A $p$-ADIC INTERPOLATIVE PROPERTY OF IWASAWA LAMBDA INVARIANTS

JORDAN SCHETTLER

1. FINITELY GENERATED $\Lambda$-MODULES

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

Suppose $X$ is a finitely generated $\Lambda$-module. Then the Structure Theorem implies that there is a $\Lambda$-module homomorphism

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

which is a pseudo-isomorphism (i.e., $\ker(\phi)$, $\coker(\phi)$ 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 $\Lambda$-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

$$\lambda(X) := \deg(f_X)$$
$$\mu(X) := \ord_p(f_X).$$

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

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

\footnote{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

\[
\mathbb{Z}_p[[\Gamma]] := \lim_{\leftarrow n} \mathbb{Z}_p[\Gamma/\Gamma_n].
\]

Fix a topological generator \( \gamma \) of \( \Gamma = \langle \gamma \rangle = \gamma\mathbb{Z}_p \). There is an isomorphism

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

and it is convenient to interpret \( \Lambda \) as both a power series and a completed group algebra. It is important to note, however, that for a finitely generated, torsion \( \mathbb{Z}_p \)-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 \( F_\infty \) denote the cyclotomic \( \mathbb{Z}_p \)-extension of \( F \), i.e., the unique subfield of \( \bigcup_n F(\zeta_{p^n}) \) containing \( F \) such that \( \text{Gal}(F_\infty/F) \cong \Gamma \). The subfields of \( F_\infty \) containing \( F \) form a tower

\[
F \subseteq F_1 \subseteq F_2 \subseteq \ldots \subseteq F_\infty
\]

such that \( \text{Gal}(F_n/F) \cong \mathbb{Z}/(p^n) \) 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

\[
X(F_n) := \text{Gal}(M_n/F_n)
\]

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

\[
X(F_\infty) := \lim_{\leftarrow n} X(F_n)
\]

is a compact module over \( \mathbb{Z}_p[[\Gamma]] \cong \Lambda \). It turns out that \( X(F_\infty) \) is a finitely generated, torsion \( \Lambda \)-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 \( |\text{Cl}(F_n)| \) of \( F_n \):

\[
\text{ord}_p |\text{Cl}(F_n)| = \lambda(F)n + \mu(F)p^n + \nu(F)
\]

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 \( G_M = \text{Gal}(\overline{M}/M) \) and let \( H^*(M,-) = H^*(G_M,-) \) denote group cohomology. Define the \( p \)-primary Selmer group by

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

where the product runs over all places \( v \) of \( M \) and

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

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

\[
0 \to E(M) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \text{Sel}_E(M)_p \to \text{III}_E(M)_p \to 0
\]

(2.1)

where \( \text{III}_E(M)_p \) is the \( p \)-primary part of the (conjecturally finite) Shafarevich-Tate group.

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

\[
g \cdot [\phi] := [\phi_{\tilde{g}}]
\]

where \( \tilde{g} \in G_F \) extends \( g \in \Gamma \) and for \( \alpha \in G_{F_\infty} \)

\[
\phi_{\tilde{g}}(\alpha) = \tilde{g} \phi(\tilde{g}^{-1} \alpha \tilde{g}).
\]

It is easy to show that \( \text{Sel}_E(F_\infty)_p \) is \( \Gamma \)-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 \( \text{Sel}_E(F_\infty)_p \) is a torsion \( \Lambda \)-module which we give the discrete topology. We define the \( p \)-Pontryagin dual functor on topological \( \Lambda \)-modules via

\[
(-)^\vee := \text{Hom}_{\text{cont}}(-, \mathbb{Q}_p/\mathbb{Z}_p)
\]

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

\[
X_E(F_\infty) := \text{Sel}_E(F_\infty)^\vee_p
\]

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

\[
\text{Sel}_E(F_n)_p \to \text{Sel}_E(F_\infty)^\Gamma_n
\]
have finite kernel and cokernel of bounded order as $n$ varies where $F_n$ is the $n$th layer in the cyclotomic $\mathbb{Z}_p$-extension $F_\infty$ of $F$. The exact sequence in Equation 2.1 shows that

$$\text{Sel}_E(F)_p$$

is finite $\iff$ $E(F), \text{III}_E(F)_p$ are finite,

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

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

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 $\Lambda$-modules can be used to show that $X_E(F_\infty)$ is indeed finitely generated and torsion over $\Lambda$ 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 $\mu$-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 $\Lambda$-module. Then $X$ is finitely generated over $\mathbb{Z}_p$ if and only if $X$ is $\Lambda$-torsion with $\mu(X) = 0$.

**Proof.** This follows immediately from the Structure Theorem. \qed

**Theorem 4.** Let $X$ be a finitely generated, compact $\Lambda$-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 $\Lambda$-torsion with $\mu(Y) = 0$. Then $X$ is $\Lambda$-torsion with $\mu(X) = 0$ and

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

Moreover, we have a ‘Kida formula’

$$\lambda(X) = p\lambda(Y) - (p - 1)\chi(X)$$

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 \( g_p := g_p^{-1} \) is a generator of \( G_p \). Note that \( \mathbb{Z}_p G_p \) is a compact local ring with maximal ideal \( m_p = (p, g_p - 1) \). By assumption and the lemma, \( Y = X / ((g_p - 1)X) \) is finitely generated over \( \mathbb{Z}_p \), so \( X / m_p X \) 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 \( \mathbb{Z}_p \) and whence over \( \mathbb{Z}_p G_p \). Using the lemma in the reverse direction then shows that \( X \) is \( \Lambda \)-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 \( \alpha(-) = \text{Hom}_{\mathbb{Z}_p}( -, \mathbb{Z}_p) \). The adjoints \( \alpha(X), \alpha(Y) \) are \( G \)-modules via the usual diagonal action and are \( \Lambda \)-modules via \( (\lambda \cdot \psi)(x) = \psi(\lambda x) \) for \( \lambda \in \Lambda \) and homomorphisms \( \psi \). With this module structure, \( \alpha(X), \alpha(Y) \) are finitely generated, torsion \( \Lambda \)-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 \( \alpha(X)^{\mathbb{G}_p} \), the \( \mathbb{Z}_p \)-pure submodule of \( \alpha(X) \) which is annihilated by \( g_p^{p^n - 1} - 1 \). 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 \( \Phi_p^n \) is the \( p^n \)th 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 \( \theta_p^n \) is a primitive \( p^n \)th root of unity in \( \mathbb{Q}_p \). 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

\[
\lambda(X) = \lambda(Y) + rp^{n-1}(p - 1),
\]

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 $\chi$ to obtain

\[(4.3) \quad \chi(X) = -\chi(\alpha(X)) = -\chi(\alpha(Y)) - rp^{n-1}\chi(\mathbb{Z}_p G_p) + rp^{n-1}\chi(\Phi_p(g_p)\mathbb{Z}_p G_p) = -\chi(Y) + rp^{n-1}.
\]

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 $F_\infty$ 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 $L_\infty \supseteq K_\infty \supseteq F_\infty$ such that $L_\infty/F_\infty$ is cyclic of degree $p^n$ for $n \geq 1$ and $L_\infty/K_\infty$ is cyclic of degree $p$. Then

\[
\lambda(L) = p\lambda(K) + (p - 1)(\chi(O_{L_\infty}^\times) + |S|) \\
\equiv \lambda(K) \pmod{p^{n-1}(p - 1)}
\]

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

\[
\lambda_E(L) = p\lambda_E(K) + (p - 1)(|P_1| + 2|P_2|) \\
\equiv \lambda_E(K) \pmod{p^{n-1}(p - 1)}
\]

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**
