}(X_{\overline{\mathbb{F}_p}}, \mathbb{Q}_l)\right)$$

and thus

$$\zeta(X,s) = \exp\left(\sum_{k\geq 0}(-1)^k \mathrm{tr}\left(\sum_{m\geq 1}\frac{1}{m}\mathrm{Frob}^m p^{-ms} \mid H^k_{\text{èt}}(X_{\overline{\mathbb{F}_p}}, \mathbb{Q}_l)\right)\right) = \prod_{k\geq 0} \det\left(1 - \mathrm{Frob}\cdot p^{-s} \mid H^k_{\text{èt}}(X_{\overline{\mathbb{F}_p}}, \mathbb{Q}_l)\right)^{(-1)^{k+1}}.$$

That is,

$$\zeta(X,s) = \prod_{k\geq 0} \mathrm{char}\left(\mathrm{Frob}\cdot T \mid H^k_{\text{èt}}(X_{\overline{\mathbb{F}_p}}, \mathbb{Q}_l)\right)^{(-1)^{k+1}}|_{T=p^{-s}}.$$

So, very roughly, we see some *extra structure* when we look at all the $\#X(\mathbb{F}_{p^m})$ together. For example, the $\#X(\mathbb{F}_{p^m})$ must satisfy a recurrence relation!

1.2. **Iwasawa's idea.** Now imagine we want to replace the variety X above by a number field F. Instead of $X(\mathbb{F}_p)$, we should have some other interesting arithmetic quantity. Iwasawa's original investigations were about $\mathrm{Cl}(F)$, so let's take that as the analogue.

For $X(\mathbb{F}_{p^m})$, we can think of this as the rational points of $X_{\mathbb{F}_{p^m}}$. If X corresponds to F, maybe $X_{\mathbb{F}_{p^m}}$ corresponds to a finite extension F_n of F. But what should be this tower of number fields? The Galois group $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ is $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$. It turns out it will be easier, instead, to focus on one of the $\mathbb{Z}_p$ components.

Definition 1.1. A $\mathbb{Z}_p^d$-extension of a number field F is an infinite Galois extension F_∞ with $\mathrm{Gal}(F_\infty/F) \simeq \mathbb{Z}_p^d$. Concretely, this is a tower of number fields F_n where $\mathrm{Gal}(F_n/F) \simeq (\mathbb{Z}/p^n\mathbb{Z})^d$.

Remark 1.2. Leopoldt's conjecture for a number field F and a prime p is equivalent to[1]: if d is the largest positive integer such that there exist a $\mathbb{Z}_p^d$ extension of F, then $d = 1 + r_2(F)$, where $r_2(F)$ is the number of complex places of F. Leopoldt's conjecture is known for abelian extensions of $\mathbb{Q}$ and abelian extensions of a quadratic imaginary field.

Example 1.3. If $F = \mathbb{Q}$, there is a unique $\mathbb{Z}_p$-extension, contained inside the tower of cyclotomic fields $\mathbb{Q}(\mu_{p^n})$.

[1] This is explained in [Was97, Theorem 13.4]

Example 1.4. If $F = K$ is a quadratic imaginary field, There is a unique $\mathbb{Z}_p^2$-extension K_∞. Complex conjugation acts on $\mathrm{Gal}(K_\infty/K)$, with eigencomponents $\mathrm{Gal}(K_\infty^{cycl}/K)$ and $\mathrm{Gal}(K_\infty^{anti}/K)$. Of course, K_∞^{cycl} is contained in the tower $K(\mu_{p^n})$. K_∞^{anti} is the unique $\mathbb{Z}_p$-extension contained in the tower of ring class fields of p-power conductor of K.

For concreteness, let's focus our attention on the cyclotomic $\mathbb{Z}_p$-extension. It is contained inside the tower $K_n := \mathbb{Q}(\mu_{p^{n+1}})$, say $F_n \subseteq K_n$ for $n \geq 0$. So $F_0 = \mathbb{Q}$ and $K_0 = \mathbb{Q}(\mu_p)$.

If we want an analogue of the zeta function ζ_X, we need to somehow assemble the groups $\mathrm{Cl}(K_n)$ together. It turns out that the groups $\mathrm{Cl}(K_n)$ do not behave well in families, but their p-primary parts do. So denote

$$X_n := \mathrm{Cl}(K_n)[p^\infty].$$

This is a $\mathbb{Z}_p[\mathrm{Gal}(K_n/\mathbb{Q})]$-module.

Definition 1.5. We let $X_\infty := \varprojlim_n X_n$ with transition maps given by the norm map $\mathrm{Nm}_{K_{n+1}/K_n} \colon \mathrm{Cl}(K_{n+1})[p^\infty] \to \mathrm{Cl}(K_n)[p^\infty]$. This is a $\mathbb{Z}_p[\![\mathrm{Gal}(K_\infty/\mathbb{Q})]\!]$-module. Call $\Lambda^{cycl} := \mathbb{Z}_p[\![\mathrm{Gal}(K_\infty/\mathbb{Q})]\!]$.

