A p-ADIC INTERPOLATIVE PROPERTY OF IWASAWA LAMBDA INVARIANTS

JORDAN SCHETTLER

1. FINITELY GENERATED Λ-MODULES

Fix a prime p. Let $\Lambda = \mathbb{Z}_p[[T]]$. Then Λ is a regular local ring with maximal ideal $\mathfrak{m} = (p, T)$. In particular, Λ is a unique factorization domain. As a topological ring, Λ is complete with respect to the $\mathfrak{m}$-adic topology.

Suppose X is a finitely generated Λ-module. Then the Structure Theorem[1] implies that there is a Λ-module homomorphism

$$\phi\colon X \longrightarrow \Lambda^r \oplus \bigoplus_{i=1}^{s} \frac{\Lambda}{(p^{m_i})} \oplus \bigoplus_{j=1}^{t} \frac{\Lambda}{(f_j(T)^{n_j})}$$

which is a pseudo-isomorphism (i.e., $\ker(\phi)$, $\operatorname{coker}(\phi)$ are finite) and where each $f_j(T) \in \mathbb{Z}_p[T]$ is irreducible with $f_j(T) \equiv T^{\deg(f_j)} \pmod{p}$. Here r, s, t are nonnegative integers while m_i, n_j are positive integers. We endow X with the topology under which $(p^m, \omega_n)X$ forms a basis of open submodules of X where $\omega_n = (T+1)^{p^n} - 1$. Now suppose, in addition, that X is Λ-torsion, so that $r = 0$. We define the characteristic polynomial

$$f_X(T) := \prod_{i=1}^{s} p^{m_i} \prod_{j=1}^{t} f_j(T)^{n_j}$$

and the Iwasawa invariants

$$\lambda(X) := \deg(f_X)$$
$$\mu(X) := \operatorname{ord}_p(f_X).$$

Consider some $\Gamma \cong \mathbb{Z}_p$ as topological groups. Choosing to write Γ multiplicatively, the only nontrivial closed subgroups are $\Gamma_n := \Gamma^{p^n}$, and we have

$$\Gamma/\Gamma_n \cong \mathbb{Z}/(p^n)$$

[1] due first to Iwasawa for completed group algebras and then restated by Serre for power series rings

for all $n \geq 0$. We define the completed group algebra as the topological inverse limit

$$\mathbb{Z}_p[[\Gamma]] := \varprojlim_n \mathbb{Z}_p[\Gamma/\Gamma_n].$$

Fix a topological generator γ of $\Gamma = \overline{\langle\gamma\rangle} = \gamma^{\mathbb{Z}_p}$. There is an isomorphism of topological $\mathbb{Z}_p$-algebras

$$\Lambda \longrightarrow \mathbb{Z}_p[[\Gamma]]\colon\ T \mapsto \gamma - 1,$$

and it is convenient to interpret Λ as both a power series and a completed group algebra. It is important to note, however, that for a finitely generated, torsion $\mathbb{Z}_p[[\Gamma]]$-module X, the characteristic polynomial $f_X(T)$ depends upon the choice of topological generator $\gamma \leftrightarrow T + 1$, but the Iwasawa invariants $\lambda(X)$, $\mu(X)$ do not depend on this choice.

2. Two Main Examples

Example 1. Suppose F is a number field. Let F_∞ denote the cyclotomic $\mathbb{Z}_p$-extension of F, i.e., the unique subfield of $\cup_n F(\zeta_{p^n})$ containing F such that $\mathrm{Gal}(F_\infty/F) \cong \Gamma$. The subfields of F_∞ containing F form a tower

$$F \subseteq F_1 \subseteq F_2 \subseteq \ldots \subseteq F_\infty$$

such that $\mathrm{Gal}(F_n/F) \cong \mathbb{Z}/(p^n)$ for all $n \geq 1$. Let M_n denote the maximal, unramified abelian p-extension of F_n, i.e., the p-Hilbert class field. Then

$$X(F_n) := \mathrm{Gal}(M_n/F_n)$$

is naturally a discrete module over $\mathbb{Z}_p[\mathrm{Gal}(F_n/F)] \cong \mathbb{Z}_p[\Gamma/\Gamma_n]$. Hence

