Intoduction to Iwasawa theory

Hung Chiang

November 7, 2024

1 Iwasawa algebra of one variable

Let $F/\mathbb{Q}_p$ be a finite extension, $\mathcal{O} \subset F$ be the ring of integers, and $\varpi \subset \mathcal{O}$ be a uniformizer. Let $\Gamma \cong \mathbb{Z}_p$ be a topological group and γ. We may start with a $\mathbb{Z}_p$-Galois extension K_∞/K with Galois group Γ and define $K_n := (F_\infty)^{\Gamma^{p^n}}$, $\Gamma_n := \mathrm{Gal}(K_\infty/K_n) = \Gamma/\Gamma^{p^n}$.

Definition 1.

$$\Lambda = \mathcal{O}[[\Gamma]] := \varprojlim_n \mathcal{O}[\Gamma_n] = \varprojlim_n \mathcal{O}[\Gamma/\Gamma^{p^n}] \cong \varprojlim_n \mathcal{O}[T]/\langle (1+T)^{p^n} - 1\rangle$$

where the last isomorphism is given by $\gamma_0 \mapsto 1 + T$.

We will show that $\varprojlim_n \mathcal{O}[T]/\langle (1+T)^{p^n} - 1\rangle = \mathcal{O}[[T]]$.

Definition 2. Let $P \in \mathcal{O}[T]$. P is called a distinguished polynomial if P is non-constant, monic, and $P \equiv T^{\deg(P)} \pmod{\varpi}$.

Proposition 1 (Division Algorithm)**.** Suppose $P = a_0 + a_1 T + \cdots \in \mathcal{O}[[T]]$, $P \not\equiv 0 \pmod{\varpi}$, and $n = \min\{k \in \mathbb{N} \mid a_k \in \mathcal{O}^\times\}$. Then for every $f \in \mathcal{O}[[T]]$ there exists a unique pair (Q, R) where $Q \in \mathcal{O}[[T]]$ and $R \in \mathcal{O}[T]$ has degree smaller than n, such that

$$f = QP + R.$$

Theorem 1 (Weierstrass Preparation)**.** For every $f \in \mathcal{O}[[T]]$ there exists a unique triple $(u, U(T), P(T))$ where $u \in \mathbb{Z}_{\geq 0}$, $U \in \mathcal{O}[[T]]^\times$, and $P(T)$ is a distinguished polynomial, such that

$$f = \varpi^u PU.$$

It is easily seen that $\mathcal{O}[[T]]$ is a UFD of dimension 2 and a set of representatives of its irreducible elements are ϖ and all irreducible distinguished polynomials.

Theorem 2. Let $P_1, P_2, \cdots$ be a sequence of distinguished polynomials such that $P_n \in (\varpi, T)^n$ and $P_n \mid P_{n+1}$ for all $n \in \mathbb{N}$. We endow $\mathcal{O}[[T]]$ with the $\mathfrak{m}$-adic

topology and $\mathcal{O}[[T]]/(P_n)$ the p-adic topology. Then the natural map

$$\varphi : \mathcal{O}[[T]] \to \varprojlim_k \mathcal{O}[[T]]/(P_n)$$

is an isomorphism of topological $\mathcal{O}$-algebras.

Proof. Since $\mathcal{O}[[T]]/(P_n)$ is p-adically complete, it is isomorphic to $\varprojlim_\ell \mathcal{O}[[T]]/(P_n, \varpi^\ell)$ with each object endowed with discrete topology. Hence

$$\varprojlim_n \mathcal{O}[[T]]/(P_n) = \varprojlim_{n,\ell} \mathcal{O}[[T]]/(P_n, \varpi^\ell) = \varprojlim_n \mathcal{O}[[T]]/(P_n, \varpi^n),$$

where each $\mathcal{O}[[T]]/(P_n, \varpi^n)$ is given discrete topology. Since $(P_n, \varpi^n) \subset \mathfrak{m}^n$, it suffices to show that for every $n \in \mathbb{N}$ is a ℓ such that $\mathfrak{m}^\ell \subset (P_n, \varpi^n)$. This is true as the radical of (P_n, ϖ^n) is $\mathfrak{m}$. □

Let $P_n := (1+T)^{p^n} - 1$. Since $\mathcal{O}[T]/(P_n) \to \mathcal{O}[[T]]/(P_n)$ is an isomorphism by division algorithm, $\varprojlim_n \mathcal{O}[T]/\langle (1+T)^{p^n} - 1 \rangle = \mathcal{O}[[T]]$.