Now note that

$$\mathrm{Gal}(K_\infty/\mathbb{Q}) = \varprojlim_n \mathrm{Gal}(K_n/\mathbb{Q}) = \varprojlim_n (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times = \mathbb{Z}_p^\times.$$

Assuming $p > 2$ for simplicity, we can choose a topological generator $\gamma \in (1 + p\mathbb{Z}_p)^\times \xrightarrow[\sim]{\log} \mathbb{Z}_p$ (for example $\gamma = 1 + p$), we identify

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

where $\Delta = (\mathbb{Z}/p\mathbb{Z})^\times \overset{\omega}{\hookrightarrow} \mathbb{Z}_p^\times$ for ω the Teichmüller character.

Definition 1.6. Let $\Lambda := \mathbb{Z}_p[\![T]\!]$ denote the *Iwasawa algebra*. It is a complete regular local ring of dimension 2 with maximal ideal $\mathfrak{m} = (p, T)$.

Proposition 1.7. $\Lambda^{cycl} \simeq \Lambda[\Delta]$ *where* $T \in \Lambda$ *is identified with* $\gamma - 1$.[2]

Proof. We just need to show that $\mathbb{Z}_p[\![\mathrm{Gal}(F_\infty/\mathbb{Q})]\!] \simeq \Lambda$. The problem is seeing that the map and its inverse are well-defined and continuous. That is, we need to see that

$$(T+1)^{p^n} \to 1 \text{ in } \Lambda$$

and that

$$(\gamma - 1)^n \to 0 \text{ in } \mathbb{Z}_p[\![\mathrm{Gal}(F_\infty/\mathbb{Q})]\!].$$

The first one simply follows from $(T+1)^{p^n} - 1 \in \mathfrak{m}^{\min_{1 \leq a \leq p^n}(a + \nu_p\binom{p^n}{a})}$. Since $\nu_p\binom{p^n}{a} = n - \nu_p(a)$ for $1 \leq a \leq p^n$, we have $(T+1)^{p^n} - 1 \in \mathfrak{m}^{n+1}$.

For the second one, we need to show that for any $m \geq 0$, we have $(\gamma - 1)^n \mod (\gamma^{p^m} - 1)$ goes to 0 in $\mathbb{Z}_p[\mathrm{Gal}(F_m/\mathbb{Q})]$. Write $n = a_0 + a_1 p + \cdots + a_k p^k$ in base p. Then

$$(\gamma - 1)^n = \prod_{i=0}^{k} (\gamma^{p^i} - 1 + p^i(\cdots))^{a_i} \equiv \prod_{i=0}^{m-1} (\gamma^{p^i} - 1 + p^i(\cdots))^{a_i} \cdot \prod_{i=m}^{k} (p^i(\cdots))^{a_i}.$$

So $(\gamma - 1)^n \mod (\gamma^{p^m} - 1)$ is divisible by $p^{\sum_{i \geq m} i a_i}$, and $\sum_{i \geq m} i a_i \to \infty$ as $n \to \infty$. $\square$

[2]In general, the completed group algebra of a $\mathbb{Z}_p^d$ extension is identified with $\mathbb{Z}_p[\![T_1, \ldots, T_d]\!]$ in a similar way.

Roughly speaking, the goal of Iwasawa theory in this case is to:

(1) Understand the structure of X_∞ as a $\Lambda^{cycl} = \Lambda[\Delta]$-module.
(2) "Descend" this information to the finite level modules X_n.

2. The Iwasawa algebra

[3] We can think of $\Lambda = \mathbb{Z}_p[\![T]\!]$ as the ring of functions of the closed p-adic unit disk. Such a function can only have finitely many zeroes, that is, we have:

Theorem 2.1 (p-adic Weierstraß preparation)**.** *Any element $f(T) \in \Lambda$ can be uniquely written as*

$$f(T) = p^\mu \lambda(T) u(T)$$

where $\mu \geq 0$, $u(T) \in \Lambda^\times$ and $\lambda(T) \in \mathbb{Z}_p[T]$ is a distinguished polynomial*, i.e. of the form*

$$\lambda(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_1 T + a_0 \quad \textit{where} \quad p \mid a_i.$$

We call μ the μ-invariant *of f, and $\deg \lambda$ the* λ-invariant *of f.*

In particular, Λ is a UFD. Its height 1 prime ideals are simply (p) and $(f(T))$ for f irreducible distinguished polynomials. Hence all the localizations $\Lambda_\mathfrak{p}$ at height 1 prime ideals are DVRs.[4]

Definition 2.2. A Λ-module M is *pseudo-null*[5] if it is annihilated by some power of $\mathfrak{m}$. A *pseudo-isomorphism* is a morphism $M_1 \to M_2$ with pseudo-null kernel and cokernel.

Remark 2.3. If there is a pseudo-isomorphism $M_1 \to M_2$, it is not true that there must be a pseudo-isomorphism $M_2 \to M_1$. But this *is* true if M_1 and M_2 are finitely generated torsion Λ-modules, where pseudo-isomorphism gives an equivalence relation.

We note that a Λ-module M has finite cardinality if and only if it is finitely generated and pseudo-null. We have the following analogue of the structure theorem for finitely generated modules over PIDs.[6]

Theorem 2.4. *Let M be a finitely generated Λ-module. Then there is a pseudo-isomorphism*

$$M \to \Lambda^r \oplus \bigoplus_i \Lambda / f_i^{e_i} \Lambda$$

for some $r \geq 0$ and f_i are finitely many irreducible elements. r is determined by M and is additive on exact sequences. If $r = 0$, then f_i and e_i are uniquely determined.

