Introduction to Iwasawa Theory

Cooper Young

October 20th, 2021

Abstract

This exposition follows Francesc Castella's lecture as part of UC Santa Barbara's seminar on Iwasawa theory for elliptic curves at supersingular primes.

Iwasawa Theory

Let us start with the original theory that Kenkichi Iwasawa developed. To do so, we begin with a number field F, a prime $p > 2$, and a Galois extension F_∞/F where $\mathrm{Gal}(F_\infty/F) \cong \mathbb{Z}_p$. By recognizing the p-adic integers as a projective limit, we can find a decomposition $F_\infty = \bigcup_{n\geq 0} F_n$ such that $\mathrm{Gal}(F_n/F) \cong \mathbb{Z}/p^n\mathbb{Z}$.

Now, we utilize the decomposition $\mathbb{Z}_p^\times \cong \Delta \times \Gamma$, where Δ is a small torsion subgroup and Γ is a procyclic, pro-p group. Specifically, $\Delta \cong \{\pm 1\}$ if $p = 2$ and otherwise Δ is isomorphic to the $(p-1)$-th roots of unity, and $\Gamma \cong \mathbb{Z}_p$. As a classic example, we can consider $F = \mathbb{Q}$, which gives us the following extension of fields

$$\begin{tikzcd}
 & F_\infty = \mathbb{Q}(\zeta_{p^\infty}) \arrow[dl, dash] \arrow[ddr, dash] & \\
\mathbb{Q}_\infty := (F_\infty)^\Delta \arrow[ddr, dash] & & \\
 & & \mathbb{Q}(\zeta_p) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

where $\zeta_n = e^{\frac{2\pi i}{n}}$.

Theorem (Iwasawa 1959 [2]): Let $A_n = Cl(\mathcal{O}_{F_n})[p^\infty]$ be the p-Sylow subgroup of the ideal class group of F_n, and let $\#A_n = p^{e_n}$. Then there exist integers λ, ν, and $\mu \geq 0$ such that

$$e_n = \lambda n + \mu p^n + \nu$$

as n goes to infinity.

This is the classical framework for Iwasawa theory, and for the remainder of this section, we will sketch the proof of the theorem above. The ideas presented in this proof provide the inspiration for the generalization of Iwasawa theory to other settings.

By class field theory, we can use the Artin map to construct an isomorphism $A_n \cong \mathrm{Gal}(L_n/F_n)$, where L_n is the maximal abelian p-extension of F_n which is unramified at all primes in F_n. We call L_n the *p-Hilbert Class field* of F_n. Now let $L_\infty := \bigcup_{n\geq 0} L_n$, which allows us to define $X_\infty := \mathrm{Gal}(L_\infty/F_\infty)$. This will be an abelian pro-p group, making it a $\mathbb{Z}_p$-module. Furthermore, it has a continuous Γ-action defined by

$$\gamma \cdot x = \tilde{\gamma} x \tilde{\gamma}^{-1} \qquad \forall \gamma \in \Gamma, \;\; x \in X_\infty$$

where $\tilde{\gamma} \in X_\infty$ is chosen such that $\tilde{\gamma}|_{F_\infty} = \gamma$. This makes X_∞ a module over the completed group ring $\Lambda := \mathbb{Z}_p[[\Gamma]]$, which we call the *Iwasawa Algebra.* We can visualize our fields with the following diagram:

$$\begin{tikzcd}
L_\infty \arrow[d, dash] \arrow[d, bend left=60, dash, "X_\infty"] \\
F_\infty \arrow[d, dash] \arrow[d, bend right=60, dash, "\Delta \times \Gamma"'] \\
F
\end{tikzcd}$$

Let's take a moment to to get a sense of what Λ "looks like." If we let $\gamma \in \Gamma$ be a topological generator (that is, $\langle\gamma\rangle$ is dense in Γ), then there exists a unique isomorphism

$$\begin{aligned} \Phi &: \Lambda \xrightarrow{\sim} \mathbb{Z}_p[[T]] \\ \Phi &: \gamma \longmapsto 1 + T \end{aligned}$$

With this isomorphism in mind, we recall the fact that $\mathbb{Z}_p[[T]]$ is a UFD, which is complete and Noetherian with maximal ideal (p, T).

Now that we've identified Λ, we want to find out more about X_∞. We start by noting that X_∞ is a finitely generated Λ-module. Next, we use the structure theorem of finitely generated modules over integrally closed Noetherian rings. This theorem implies that there exists a Λ-module homomorphism

$$X_\infty \longrightarrow \Lambda^r \oplus \bigoplus_{i=1}^{s} \Lambda/\big(f_i(T)\big)^{a_i} \oplus \bigoplus_{j=1}^{t} \Lambda/\big(p\big)^{b_j}$$

with finite kernel and cokernel, where $r, s, t \geq 0$ and $f_i(T) = T^{\deg(f_i)} + pg_i(T)$ are irreducible distinguished polynomials. This theorem and its proof are similar to the structure theorem of finitely generated modules over PIDs, but we have to use this slightly weaker version since $\mathbb{Z}_p[[T]]$ isn't a PID.