$$X(F_\infty) := \varprojlim_n X(F_n)$$

is a compact module over $\mathbb{Z}_p[[\Gamma]] \cong \Lambda$. It turns out that $X(F_\infty)$ is a finitely generated, torsion Λ-module, and this along with the Structure Theorem can be used to prove Iwasawa's growth formula for the p-parts of the class numbers $|\mathrm{Cl}(F_n)|$ of F_n:

$$\mathrm{ord}_p\,|\mathrm{Cl}(F_n)| = \lambda(F)n + \mu(F)p^n + \nu(F)$$

for all $n \gg 0$ where $\lambda(F) = \lambda(X(F_\infty))$, $\mu(F) = \mu(X(F_\infty))$, and $\nu(F) \in \mathbb{Z}$ is a constant. Iwasawa conjectured $\mu(F) = 0$. This conjecture has been verified when F is abelian over $\mathbb{Q}$ or an imaginary quadratic field. The conjecture also holds for finite p-extensions of F whenever the conjecture holds for F itself.

Example 2. Now suppose E is an elliptic curve over a number field F, and let $E[p^\infty]$ denote the p-primary part of the group $E(\overline{F})$ for a fixed algebraic closure $\overline{F}$ of F. For any algebraic extension M/F, we take $G_M = \mathrm{Gal}(\overline{M}/M)$ and let $H^\bullet(M,-) = H^\bullet(G_M,-)$ denote group cohomology. Define the p-primary Selmer group by

$$\mathrm{Sel}_E(M)_p = \ker\left(H^1(M, E[p^\infty]) \longrightarrow \prod_v H^1(M_v, E[p^\infty])/\mathrm{im}(\kappa_v)\right)$$

where the product runs over all places v of M and

$$\kappa_v \colon E(M_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \to H^1(M_v, E[p^\infty])$$

is the Kummer homomorphism for M_v, the completion of M at v. This Selmer group appears in the short exact sequence

$$0 \longrightarrow E(M) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \mathrm{Sel}_E(M)_p \longrightarrow Ш_E(M)_p \longrightarrow 0 \tag{2.1}$$

where $Ш_E(M)_p$ is the p-primary part of the (conjecturally finite) Shafarevich-Tate group.

There is a $\mathbb{Z}_p$-linear action of Γ on $H^1(F_\infty, E[p^\infty])$ described by

$$g \cdot [\phi] := [\phi_{\widetilde{g}}]$$

where $\widetilde{g} \in G_F$ extends $g \in \Gamma$ and for $\alpha \in G_{F_\infty}$

$$\phi_{\widetilde{g}}(\alpha) = \widetilde{g}\phi(\widetilde{g}^{-1}\alpha\widetilde{g}).$$

It is easy to show that $\mathrm{Sel}_E(F_\infty)_p$ is Γ-invariant under this action, and every $[\phi] \in H^1(F_\infty, E[p^\infty])$ is killed by a power of $T \leftrightarrow \gamma - 1$, so $\mathrm{Sel}_E(F_\infty)_p$ is a torsion Λ-module which we give the discrete topology. We define the p-Pontryagin dual functor on topological Λ-modules via

$$(-)^\vee := \mathrm{Hom}_{\mathrm{cont}}(-, \mathbb{Q}_p/\mathbb{Z}_p)$$

with the compact-open topology, the diagonal Γ action, and where Γ acts trivially on $\mathbb{Q}_p/\mathbb{Z}_p$. This functor interchanges compact and discrete Λ-modules. Thus

$$X_E(F_\infty) := \mathrm{Sel}_E(F_\infty)_p^\vee$$

is a compact Λ-module. In fact, $X_E(F_\infty)$ is always finitely generated over Λ. Assume now that E has good ordinary reduction at all primes of F lying above p. Mazur conjectured that $X_E(F_\infty)$ is Λ-torsion in this case, and he proved the Control Theorem, which states that the natural maps

$$\mathrm{Sel}_E(F_n)_p \longrightarrow \mathrm{Sel}_E(F_\infty)_p^{\Gamma_n}$$

have finite kernel and cokernel of bounded order as n varies where F_n is the nth layer in the cyclotomic $\mathbb{Z}_p$-extension F_∞ of F. The exact sequence in Equation 2.1 shows that

$$\text{Sel}_E(F)_p \text{ is finite} \iff E(F), Ш_E(F)_p \text{ are finite,} \tag{2.2}$$

and, in this case, we have an analog of Iwasawa's Growth Formula:

$$\text{ord}_p |Ш(F_n)| = \lambda_E(F)n + \mu_E(F)p^n + \nu_E(F)$$

for all $n \gg 0$ where $\lambda_E(F) = \lambda(X_E(F_\infty)) - \text{rank}\, E(F_\infty)$, $\mu = \mu(X_E(F_\infty))$ and $\nu_E(F) \in \mathbb{Z}$ is a constant. Mazur's Control Theorem along with Nakayama's Lemma for compact Λ-modules can be used to show that $X_E(F_\infty)$ is indeed finitely generated and torsion over Λ when $\text{Sel}_E(F)_p$ is finite. The modularity theorem shows that Mazur's conjecture is true when E is defined over $\mathbb{Q}$ and F is an abelian number field by the work of Rubin (for CM-fields) and Kato (in general).

If E' is another elliptic curve over F which is isogenous to E, then $\lambda_E(F) = \lambda_{E'}(F)$, but $\mu_E(F)$ may be different than $\mu_{E'}(F)$ and, in fact, there is a precise formula relating these μ-invariants due to Peter Schneider. It is conjectured that when $F = \mathbb{Q}$, there is an isogenous elliptic curve E' such that $\mu_{E'}(F) = 0$, but there are counterexamples to the analogous statement when $F \neq \mathbb{Q}$.

3. Statements

Lemma 3. *Let X be a finitely generated Λ-module. Then X is finitely generated over $\mathbb{Z}_p$ if and only if X is Λ-torsion with $\mu(X) = 0$.*

Proof. This follows immediately from the Structure Theorem. □

Theorem 4. *Let X be a finitely generated, compact Λ-module with a $\mathbb{Z}_p$-linear action of a cyclic group G of order p^n where $n \geq 1$. Take G_p to be the order p subgroup of G. Suppose that $Y := X_{G_p}$ is Λ-torsion with $\mu(Y) = 0$. Then X is Λ-torsion with $\mu(X) = 0$ and*

$$\lambda(X) \equiv \lambda(Y) \pmod{p^{n-1}(p-1)}.$$

Moreover, we have a 'Kida formula'

$$\lambda(X) = p\lambda(Y) - (p-1)\chi(X) \tag{4.1}$$

where

$$\chi(-) := \dim_{\mathbb{F}_p} H^2(G_p, -) - \dim_{\mathbb{F}_p} H^1(G_p, -)$$

is the Euler characteristic for G_p.

Proof. Let g be a generator of G, so that $g_p := g^{p^{n-1}}$ is a generator of G_p. Note that $\mathbb{Z}_p G_p$ is a compact local ring with maximal ideal $\mathfrak{m}_p = (p, g_p - 1)$. By assumption and the lemma, $Y = X/(g_p - 1)X$ is finitely generated over $\mathbb{Z}_p$, so $X/\mathfrak{m}_p X$ is finitely generated over $\mathbb{Z}_p$ and whence over $\mathbb{Z}_p G_p$. Thus Nakayama's lemma implies that X is finitely generated over $\mathbb{Z}_p G_p$ and whence over $\mathbb{Z}_p$. Using the lemma in the reverse direction then shows that X is Λ-torsion with $\mu(X) = 0$.

The canonical exact sequence of G-modules

$$X \longrightarrow Y \longrightarrow 0$$

induces an exact sequence of adjoints

$$0 \longrightarrow \alpha(Y) \longrightarrow \alpha(X)$$

where $\alpha(-) = \mathrm{Hom}_{\mathbb{Z}_p}(-, \mathbb{Z}_p)$. The adjoints $\alpha(X)$, $\alpha(Y)$ are G-modules via the usual diagonal action and are Λ-modules via $(\lambda \cdot \psi)(x) = \psi(\lambda x)$ for $\lambda \in \Lambda$ and homomorphisms ψ. With this module structure, $\alpha(X)$, $\alpha(Y)$ are finitely generated, torsion Λ-modules with the same Iwasawa invariants as X, Y, respectively. Moreover, there are no nontrivial homomorphisms from a finite group into $\mathbb{Z}_p$, so $\alpha(X)$, $\alpha(Y)$ are $\mathbb{Z}_p G$-modules which are free of finite rank over $\mathbb{Z}_p$. In particular, $\alpha(Y)$ is isomorphic to $\alpha(X)^{G_p}$, the $\mathbb{Z}_p$-pure submodule of $\alpha(X)$ which is annihilated by $g^{p^{n-1}} - 1$. Thus the quotient $Q := \alpha(X)/\alpha(Y)$ is free of finite rank over $\mathbb{Z}_p$ and is annihilated by $\Phi_{p^n}(g)$ where Φ_{p^n} is the p^nth cyclotomic polynomial. Therefore Q is a torsion free module over the ring