We define

Definition 2.5. For M a finitely generated torsion Λ-module, we define its *characteristic ideal* $\mathrm{Ch}(M) = \prod_\mathfrak{p} \mathfrak{p}^{\mathrm{length}_{\Lambda_\mathfrak{p}} M \otimes_\Lambda \Lambda_\mathfrak{p}}$

[3][Was97, Section 13.2] or [Sha, Section 2.4] contain proofs for the statements in this section.
[4]More generally, $\mathbb{Z}_p[\![T_1, \ldots, T_n]\!]$ is still a *Krull domain*, a certain higher dimension generalization of Dedekind domains
[5]A module over a Krull domain is said to be pseudo-null if its annihilator ideal has height ≥ 2.
[6]This also holds over Krull domains, although it is not true that pseudo-null is the same as finite cardinality.

By definition, the characteristic ideal is multiplicative in exact sequences of finitely generated torsion Λ-modules. Moreover, for M finitely generated torsion, M is pseudo-null exactly if $\mathrm{Ch}(M) = \Lambda$. Thus

Proposition 2.6. *If $M \to \bigoplus_i \Lambda/f_i^{e_i}$ as above is a pseudo isomorphism, then* $\mathrm{Ch}(M) = \left(\prod_i f_i^{e_i}\right)$.

3. The descent procedure

Let's now come back to the case that $X_n = \mathrm{Cl}(K_n)[p^\infty]$ for $K_n = \mathbb{Q}(\mu_{p^{n+1}})$. We formed $X_\infty = \varprojlim_n X_n$ under norms. How can we hope to recover X_n? By the definition of X_∞, we have a natural map

$$X_\infty \to X_n.$$

Proposition 3.1. *The natural map $X_\infty \to X_n$ is surjective.*

Proof. In fact, we will prove that $\mathrm{Nm}_{K_{n+1}/K_n} \colon X_{n+1} \to X_n$ is surjective for all $n \geq 0$. This will rely on the fact that p is totally ramified in K_{n+1}.[7] Let L_n denote the maximal unramified abelian p-extension of K_n. Then we have the diagram, where labels denote the behaviour of primes above p.

$$\begin{tikzcd}[arrows=dash]
L_{n+1} \arrow[d] & \\
L_nK_{n+1} \arrow[dd] \arrow[dr] & \\
& K_{n+1} \arrow[dd, "tot.ram"] \\
L_n \arrow[dr, "unr"'] & \\
& K_n
\end{tikzcd}$$

By ramification reasons, we must have $L_n \cap K_{n+1} = K_n$. Thus

$$X_{n+1} = \mathrm{Gal}(L_{n+1}/K_{n+1}) \twoheadrightarrow \mathrm{Gal}(L_nK_{n+1}/K_{n+1}) = \mathrm{Gal}(L_n/K_n) = X_n$$

and such map is identified with $\mathrm{Nm}_{K_{n+1}/K_n} \colon X_{n+1} \to X_n$. $\square$

Proposition 3.2 ([Was97, Proposition 13.22])**.** *We have $X_n = X_\infty/\nu_n X_\infty$ where*

$$\nu_n := (1+T)^{p^n} - 1 \in \Lambda.$$

Proof. Recall that $1 + T = \gamma$, and thus $\alpha := 1 + \nu_n$ is a topological generator of $\mathrm{Gal}(K_\infty/K_n)$.

[7] This is not true for all $\mathbb{Z}_p$ extensions. For instance, it is not true for K_∞^{anti}/K for a quadratic imaginary field K.

Consider the diagram as in the previous proof

$$\begin{tikzcd}
L_\infty \arrow[d, dash] & \\
L_nK_\infty \arrow[dr, dash] \arrow[dd, dash] & \\
& K_\infty \arrow[dd, dash, "tot.ram"] \\
L_n \arrow[dr, dash, "unr"] & \\
& K_n
\end{tikzcd}$$

Then $G := \mathrm{Gal}(L_\infty/K_n) = X_\infty \hat{\rtimes} \langle \alpha \rangle$ for a choice of lift of α. L_n is the maximal unramified abelian subextension of L_∞/K_n, so

$$X_n = \mathrm{Gal}(L_n/K_n) = (X_\infty \hat{\rtimes} \langle \alpha \rangle)/\overline{([G,G],\alpha)} = X_\infty/(g \sim \alpha \cdot g \colon g \in X_\infty) = X_\infty/\nu_n X_\infty,$$

as $\alpha^{-1} g \alpha g^{-1} \in [G,G]$ and thus we must have $\alpha \cdot g = \alpha^{-1} g \alpha \sim g$. □

Corollary 3.3. *X_∞ is a finite generated torsion Λ-module.*

Proof. As $X_0/pX_0 = X_\infty/\mathfrak{m}X_\infty$ is finite, we conclude that X_∞ is a finitely generated Λ-module by Nakayama. It is also Λ-torsion as X_0 is finite. □

Now given $\chi = \omega^i$ a power of the Teichmüller character, assume that we had a pseudo-isomorphism $X_\infty^\chi \to \bigoplus \Lambda/f_i$. Then we can consider the diagram

$$\begin{tikzcd}
X_\infty^\chi \arrow[r] \arrow[d, "\cdot \nu_n"] & \bigoplus \Lambda/f_i \arrow[d] \\
X_\infty^\chi \arrow[r] & \bigoplus \Lambda/f_i
\end{tikzcd}$$

to try to compare $X_n^\chi = X_\infty^\chi/\nu_n X_\infty^\chi$ and $\bigoplus \Lambda/(f_i, \nu_n)$. Following this, one can prove

Lemma 3.4 ([Was97, Theorem 13.13])**.** *If X is a finitely generated torsion Λ-module with $X/\nu_n X$ finite for all $n \geq 0$, then there is $n_0 \geq 0$ and $c \in \mathbb{Z}$ such that*

$$\# X/\nu_n X = p^{np^\mu + n\lambda + c} \text{ for all } n \geq n_0,$$

where μ, λ are the invariants of $\mathrm{Ch}(X)$.