Limits and colimits of finite $\mathcal{O}[\Gamma]$-modules are naturally Λ-modules. Therefore we would like to study the structure of some class of Λ-modules.

Definition 3. Let M, N are Λ-modules. We say $M \sim N$ if there is a morphism $M \to N$ with finite kernel and cokernel.

$\sim$ defined above is not an equivalence relation. It defines an equivalence relation on the class of finitely generated torsion Λ-modules.

Example 1. $\mathfrak{m} \sim \Lambda$ but the converse does not hold. If f, g are coprime,

$$\Lambda/(fg) \to \Lambda/(f) \oplus \Lambda/(g), \ \Lambda/(f) \oplus \Lambda/(g) \xrightarrow{\begin{pmatrix} g & f \end{pmatrix}} \Lambda/(fg)$$

are both injective with finite cokernel.

Theorem 3. Let M be a finitely generated Λ-module. Then

$$M \sim \Lambda^r \oplus \left(\bigoplus_{i=1}^{s} \Lambda/(\varpi)^{n_i} \right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(f_j)^{m_j} \right)$$

For some r, s, t, n_i, m_j, and irreducible distinguished f_j. These are invariants of M.

When M is torsion, we define $Ch_\Lambda(M) = (\varpi^\mu f_M) \subset \Lambda^\times$ where μ is the sum of all n_i and f_M is the product of all $f_j^{m_j}$.

Lemma 1 (Nakayama's lemma)**.** Let X be a compact Λ-module. X is finitely generated iff $X/\mathfrak{m}\,X$ is finite. In this case, generators of $X/\mathfrak{m}\,X$ as abelian groups generates X as Λ-modules.

Proof. In light of the usual Nakayama's lemma, We should show that if X is compact and $\mathfrak{m}\,X = X$, $X = 0$. Fix $U \subset X$ an open neighborhood at 0. For every $x \in X$ there is an open neighborhood $x \in U_x$ and $n_x \geq 0$ such that $\mathfrak{m}^{n_x} U_x \subset U$. Since X is covered by finitely many U_x, $\mathfrak{m}^n X \subset U$ for some $n \geq 0$.

If $\mathfrak{m}\,X = X$, $\mathfrak{m}^n X = X$ for all n and we have that U can only be X. Therefore $X = 0$. □

2 Iwasawa's theorem

Let K be a number field, K_∞/K be a $\mathbb{Z}_p$-extension.

Proposition 2. K_∞/K is unramified outside all places lying above p.

Proof. Let v be a place and let I_v be the inertia group in the extension, which is a closed subgroup of Γ. I_v is trivial or Γ^{p^n} for some n. If v is archimedean, I_v has order 1 or 2, hence trivial in this case. If v is nonarchimeden, consider the completion of the extension. This is an abelian extension over K_v, whose Galois group is a quotient of the profinite limit of $K_v^\times$. Therefore, if I_v is not trivial, K_v is a finite extension of $\mathbb{Q}_p$. □

Lemma 2. Suppose K_∞/K_n is ramified. There is a n such that in K_∞/K_n, all primes that are ramified are totally ramified.

Proof. Find all I_v where $v|p$ and v is ramified in K_∞/K. Suppose their intersection is Γ^{p^n}. The assertion holds for this n. □

Definition 4. A_n is defined as the p-elementary part of the ideal class group of K_n. Let L_n/K_n be the maximal unramified p-extension. Then $\mathrm{Gal}(L_n/K_n) \cong A_n$. Let L_∞ be the union of all L_n, which is over K_∞.

If $m \geq n$, elements in A_n extends to elements in A_m and the norm map from K_m to K_n sends A_m to A_n. We set

$$A_\infty := \varinjlim_n A_n, X_\infty := \varprojlim_n A_n$$

Theorem 4 (Iwasawa)**.** There exists $n_0, \nu, \lambda \geq 0, \mu \geq 0$ such that for all $n \geq n_0$, $\log_p(|A_n|) = \lambda n + \mu p^n + \nu$.