$$\frac{\mathbb{Z}_p G}{\Phi_{p^n}(g)\mathbb{Z}_p G} \cong \mathbb{Z}_p[\theta_{p^n}]$$

where θ_{p^n} is a primitive p^nth root of unity in $\overline{\mathbb{Q}_p}$. Now $\mathbb{Z}_p[\theta_{p^n}]$ is a PID, so, in fact, Q is free of finite rank over $\mathbb{Z}_p[\theta_{p^n}]$. Hence we have a short exact sequence of $\mathbb{Z}_p$-modules

$$0 \longrightarrow \alpha(Y) \longrightarrow \alpha(X) \longrightarrow \mathbb{Z}_p[\theta_{p^n}]^{\oplus r} \longrightarrow 0$$

for some nonnegative integer r. Taking $\mathbb{Z}_p$-ranks yields

$$\lambda(X) = \lambda(Y) + rp^{n-1}(p-1), \tag{4.2}$$

which proves the congruence. Using the same reasoning as above we obtain an exact sequence of $\mathbb{Z}_p G_p$-modules

$$0 \longrightarrow \alpha(Y) \longrightarrow \alpha(X) \longrightarrow \left(\frac{\mathbb{Z}_p G_p}{\Phi_p(g_p)\mathbb{Z}_p G_p}\right)^{\oplus rp^{n-1}} \longrightarrow 0.$$

Now we use duality and the additivity of the Euler characteristic χ to obtain

$$\begin{aligned}(4.3)\qquad \chi(X) &= -\chi(\alpha(X)) \\ &= -\chi(\alpha(Y)) - rp^{n-1}\chi(\mathbb{Z}_p G_p) + rp^{n-1}\chi(\Phi_p(g_p)\mathbb{Z}_p G_p) \\ &= -\lambda(Y) + rp^{n-1}.\end{aligned}$$

Combining 4.2 and 4.3 gives

$$\frac{\lambda(X) - \lambda(Y)}{p-1} = rp^{n-1} = \lambda(Y) + \chi(X)$$

which yields the 'Kida formula' 4.1. □

Combining the above theorem with results from [Iwa81] and [HM99], we get the following consequence.

Corollary 5. *Fix a prime $p \geq 5$. Let F_∞ be the cyclotomic $\mathbb{Z}_p$-extension of an abelian number field F and $E/\mathbb{Q}$ be an elliptic curve having good, ordinary reduction at all primes of F lying over p. Suppose L, K are number fields with cyclotomic $\mathbb{Z}_p$-extensions $L_\infty \supset K_\infty \supseteq F_\infty$ such that L_∞/F_∞ is cyclic of degree p^n for $n \geq 1$ and L_∞/K_∞ is cyclic of degree p. Then*

$$\begin{aligned}\lambda(L) &= p\lambda(K) + (p-1)(\chi(\mathcal{O}_{L_\infty}^\times) + |S|) \\ &\equiv \lambda(K) \pmod{p^{n-1}(p-1)}\end{aligned}$$

where $\chi(-)$ denotes the Euler characteristic for $\mathrm{Gal}(L_\infty/K_\infty)$ and S is the set of primes in L_∞ which ramify in L_∞/K_∞ and do not lie over p. If, in addition, $\mu_E(F) = 0$, then

$$\begin{aligned}\lambda_E(L) &= p\lambda_E(K) + (p-1)(|P_1| + 2|P_2|) \\ &\equiv \lambda_E(K) \pmod{p^{n-1}(p-1)}\end{aligned}$$

where P_1 is the set of primes in S at which E has split, multiplicative reduction and P_2 is the set of primes w in S at which E has good reduction and $E(L_\infty, w)[p] \neq 0$.

REFERENCES

[HM99] Yoshitaka Hachimori and Kazuo Matsuno, *An analogue of Kida's formula for the Selmer groups of elliptic curves*, J. Algebraic Geom. **8** (1999), no. 3, 581–601.

[Iwa81] Kenkichi Iwasawa, *Riemann-Hurwitz formula and p-adic Galois representations for number fields*, Tohoku Math. J. (2) **33** (1981), no. 2, 263–288.