But often we can be more precise than that. The main issue for the ambiguity in the lemma above is that $X \to \bigoplus \Lambda/f_i$ in general can have both a kernel and cokernel. But fortunately, often for the modules in Iwasawa theory the kernel must be 0. For example:

Proposition 3.5. *X_∞^χ has no nonzero pseudo-null submodules.*

Proof. If it did contain a nonzero pseudo-null submodule Y, then $\mathfrak{m}^k Y = 0$ for some k. So it suffices to prove that if $Y \subseteq X_\infty^\chi$ is a submodule with $\mathfrak{m}Y = 0$, then $Y = 0$. If $c = (c_n)_{n \geq 0} \in Y$, then $pc = 0$, and thus $c_n \in \mathrm{Cl}(K_n)[p]$ for all n. As $Tc = 0$, we also have $(\gamma - 1)c = 0$ for any $\gamma \in \mathrm{Gal}(K_\infty/K_0)$. So $c_n \in \mathrm{Cl}(K_n)[p]^{G_{K_0}}$ But then $c_n = \mathrm{Nm}_{K_{n+1}/K_n} c_{n+1} = p \cdot c_{n+1} = 0$ for all $n \geq 0$. □

Corollary 3.6. *We have* $\# X_n^\chi = \prod_i \#\Lambda/(f_i, \nu_n)$. *In particular,* $\# X_0^\chi = \#\mathbb{Z}_p/\mathrm{Ch}(X_\infty^\chi)(0)$.

Proof. This follows from applying the snake lemma to

$$\begin{tikzcd} 0 \arrow[r] & X_\infty^\chi \arrow[r] \arrow[d, "\cdot\nu_n"] & \bigoplus_i \Lambda/f_i \arrow[r] \arrow[d, "\cdot\nu_n"] & \mathrm{coker} \arrow[r] \arrow[d, "\cdot\nu_n"] & 0 \\ 0 \arrow[r] & X_\infty^\chi \arrow[r] & \bigoplus_i \Lambda/f_i \arrow[r] & \mathrm{coker} \arrow[r] & 0 \end{tikzcd}$$

Since X_n^χ is finite, the Snake lemma implies that $\Lambda/(f_i, \nu_n)$ must have finite cardinality. This means that f_i and ν_n are coprime, and hence that $\ker(\Lambda/f_i \xrightarrow{\cdot\nu_n} \Lambda/f_i) = 0$. Now the claim follows from the Snake lemma by noting that $\mathrm{coker}[\nu_n]$ and coker/ν_n have the same cardinality as coker has finite cardinality. $\square$

Recall that we should have

$$\mathrm{Cl}(\mathbb{Q}(\mu_p))[p^\infty]^\chi = \begin{cases} 0 & \text{if } \chi = \omega, \\ |L(0, \chi^{-1})|_p & \text{if } \chi \text{ is odd and } \chi \neq \omega, \\ |(\mathcal{O}_{\mathbb{Q}(\mu_p)^+}^\times/C)^\chi|_p & \text{if } \chi \text{ is even.} \end{cases}$$

We proved this for χ even using Euler systems, but historically it was first deduced from Mazur–Wiles proof of:

Conjecture 3.7 (Iwasawa Main Conjecture)**.** *Let* E_n *denote the units of* K_n^+ *that are congruent to* 1 *modulo the prime above* p. *Let* $C_n \subseteq E_n$ *be the subset of cyclotomic units. Denote* E_∞, C_∞ *their limits under the norm map. For* χ *even nontrivial, denote also* $\mathscr{L}_{KL}^\chi \in \Lambda$ *the Kubota–Leopoldt* p*-adic* L *function for* χ. *Then for* $\chi \neq \omega^0, \omega^1$, *we have*

$$\mathrm{Ch}(X_\infty^\chi) = \begin{cases} (\mathscr{L}_{KL}^{\omega\chi^{-1}}) & \textit{if } \chi \textit{ is odd,} \\ \mathrm{Ch}(E_\infty/C_\infty)^\chi & \textit{if } \chi \textit{ is even.} \end{cases}$$

Here, for χ even nontrivial, the Kubota–Leopoldt p-adic L-function is the unique element $\mathscr{L}_{KL}^\chi \in \Lambda$ such that $\epsilon_{cycl}^n(\mathscr{L}_{KL}^\chi) = L^*(n, \chi\omega^{n-1})$ for all $n \leq 0$. For an explicit construction of element, see [Was97, Theorem 7.10]. We will later give another way to construct this.