The next major result that can be shown is that X_∞ is actually a Λ-torsion module, meaning that $r = 0$ in our equation above. Furthermore, we are ready to state that the variables λ and μ from Iwasawa's Theorem come from:

$$\begin{aligned} \lambda &= \sum_{i=1}^{s} a_i \cdot \deg(f_i) \\ \mu &= \sum_{j=1}^{t} b_j \end{aligned}$$

The proof proceeds by showing that

$$(X_\infty)_{\Gamma_n} \cong \mathrm{Gal}(L_n/F_n)$$

where Γ_n is the unique subgroup of Γ with $[\Gamma : \Gamma_n] = p^n$ and $(X_\infty)_{\Gamma_n}$ is the largest quotient submodule of X_∞ on which Γ_n acts trivially. That is, if γ is our topological generator of Γ, then Γ_n is topologically generated by γ^{p^n} and $(X_\infty)_{\Gamma_n} = X_\infty/(\gamma^{p^n} - 1)X_\infty$. Recall that we've already identified $A_n = Cl(\mathcal{O}_{F_n})[p^\infty]$ with $\mathrm{Gal}(L_n/F_n)$, so to study the size of A_n, we can study the left-hand size of our isomorphism above by applying the structure theorem we mentioned earlier to $(X_\infty)_{\Gamma_n}$. For more details, see the original paper or one of many expositions such as [1].

Now that we have walked through Iwasawa'a theorem, we can turn our attention to his main conjecture. Before we state the conjecture, we must define the *characteristic power series* of X_∞, which is the principal ideal

$$\mathrm{Char}_\Lambda(X_\infty) := \Big(p^\mu \prod_{i=1}^{s} f_i(T)^{a_i}\Big) \subseteq \Lambda$$

We can now state

Iwasawa's Main Conjecture (Iwasawa 1969): Let F_∞ be a cyclotomic $\mathbb{Z}_p$-extension of $F = \mathbb{Q}(\mu_p)$. Then with the notion from above,

$$\mathrm{Char}_\Lambda(X_\infty) = \big(\zeta_p\big)$$

where ζ_p is the p-adic analogue of the Riemann zeta function.

Mazur's Program

After Iwasawa's main conjecture was proved in 1984 by Barry Mazur and Andrew Wiles [8], mathematicians set out to prove generalizations of the conjecture to other situations. For instance, if we replace the p-adic zeta function with a different L-function, what should be our new Λ-module X_∞? For the remainder of this section, we will explore what happens when the p-adic zeta function is replaced by the Hasse–Weil zeta function, and we will see how Iwasawa's theory translates to the world of elliptic curves.

Let $E/\mathbb{Q}$ be an elliptic curve and $p > 2$ be a good ordinary prime for E (that is, $p \nmid a_p$ where $a_p := p + 1 - \#\tilde{E}(\mathbb{F}_p)$). Consider a cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty/\mathbb{Q}$ which gives us a tower of extensions $\mathbb{Q}_n/\mathbb{Q}$ where $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong \mathbb{Z}/p^n\mathbb{Z}$. This setup is similar to what we did in the previous section, but whereas before we focused on the class group, we will now focus on the Selmer group.

For an algebraic field extension $L/\mathbb{Q}$, the p^∞-Selmer group fits into the following short exact sequence

$$0 \longrightarrow E(L) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \mathrm{Sel}_{p^\infty}(E/L) \longrightarrow Ш(E/L)[p^\infty] \longrightarrow 0$$

and recall that $\mathrm{Sel}_{p^\infty}(E/L) \subset H^1(G_L, E[p^\infty])$. If we let $\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$, it can be shown that $\mathrm{Sel}_{p^\infty}(E/L)$ is a $\Lambda = \mathbb{Z}_p[[\Gamma]]$-module. This makes it a reasonable substitute for what we called X_∞ in the previous section. However, this turns out not to be the correct analogous object. Instead, we have to introduce the *Pontryagin dual* of a module M, which is the group of continuous homomorphisms $M^\wedge := \mathrm{Hom}_{\mathrm{cts}}(M, \mathbb{Q}_p/\mathbb{Z}_p)$. With this, we have

Mazur's Main Conjecture: Let $\chi_\infty := \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_\infty)^\wedge$ be the Pontryagin dual of our p^∞-Selmer group. Then χ_∞ is Λ-torsion and

$$\mathrm{Char}_\Lambda(\chi_\infty) = \big(L_p(E)\big) \subset \Lambda$$

where $L_p(E)$ is the p-adic analogue of the Hassel-Weil L-function of E.