Note that we may prove this by replacing K with any K_m. We may assume that in K_∞/K, all primes that are ramified are totally ramified.

With this assumption, each K_{n+1}/K_n is ramified. $K_{n+1} \cap L_n$, and all $K_m \cap L_n$

for $m > n$ are therefore K_n. The surjective map

$$A_{n+1} \cong \mathrm{Gal}(L_{n+1}/K_{n+1}) \to \mathrm{Gal}(L_n/K_n) \cong A_n$$

corresponds to the norm map by class field theory. We see that $A_n = \mathrm{Gal}(L_n K_\infty/K_\infty)$ and $\mathrm{Gal}(L_\infty/K_\infty) = \varprojlim_n A_n = X_\infty$.

Each A_n has a Γ_n-action: We lift $\gamma \in \Gamma_n = \mathrm{Gal}(K_n/K)$ to $\widetilde{\gamma} \in \mathrm{Gal}(L_n/K)$ and define $\gamma(x) := \mathrm{Ad}_{\widetilde{\gamma}}(x)$ for $x \in \mathrm{Gal}(L_n/K_n)$. All such liftings differ from elements in $\mathrm{Gal}(L_n/K_n)$ so $\gamma(x)$ is well-defined and give a group action. X_∞ is therefore a natural profinite module of $\Lambda := \mathbb{Z}_p[[\Gamma]]$. Let $G = \mathrm{Gal}(L_\infty/K_\infty)$. The Γ-action on X_∞ is given by lifting $\gamma \in \Gamma$ to $\widetilde{\gamma} \in G$ and apply conjugation on X_∞.

Let $\mathfrak{p}_1, \cdots, \mathfrak{p}_s$ be the prime ideals of K that are ramified in K_∞ and $I_1, \cdots, I_s$ be their respective inertia groups in G. Each $I_i \cap X$ is trivial and $I_i \to \Gamma$ surjectively, so $I_i X = G$. We define $\sigma_i \in I_i$ be the element mapped to γ. There is a unique $a_i \in X$ such that $\sigma_i = a_i \sigma_1$. We write $G = \Gamma X = I_i X$.

Lemma 3.

$$[G, G] = (\gamma - 1)(X) = TX.$$

Proof. $(\gamma - 1)(X) \subset [G, G]$ by considering the action of Γ on X. Note that TX is closed and $\Gamma X/TX = \Gamma(X/TX)$ and it is abelian. □

Definition 5. $Y_0 \subset X$ is the $\mathbb{Z}_p$-submodule generated by $a_2, \cdots, a_s$ and TX. $P_n := 1 + \gamma + \gamma^2 \cdots + \gamma^{p^n - 1} = \dfrac{(1+T)^{p^n} - 1}{T}$.

Lemma 4.

$$X/P_n Y_0 \cong X_n.$$

Proof. Let $n = 0$. $X_0 = \mathrm{Gal}(L_0/K)$ and L_0/K is the maximal unramified abelian extension in L_∞/K. $\mathrm{Gal}(L/L_0)$ is therefore the closed subgroup generated by $I_1, \cdots, I_s$ and $[G, G]$. By definition of Y_0, the quotient of G by such subgroup is exactly X/Y_0.

For $n > 0$, we replace K by K_n. We have to replace γ with γ^{p^n}. With this, σ_i is replaced by $\sigma_i^{p^n}$. The equation

$$\sigma_i^{p^n} = P_n(a_i) \sigma_1^{p^n}$$

yields that a_i is replaced by $P_n(a_i)$, and $[G,G]$ is replaced by $(\gamma^{p^n}-1)(X) = P_nTX$. All these gives that Y_0 is replaced by P_nY_0. $\square$

Since $P_1 \in \mathfrak{m}$ and $X/P_1Y_0 \cong X_1$ is finite, we have that X is a finitely generated Λ-module.

For the general case, we choose e such that the assumption holds for K_∞/K_e and define Y_e be the Y_0 for K_e. Let $P_{n,e} := \dfrac{P_n}{P_e}$. We have $X_n \cong X/P_{n,e}Y_e$ for all $n \geq e$.

We compute $|M/P_{n,e}M|$ for some standard choices of M. Note that $P_{n,e}$ is a distinguished polynomial of degree $p^n - p^e$.

1. $M = \Lambda$. $|M/P_{n,e}M| = \infty$.