In fact, the Euler system argument we gave can be adapted to prove the above conjecture when χ is even: see [Was97, Section 15] for details. We will explain how, in fact, the two parts of the main conjecture are *equivalent*. This is often called the *reflection theorem* in this classical context. We will see next week how this is a particular case of a more general philosophy connecting Euler systems and Iwasawa main conjectures.

To build up for the proof of the reflection theorem, we will reinterpret the modules we have been considering in terms of Selmer groups.

4. In terms of Selmer groups

Suppose we have a p-adic representation V with a G_K-stable lattice Λ. Denote $W := V/\Lambda$. From the exact sequence $0 \to \Lambda \to V \to W \to 0$, we have for a place v

$$H^1(K_v, \Lambda) \xrightarrow{\alpha} H^1(K_v, V) \xrightarrow{\beta} H^1(K_v, W).$$

A Selmer structure on $H^1_{\mathcal{L}}(K_v, V)$ can be *propagated* to $H^1(K_v, \Lambda)$ and $H^1(K_v, W)$ simply by defining

$$H^1_{\mathcal{L}}(K_v, \Lambda) := \alpha^{-1}(H^1_{\mathcal{L}}(K_v, V)), \quad H^1_{\mathcal{L}}(K_v, W) := \beta(H^1_{\mathcal{L}}(K_v, V)).$$

We will look mostly at $H^1_{\mathcal{L}}(K, W)$. Recall from Gefei's talk

Proposition 4.1. *The Kummer map induces an isomorphism $\mathcal{O}_K^\times \otimes \mathbb{Q}_p \xrightarrow{\sim} H^1_f(K, \mathbb{Q}_p(1))$. For an elliptic curve E/K, the Kummer map $E(K) \otimes \mathbb{Q}_p \to H^1_f(K, V_pE)$ is an isomorphism if and only if $Ш(E/K)[p^\infty]$ is finite.*

But in fact, we actually have

Proposition 4.2. *The inverse limit of the finite level Kummer maps identify $\mathcal{O}_K^\times \otimes \mathbb{Z}_p \xrightarrow{\sim} H^1_f(K, \mathbb{Z}_p(1))$. The direct limit of the finite level Kummer map fits into an exact sequence*

$$0 \to \mathcal{O}_K^\times \otimes \mathbb{Q}_p/\mathbb{Z}_p \to H^1_f(K, \mathbb{Q}_p/\mathbb{Z}_p(1)) \to \mathrm{Cl}(K)[p^\infty] \to 0.$$

Similarly, if E is an elliptic curve over K, then the natural map $E(K)\otimes\mathbb{Z}_p \hookrightarrow H^1_f(K, T_pE)$ is an isomorphism iff $Ш(E/K)[p^\infty]$ is finite, and we also have that $H^1_f(K, E[p^\infty]) = \mathrm{Sel}_{p^\infty}(E/K)$ fits into the exact sequence

$$0 \to E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to H^1_f(K, E[p^\infty]) \to Ш(E/K)[p^\infty] \to 0.$$

Let's also look at the trivial representation $\mathbb{Q}_p$. Since its weight is 0, the Bloch–Kato conditions are unramified everywhere. The propagations to $\mathbb{Z}_p$ and $\mathbb{Q}_p/\mathbb{Z}_p$ can be checked to also be just the unramified cohomology. Thus

$$H^1_f(K, \mathbb{Q}_p) = H^1_f(K, \mathbb{Z}_p) = 0, \quad H^1_f(K, \mathbb{Q}_p/\mathbb{Z}_p) = \mathrm{Hom}(\mathrm{Cl}(K), \mathbb{Q}_p/\mathbb{Z}_p).$$

So X_∞ is identified with

$$\mathrm{Hom}\left(\varinjlim_n H^1_f(K_n, \mathbb{Q}_p/\mathbb{Z}_p), \mathbb{Q}_p/\mathbb{Z}_p\right),$$

where the transition maps are simply the restriction.

Following Greenberg, we an give a different description of this direct limit.

Proposition 4.3. *Let V be a p-adic representation of G_K unramified away from Σ with G_K-stable lattice T. Denote $W = V/T$. Let K_∞/K be an abelian tower of finite extensions K_n/K unramified away from Σ. Let $\Lambda_{K_\infty/K} := \mathbb{Z}_p[\![\mathrm{Gal}(K_\infty/K)]\!]$, and $\Lambda^\vee_{K_\infty/K} := \mathrm{Hom}(\Lambda_{K_\infty/K}, \mathbb{Q}_p/\mathbb{Z}_p)$ as G_K-modules, and Λ^{cycl}-action by $(\lambda \cdot f)(x) = f(x\lambda)$. Let $\mathbb{T}_T := T \otimes_{\mathbb{Z}_p} \Lambda_{K_\infty/K}$ and $\mathbb{W}_T := T \otimes_{\mathbb{Z}_p} \Lambda^\vee_{K_\infty/K}$. Then*

$$\varprojlim_n H^1(K_\Sigma/K_n, T) = H^1(K_\Sigma/K, \mathbb{T}_T) \quad \textit{and} \quad \varinjlim_n H^1(K_\Sigma/K_n, W) = H^1(K_\Sigma/K, \mathbb{W}_T).$$

Proof. We only prove the second equality, since the first is analogous.