This conjecture is also called Iwasawa's main conjecture for elliptic curves at ordinary primes. The conjecture has been proven for many cases through the work of Kato [3], Skinner, and Urban [7]. There are numerous consequences of this conjecture:

First, we can use Mazur's Control Theorem [5] to show that $L(E,1) \neq 0$ if and only if $\#\,\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) < \infty$. Now we can utilize the the conjecture to show that the p^∞-Selmer group is finite if and only if $\mathrm{rank}_\mathbb{Z}\, E(\mathbb{Q}) = 0$ and $\#\text{Ш}(E/\mathbb{Q})[p^\infty] < \infty$. Together, this proves the Birch Swinnerton-Dyer conjecture in rank 0.

Second, if $L(E,1) \neq 0$, then we can use Iwasawa theory to show that

$$\mathrm{ord}_p\Big(\frac{L(E,1)}{\Omega}\Big) = \mathrm{ord}_p\Big(\frac{\#\text{Ш}(E/\mathbb{Q}) \cdot C_{E/\mathbb{Q}}}{(\#E(\mathbb{Q})_{\mathrm{tors}})^2}\Big)$$

which proves the p-part of the Birch Swinnerton-Dyer formula.

Supersingular Case

One small but important assumption that we made in the last section is that our prime p was an ordinary prime for E. Now, suppose that $p|a_p$ (where as before $a_p = p + 1 - \#\tilde{E}(\mathbb{F}_p)$). When trying to model the situation like we did above, we run into two problems. First off, we have two p-adic L-functions, $L_{p,\alpha}(E), L_{p,\beta}(E) \in \mathbb{Q}_p[[T]]$, where α and β are the roots of $x^2 - a_p x + p$. And while $\Lambda \subset \mathbb{Q}_p[[T]]$, because $\mathrm{ord}_p(\alpha), \mathrm{ord}_p(\beta) > 0$, we actually have $L_{p,\alpha}(E), L_{p,\beta}(E) \notin \Lambda$. The second issue is that now, $\chi_\infty = \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_\infty)^\wedge$ is not actually a Λ-torsion module.

Luckily for us, Pollack and Kobayashi found the right function and object X_∞ so that we get a result which mirrors Iwasawa's original main conjecture. We let $a_p = 0$, which happens automatically for primes $p > 3$ which are supersingular.

Pollack showed in [6] that there exists a function $L_p^\pm \in \Lambda$ which satisfies

$$L_{p,\alpha}(E) = L_p^+ \log_p^+ + L_p^- \log_p^- \alpha \qquad\qquad L_{p,\beta}(E) = L_p^+ \log_p^+ - L_p^- \log_p^- \alpha$$

and note that we have $\beta = -\alpha$.

Now focusing on our Selmer group, we have by definition $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_\infty) = \varinjlim \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_n)$ where $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_n) = \{c \in H^1(G_{\mathbb{Q}_n}, E[p^\infty]) \,\big|\, \mathrm{res}_v(c) \in \delta_v\big(E(\mathbb{Q}_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p\big)\}$. But as we said above, this module is too big. Instead, Kobayashi showed in [4] that we should use

$$\mathrm{Sel}^\pm_{p^\infty}(E/\mathbb{Q}_n) = \{c \in \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_n) \mid \mathrm{res}_v(c) \in \delta_v\big(E^\pm(\mathbb{Q}_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p\big)\}$$

for $p|v$, where $E^\pm(\mathbb{Q}_{n,v})$ is Kobayashi's $\pm$-norm subgroup. With these objects, we are now ready to state

Kobayashi's Main Conjecture: With the notation from this section, $\chi_\infty^\pm := \mathrm{Sel}_{p^\infty}^\pm(E/\mathbb{Q}_\infty)^\wedge$ is a Λ-torsion module and

$$\mathrm{Char}_\Lambda\left(\chi_\infty^\pm\right) = \left(L_p^\pm\right)$$

which has been proven in many cases due to work done by Pollack, Rubin, and Wan.

References

[1] Brown, Jim. *An Introduction to Iwasawa Theory.* http://www.math.caltech.edu/ jimlb/iwasawa.pdf (2006).

[2] Iwasawa, Kenkichi. *On Γ-extensions of algebraic number fields.* Bull. Amer. Math. Soc. 65 (1959), p. 183Ð226.

[3] Kato, Kazuya. *p-adic Hodge theory and values of zeta functions of modular forms.* Astérisque, tome 295 (2004), p. 117-290.

[4] Kobayashi, Shin-ichi. *Iwasawa theory for elliptic curves at supersingular primes.* Inventiones mathematicae, 152 (2003), p. 1-36.

[5] Mazur, Barry. *Rational points of abelian varieties with values in towers of number fields.* Inventiones Mathematicae, 18 (1972), p. 183Ð266,

[6] Pollack, Robert. *On the p-adic L-function of a modular form at a supersingular prime.* Duke Mathematical Journal, 118 (2003) no. 3, 523-558

[7] Skinner, Christopher, and Eric Urban. *The Iwasawa main conjectures for* GL_2 . Invent. Math. 195 (2014), no. 1, 1-277.

[8] Wiles, Andrwe, and Barry Mazur. *Class fields of abelian extensions of* $\mathbb{Q}$. Invent. Math. 76 (1984), p. 179-330.