2. $M = \Lambda/(p^k)$. $M/P_{n,e}M$ is isomorphic to the space of polynomials in $\mathbb{Z}/p^k\mathbb{Z}$ with degree $< p^n - p^e$. The size is $p^{k(p^n-p^e)} = p^{kp^n+c}$ where $c = kp^e$.

3. $M = \Lambda/(f)$ for some distinguished f of degree d. If $(f, P_{n,e}) \neq 1$, $|M/P_{n,e}M| = \infty$. Suppose this does not happen. We have P_{n+2}/P_{n+1} acts by p times a unit on M for all $p^n \geq d$. Assume $n_0 > e$, $p^{n_0} \geq d$, $n \geq n_0$. We have $|M/P_{n,e}M| = p^{dn+c}$ for some constant c.

$$X \sim E = \Lambda^r \oplus \left(\bigoplus_{i=1}^{s} \Lambda/(\varpi)^{n_i}\right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(f_j)^{m_j}\right).$$

One can prove that if $M \sim N$ and $|M/P_{n,e}M| < \infty$ for all n, then $|N/P_{n,e}N| < \infty$ for all n and the ratio between the order of these tow quotients is a constant for $n >> 0$. Apply this to $M = Y_e$, $N = E$, use the computation above and $|A_n| = |X/Y_e||Y_e/P_{n,e}Y_e|$ and we get the theorem.

3 Iwasawa main conjecture for GL_1 over $\mathbb{Q}$

Let $\mathbb{Q}_\infty / \mathbb{Q}$ be the cyclotomic $\mathbb{Z}_p$-extension and $\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty / \mathbb{Q})$. Let $\Lambda = \mathbb{Z}_p[[\Gamma]]$. We fix a topological generator $\gamma \in \Gamma$. Let ω be the Teichmuller character and χ be the p-adic cyclotomic character.

We define $[\cdot] : \Gamma \to \Lambda^\times$ sending $\gamma \in \Gamma$ to the corresponding group-like element and ϵ_Λ the universal character of $G_\mathbb{Q}$ with value in Λ by $\epsilon_\Lambda : G_\mathbb{Q} \to \Gamma \xrightarrow{[\cdot]} \Lambda^\times$. This universal character is a p-adic family of characters over the weight space. Let $\zeta \in \mu_{p^\infty}(\overline{\mathbb{Q}_p})$. We define $\phi_{k,\zeta} \in \mathrm{Hom}(\Lambda, \overline{\mathbb{Q}_p})$ by the character on Γ sending γ to $\zeta\chi(\gamma)^k$. The evaluation of ϵ_Λ at the point $\phi_{\zeta,k}$ has the form $\psi_\zeta\omega^{-k}\chi^k$, where ψ_ζ is a character of order p-power.

Let ψ be an odd primitive Dirichlet character. The L-value $L(0, \psi\epsilon_\Lambda(\zeta, k)) = L(-k, \psi\psi_\zeta\omega^{-k})$ is interpolated by the Kubota-Leopoldt p-adic L-function

$$\mathcal{L}_\psi = \frac{g_\psi}{h_\psi} \in \mathrm{Frac}(\Lambda)$$

where $h_\psi = \xi\chi(\gamma)\gamma - 1$ if ψ has the form $\psi_\xi\omega^{-1}$, or 1 otherwise. At the classical point (ζ, k),

$$\mathcal{L}_\psi(\zeta, k) = L^{\{p\}}(0, \psi\epsilon_\Lambda(\zeta, k)).$$

More generally, we for a finite set of primes not including p, say Σ, we define the imprimitive p-adic L-function as follows:

$$g_\psi^\Sigma := g_\psi \times \prod_{\ell\in\Sigma}(1 - \ell^{-1}(\psi^{-1}\ell^{-1}\epsilon_\Lambda^{-1})(\mathrm{Frob}_\ell)),\ \mathcal{L}_\psi^\Sigma := \frac{g_\psi^\Sigma}{h_\psi}.$$

These imprimitive p-adic L-functions are designed to interpolate imprimitive special L-values at positive integers.