By Shapiro's lemma, we have $H^1(K_\Sigma/K_n, W) = H^1(K_\Sigma/K, \mathrm{Ind}^{G_K}_{G_{K_n}} W)$. So It suffices to see that $\varinjlim_n \mathrm{Ind}^{G_K}_{G_{K_n}} W = \mathbb{W}$ as G_K-modules. We have

$$\mathrm{Ind}^{G_K}_{G_{K_n}} W = \{f\colon G_K \to W\colon f(\sigma x) = f(x)^\sigma \text{ for } x \in G_K,\ \sigma \in G_{K_n}\}$$

and so

$$\varinjlim_n \mathrm{Ind}^{G_K}_{G_{K_n}} W = \mathrm{Hom}(\Lambda_{K_\infty/K}, W)$$

which is $\mathbb{W}_T$ as $W = T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p$. $\square$

One can define Selmer structures on these cohomology groups by the inverse/direct limit of the Bloch–Kato local conditions.[8] Then we indeed have $H^1_f(K, \mathbb{T}_T) = \varprojlim H^1_f(K_n, T)$ and $H^1_f(K, \mathbb{W}_T) = \varinjlim H^1_f(K_n, W)$.

Definition 4.4. We denote $\mathrm{Sel}(T) = H^1_f(\mathbb{Q}, \mathbb{T}_T)$, $S(T) = H^1_f(\mathbb{Q}, \mathbb{W}_T)$ and $X(T) = \mathrm{Hom}(S(T), \mathbb{Q}_p/\mathbb{Z}_p)$ when the extension K_∞/K is implied.

Example 4.5. For $T = \mathbb{Z}_p$ and $T = \mathbb{Z}_p(1)$, we have

$$\mathrm{Sel}(\mathbb{Z}_p) = 0, \quad \mathrm{Sel}(\mathbb{Z}_p(1)) = \varprojlim_n (\mathcal{O}_{K_n}^\times \otimes \mathbb{Z}_p), \quad X(\mathbb{Z}_p) = \varprojlim_n \mathrm{Cl}(K_n)[p^\infty],$$

and $X(\mathbb{Z}_p(1))$ fits in the exact sequence

$$0 \to \left(\varinjlim_n \mathrm{Cl}(K_n)[p^\infty] \right)^\vee \to X(\mathbb{Z}_p(1)) \to \left(\varinjlim_n (\mathcal{O}_{K_n}^\times \otimes \mathbb{Z}_p) \right)^\vee \to 0$$

5. Reflection theorem

Let's return to the case $K_n = \mathbb{Q}(\mu_{p^n})$.

5.1. **Local conditions.** We think of Λ^{cycl} as a *p-adic interpolation of the Tate twists $\mathbb{Z}_p(k)$*. Indeed, we have $G_\mathbb{Q}$-equivariant specializations $\mathrm{sp}_k \colon \Lambda^{cycl} \to \mathbb{Z}_p(k)$ given by $g \mapsto \epsilon_{cycl}^k(g)$. So we note the following quite confusing fact:

Proposition 5.1. *$H^1_{f,\{p\}}(\mathbb{Q}, \mathbb{T}_{\mathbb{Z}_p(1)}) = H^1_{f,\{p\}}(\mathbb{Q}, \mathbb{T}_{\mathbb{Z}_p}) \otimes \epsilon_{cycl}^{-1}$ as Λ^{cycl}-modules. Similarly, $H^1_{f,\{p\}}(\mathbb{Q}, \mathbb{W}_{\mathbb{Z}_p(1)}) = H^1_{f,\{p\}}(\mathbb{Q}, \mathbb{W}_{\mathbb{Z}_p}) \otimes \epsilon_{cycl}$ as Λ^{cycl}-modules.*

Proof. We have $\mathbb{T}_{\mathbb{Z}_p(1)} = \mathbb{Z}_p(1) \otimes_{\mathbb{Z}_p} \Lambda^{cycl} = \mathbb{Z}_p \otimes_{\mathbb{Z}_p} \Lambda^{cycl}(1)$. But note that we have a $G_\mathbb{Q}$-equivariant isomorphism of Λ^{cycl}-modules $\Lambda^{cycl}(1) \xrightarrow{\sim} \Lambda^{cycl}(\epsilon_{cycl}^{-1})$ where ϵ_{cycl} denotes a twist only on the Λ^{cycl}-action, not on the $G_\mathbb{Q}$ action. This is simply given by $g \mapsto \epsilon_{cycl}^{-1}(g)g$. Hence $\mathbb{T}_{\mathbb{Z}_p(1)} \xrightarrow{\sim} \mathbb{T}_{\mathbb{Z}_p} \otimes \epsilon_{cycl}^{-1}$. Similarly, $\mathbb{W}_{\mathbb{Z}_p(1)} \xrightarrow{\sim} \mathbb{W}_{\mathbb{Z}_p} \otimes \epsilon_{cycl}$. Finally, one can check that the local conditions outside p agree, since they are in fact trivial for both $\mathbb{W}_{\mathbb{Z}_p}$ and $\mathbb{W}_{\mathbb{Z}_p(1)}$, as we explain in what follows.

In fact, if $l \neq p$, then $H^1_f(\mathbb{Q}_l, \mathbb{T}_T) = 0$ for any T. If p^e is the largest power of p that divides $l-1$, then l splits completely over $K_e/\mathbb{Q}$, and each prime λ above l is totally inert in K_∞/K_e. Fix such λ, and let λ_n be the unique prime above it in K_n. We are looking at $\varinjlim_n H^1(k(\lambda_n), W^{I_{\lambda_n}})$. Now for any $c_n \in H^1(k(\lambda_n), W^{I_{\lambda_n}})$, choose a large enough so that $c_n(\mathrm{Frob}_{\lambda_n})$ is fixed by $G_{K_{n+a}}$. Then $c_n(\mathrm{Frob}_{\lambda_{n+a}}) = \mathrm{Nm}_{K_{n+a}/K_n} c_n(\mathrm{Frob}_{\lambda_n})$ by the cocycle condition. Choose b such that $p^b c_n(\mathrm{Frob}_{\lambda_n}) = 0$. Then the above says that the restriction of c_n to $H^1(k(\lambda_{n+a+b}), W^{I_{\lambda_{n+a+b}}})$ is zero. $\square$

Now let's discuss the local conditions above p.

Proposition 5.2. *$H^1_f(\mathbb{Q}_p, \mathbb{T}_{\mathbb{Z}_p}) = 0$ and $H^1_f(\mathbb{Q}_p, \mathbb{W}_{\mathbb{Z}_p(1)}) = H^1(\mathbb{Q}_p, \mathbb{W}_{\mathbb{Z}_p(1)})$.*

Proof. We have

$$H^1_f(K_{n,p}, \mathbb{Z}_p) = H^1_{unr}(K_{n,p}, \mathbb{Z}_p) = H^1(\mathbb{F}_{(p-1)p^n}, \mathbb{Z}_p) = \mathrm{Hom}(G_{\mathbb{F}_{(p-1)p^n}}, \mathbb{Z}_p)$$

[8] To be precise, one needs to consider the inverse/direct limit of the semi-local cohomology groups: for a place v of K, consider $H^1_f(K_{n,v}, ?) := \bigoplus_{w|v \text{ in } K_n} H^1_f(K_{n,w}, ?)$.

but then the transition maps are identified with the restrictions $G_{\mathbb{F}_{(p-1)p^n}} \to G_{\mathbb{F}_{(p-1)p^{n+1}}}$. And then we conclude $H^1_f(\mathbb{Q}_p, \mathbb{T}_{\mathbb{Z}_p}) = \mathrm{Hom}(G_{\mathbb{F}_{(p-1)p^\infty}}, \mathbb{Z}_p) = 0$.

The second claim follows from local duality. □

For $\mathbb{Z}_p(1)$, the local condition at p is more subtle: we have $0 \to \mu_{p-1} \to \mathcal{O}^\times_{\mathbb{Q}_p(\mu_{p^n})} \to H^1_f(\mathbb{Q}_p(\mu_{p^n}), \mathbb{Z}_p(1)) \to 0$, and so we are looking at $\varprojlim_{\mathrm{Nm}}(\mathcal{O}^\times_{\mathbb{Q}_p(\mu_{p^n})})$. This module can be very concretely described, as done by Coleman:

Theorem 5.3 ([Sha, Theorem 5.4.31])**.** *Fix a choice of norm-compatible roots of unity ζ_{p^n}. Then there exist an exact sequence of Λ^{cycl}-modules*

$$0 \to \mu_{p-1} \times \mathbb{Z}_p(1) \xrightarrow{(\xi,a)\mapsto(\xi\zeta^a_{p^n})_n} \varprojlim_{\mathrm{Nm}}(\mathcal{O}^\times_{\mathbb{Q}_p(\mu_{p^n})}) \xrightarrow{\mathrm{Col}} \Lambda^{cycl} \xrightarrow{\epsilon_{cycl}} \mathbb{Z}_p(1) \to 0.$$

The map Col is explicit, and we have explicit norm compatible cyclotomic units $C_\infty \subseteq \varprojlim_{\mathrm{Nm}}(\mathcal{O}^\times_{\mathbb{Q}_p(\mu_{p^n})})$. One can compute their image on the Coleman map:

Theorem 5.4 (Explicit reciprocity law, [Sha, Theorem 6.13])**.** *If $\chi\colon \Delta \to \mathbb{Z}_p^\times$ is even and nontrivial, then the image of $\mathrm{Col}(C^\chi_\infty) \in \Lambda^{cycl,\chi} = \Lambda$ is generated by a function $f(T)$ with $f((1+p)^k - 1) = L^*(1-k, \chi\omega^{-k})$ for all $k > 0$. In particular, we must have $\epsilon^k_{cycl}(f) = \epsilon^{1-k}_{cycl}(\mathscr{L}^\chi_{KL})$ for all $k \in \mathbb{Z}$.*

This result is a very explicit computation. It is also constructing the Kubota–Leopoldt p-adic L-function! Moreover, it gives an interpretation of $\epsilon^k_{cycl}(\mathscr{L}^\chi_{KL})$ for $k \in \mathbb{Z}$ *outside* the range of interpolation. For instance, it recovers the following formula.