For every $k \geq 0$ and primitive Dirichlet characters ψ we define the following Selmer groups:

$$\mathrm{Sel}(\psi\chi^{-k})^\Sigma := \ker\left(H^1(\mathbb{Q}, \mathbb{Q}_p[\psi]/\,\mathbb{Z}_p[\psi](\psi\chi^{-k})) \xrightarrow{\mathrm{Res}} \prod_{\ell\notin\Sigma} H^1(I_\ell, \mathbb{Q}_p[\psi]/\,\mathbb{Z}_p[\psi](\psi\chi^{-k}))\right),$$

$$\mathrm{Sel}_\infty(\psi)^\Sigma := \ker\left(H^1(\mathbb{Q}, \Lambda[\psi]^*(\psi\epsilon_\lambda^{-1})) \xrightarrow{\mathrm{Res}} \prod_{\ell\notin\Sigma} H^1(I_\ell, \Lambda[\psi]^*(\psi\epsilon_\lambda^{-1}))\right),$$

and Iwasawa modules

$$X^{\Sigma}(\psi\chi^{-k}) := (\mathrm{Sel}(\psi\chi^{-k})^{\Sigma})^*,\ X^{\Sigma}_{\infty}(\psi) := (\mathrm{Sel}_{\infty}(\psi)^{\Sigma})^*$$

We omit Σ if it is the empty set. Roughly speaking, $X^{\Sigma}(\psi)$ catches an isotypic quotient of the Galois group of a maximal abelian pro-p-extension unramified outside Σ.

Proposition 3. Suppose for every $\ell \notin \{p\} \cup \Sigma$ we have that the order of ψ on I_ℓ is not a nontrivial p-power (for example, Σ contains all ramified primes). Then then there are isomorphisms

$$\mathrm{Sel}(\psi\psi_{\zeta}^{-1}\omega^k\chi^{-k})^{\Sigma} \cong (\mathrm{Sel}^{\Sigma}_{\infty}(\psi) \otimes \mathcal{O}[\zeta])[\gamma - (\zeta\chi^k)(\gamma)],$$

and dually

$$X(\psi\psi_{\zeta}^{-1}\omega^k\chi^{-k})^{\Sigma} \cong \frac{X^{\Sigma}_{\infty}(\psi) \otimes \mathcal{O}[\zeta]}{(\gamma - (\zeta\chi^k)(\gamma))X^{\Sigma}_{\infty}(\psi) \otimes \mathcal{O}[\zeta]}$$

unless $k = 0$ and $\psi = \psi_\zeta$ on $G_{\mathbb{Q}_p}$. In that exceptional case we have the short exact sequence

$$0 \to \mathrm{Sel}(\psi\psi_{\zeta}^{-1})^{\Sigma} \to \mathrm{Sel}^{\Sigma}_{\infty}(\psi) \otimes \mathcal{O}[\zeta])[\gamma - \zeta] \to \mathbb{Q}_p[\psi]/\,\mathbb{Z}_p[\psi] \to 0$$

and the dual one.

The exceptional case reflects the fact that the interpolated special value is 0 for those cases. That never happen when ψ is odd.

Iwasawa proved that $X^{\Sigma}_{\infty}(\psi)$ is a finite Λ_ψ-module and moreover, if ψ is odd, is torsion. If moreover $p \nmid [\mathbb{Q}(\mu_N) : \mathbb{Q}]$ where N is the conductor of ψ, $X^{\Sigma}_{\infty}(\psi)$ has no nontrivial finite order $\Lambda[\psi]$-submodules.

Let (f^{Σ}_{ψ}) be the characteristic ideal of $X^{\Sigma}_{\infty}(\psi)$.

Theorem 5 (Iwasawa's Main Conjecture for $\mathbb{Q}$)**.** Let ψ be an odd primitive Dirichlet character. Then

$$(f^{\Sigma}_{\psi}) = (g^{\Sigma}_{\psi^{-1}}) \subset \Lambda[\psi] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p\,.$$

If p does not divide the order of ψ, then moreover they are the same in $\Lambda[\psi]$.

One side of the divisibility is given by Iwasawa's analytic number formula: When we fix a conductor and add on the λ-invariant over all odd Dirichlet character factoring through $\mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})$, we get the same number for f and g, and also the equality for μ-invariant when $p \nmid [\mathbb{Q}(\mu_N) : \mathbb{Q}]$. Since such formula is not discovered in general, the divisibility obtained from this side is often done by finding an Euler system.