Corollary 5.5 (Leopoldt)**.** *For $\chi\colon \Delta \to \mathbb{Z}_p^\times$ a nontrivial even character,*

$$\epsilon_{cycl}(\mathscr{L}^\chi_{KL}) = \frac{\sum_{a=1}^{p-1} \chi^{-1}(a) \log_p(1-\zeta^a_p)}{\sum_{a=1}^{p-1} \chi^{-1}(a)\zeta^a_p}.$$

5.2. Reflection theorem.

By the analysis of the local conditions above, we have

$$0 \to \mathrm{Sel}(\mathbb{Z}_p) \otimes \epsilon^{-1}_{cycl} \to \mathrm{Sel}(\mathbb{Z}_p(1)) \xrightarrow{\mathrm{loc}_p} H^1_f(\mathbb{Q}_p, \mathbb{T}_{\mathbb{Z}_p(1)})$$

and

$$0 \to S(\mathbb{Z}_p) \otimes \epsilon_{cycl} \to S(\mathbb{Z}_p(1)) \xrightarrow{\mathrm{loc}_p} H^1_{/f}(\mathbb{Q}_p, \mathbb{W}_{\mathbb{Z}_p}) \otimes \epsilon_{cycl}.$$

We can piece these together by global duality. Since $\mathrm{Sel}(\mathbb{Z}_p) = 0$, we get

$$0 \to \mathrm{Sel}(\mathbb{Z}_p(1)) \xrightarrow{\mathrm{loc}_p} H^1_f(\mathbb{Q}_p, \mathbb{T}_{\mathbb{Z}_p(1)}) \xrightarrow{\mathrm{loc}_p^\vee} X(\mathbb{Z}_p(1)) \otimes \epsilon_{cycl} \to X(\mathbb{Z}_p) \to 0.$$

Dividing by the cyclotomic units, we get

$$0 \to \frac{\mathrm{Sel}(\mathbb{Z}_p(1))}{C_\infty} \xrightarrow{\mathrm{loc}_p} \frac{H^1_f(\mathbb{Q}_p, \mathbb{T}_{\mathbb{Z}_p(1)})}{\mathrm{loc}_p(C_\infty)} \xrightarrow{\mathrm{loc}_p^\vee} X(\mathbb{Z}_p(1)) \otimes \epsilon_{cycl} \to X(\mathbb{Z}_p) \to 0.$$

Since C^χ_∞ is only nonzero if $\chi\colon \Delta \to \mathbb{Z}_p^\times$ is even and nontrivial, let's take such χ and consider

$$0 \to \frac{\mathrm{Sel}(\mathbb{Z}_p(1))^\chi}{C^\chi_\infty} \xrightarrow{\mathrm{loc}_p} \frac{H^1_f(\mathbb{Q}_p, \mathbb{T}_{\mathbb{Z}_p(1)})^\chi}{\mathrm{loc}_p(C^\chi_\infty)} \xrightarrow{\mathrm{loc}_p^\vee} X(\mathbb{Z}_p(1))^{\chi\omega^{-1}} \otimes \epsilon_{cycl} \to X(\mathbb{Z}_p)^\chi \to 0.$$

Now the explicit reciprocity law says that the second Λ-module is torsion. We already known the last one is also torsion. So all four modules are torsion, and we can compare their characteristic ideals.

From the description of $X(\mathbb{Z}_p(1))$, note that since $\chi\omega^{-1}$ is odd and not ω^{-1}, we have

$$\mathrm{Hom}\left(\varinjlim_n \mathrm{Cl}(K_n)[p^\infty]^{\omega\chi^{-1}}, \mathbb{Q}_p/\mathbb{Z}_p\right) \xrightarrow{\sim} X(\mathbb{Z}_p(1))^{\chi\omega^{-1}}$$

An exercise in algebra let us conclude from this that $\mathrm{Ch}\left(X(\mathbb{Z}_p(1))^\chi\right) = \iota(\mathrm{Ch}(X_\infty^{\chi^{-1}}))$, where $\iota\colon \Lambda \to \Lambda$ is the involution given by inversion $\iota(g) = g^{-1}$. More generally, the following is true.

Proposition 5.6 ([Was97, Proposition 15.32])**.** *If X is a finitely generated torsion Λ-module with $X/\nu_n X$ finite, then* $\mathrm{Ch}\left(\mathrm{Hom}(\varinjlim X/\nu_n X, \mathbb{Q}_p/\mathbb{Z}_p)\right) = \iota(\mathrm{Ch}(X))$.

The explicit reciprocity law says that

$$\mathrm{Ch}\left(\frac{H^1_f(\mathbb{Q}_p, \mathbb{T}_{\mathbb{Z}_p(1)})^\chi}{\mathrm{loc}_p(C_\infty^\chi)}\right) = (\mathrm{Tw}\circ\iota)(\mathscr{L}_{KL}^\chi)$$

where $\mathrm{Tw}\colon \Lambda \to \Lambda$ is $g \mapsto \epsilon_{cycl}(g)g$. So the above exact sequence tells us that

$$\frac{\mathrm{Ch}(E_\infty/C_\infty)^\chi}{\mathrm{Ch}(X_\infty^\chi)} = (\mathrm{Tw}\circ\iota)\left(\frac{(\mathscr{L}_{KL}^\chi)}{\mathrm{Ch}(X_\infty^{\omega\chi^{-1}})}\right).$$

That is, this proves:

Theorem 5.7 (Reflection Theorem)**.** *For $\chi \neq \omega^0, \omega^1$, the Iwasawa main conjecture for χ and $\omega\chi^{-1}$ are equivalent.*

References

[Sha] Romyar Sharifi. Iwasawa Theory, Lecture Notes. URL: https://www.math.ucla.edu/~sharifi/iwasawa.pdf.

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