IWASAWA THEORY OF ELLIPTIC CURVES

A THESIS SUBMITTED FOR THE COMPLETION OF REQUIREMENTS FOR THE DEGREE OF

BACHELOR OF SCIENCE (RESEARCH)

BY

SUDHARSHAN K V
UNDERGRADUATE PROGRAMME
INDIAN INSTITUTE OF SCIENCE

भारतीय विज्ञान संस्थान

UNDER THE SUPERVISION OF

PROF. MAHESH KAKDE
DEPARTMENT OF MATHEMATICS, INDIAN INSTITUTE OF SCIENCE

Abstract: We study Mazur's development of the Iwasawa theory of elliptic curves by drawing parallels to classical Iwasawa theory. We motivate the involvement of the Selmer and Tate-Shafarevich groups, and present Mazur's control theorem along with some of its consequences.

1. Introduction

Iwasawa theory involves the study of the growth of arithmetic objects in a tower of number fields. Classical Iwasawa theory concerns the study of the p-parts of the ideal class groups of the number fields inside the tower of a $\mathbb{Z}_p$-extension: Let F be a number field and let F_∞/F be a $\mathbb{Z}_p$-extension. Let

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n \subseteq \cdots \subseteq F_\infty$$

be the tower determined by the extension F_∞/F, so that $\mathrm{Gal}(F_n/F) \cong \mathbb{Z}/p^n\mathbb{Z}$ for all $n \geq 0$. Let A_n denote the p-part of the ideal class group of the number field F_n. Iwasawa proved the following result about the growth of the order of A_n.

Theorem 1.1 (Iwasawa, 1959)**.** *There exist non-negative integers λ, μ and an integer ν such that*

$$|A_n| = p^{\mu p^n + \lambda n + \nu}$$

for all sufficiently large n.

Alternatively, one can look at arithmetic objects attached to number fields that pertain to elliptic curves. Mazur studied the ranks of the Mordell-Weil groups of an elliptic curve in a tower of number fields: Given a number field K and an elliptic curve E defined over K, the group $E(K)$ of K-rational points of E is called a Mordell-Weil group. It is a finitely generated abelian group due to the Mordell-Weil theorem. Therefore, we can write

$$E(K) \cong \mathbb{Z}^r \oplus \Delta,$$

where Δ, the collection of torsion points of $E(K)$, is a finite group. The rank of $E(K)$ is its rank as an abelian group.

We can study the ranks of elliptic curves through their Selmer groups. The focus of this thesis is to study the Galois-theoretic behavior of the p-primary parts of the Selmer groups $\mathrm{Sel}_E(F_n)$ for the tower

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n \subseteq \cdots \subseteq F_\infty$$

inside the $\mathbb{Z}_p$ extension F_∞/F. An important result in this regard is Mazur's Control Theorem (Theorem 4.1).

We can also study the Tate-Shafarevich groups $Ш_E(K)$ for $K = F_0, F_1, \ldots, F_n, \ldots$. The following result on the sizes of the Tate-Shafarevich groups in a tower is reminiscent of Iwasawa's theorem.

Proposition 1.2. *Let F be a number field, and let E be an elliptic curve having good, ordinary reduction at all primes of F above p. Let $F_\infty = \bigcup F_n$ be a $\mathbb{Z}_p$-extension of F. Suppose that $\mathrm{Sel}_E(F_\infty)_p$ is Λ-cotorsion, and that $Ш_E(F_n)_p$ is finite for all n. Then, there exist integers λ, μ and ν such that*

$$|Ш_E(F_n)_p| = p^{\lambda n + \mu p^n + \nu}$$

for all $n >> 0$.

We present this result as a consequence of Theorem 4.1, assuming $E(F_n)$ is finite for all n. Dropping this assumption lengthens the proof considerably.

2. Selmer Groups

Let E be an elliptic curve over a field L of characteristic zero. For any $n \geq 1$, the multiplication by n map is an isogeny: So we have an exact sequence

$$0 \to E[n](\overline{L}) \to E(\overline{L}) \to E(\overline{L}) \to 0.$$

Taking the cohomology long exact sequence, we extract the Kummer exact sequence

$$0 \to E(L)/nE(L) \to H^1(L, E[n](\overline{L})) \to H^1(L, E(\overline{L}))[n] \to 0.$$

This sequence limits to the exact sequence $n \to \infty$, we have the exact sequence

$$0 \to E(L) \otimes \mathbb{Q}/\mathbb{Z} \to H^1(L, E(\overline{L})_{\mathrm{tor}}) \to H^1(L, E(\overline{L})) \to 0.$$

For an algebraic extension $K/\mathbb{Q}$, one can consider an elliptic curve over K as an elliptic curve over the completions K_v of K at a place v. We have a commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & E(K)\otimes\mathbb{Q}/\mathbb{Z} \arrow[r, "\kappa"] \arrow[d, "a_v"] & H^1(K, E(\overline{K})_{\mathrm{tor}}) \arrow[r, "\lambda"] \arrow[d, "b_v"] & H^1(K, E(\overline{K}) \arrow[r] \arrow[d, "c_v"] & 0 \\ 0 \arrow[r] & E(K_v)\otimes\mathbb{Q}/\mathbb{Z} \arrow[r, "\kappa_v"] & H^1(K_v, E(\overline{K}_v)_{\mathrm{tor}}) \arrow[r, "\lambda_v"] & H^1(K_v, E(\overline{K}_v) \arrow[r] & 0. \end{tikzcd}$$

The Selmer group $\mathrm{Sel}_E(K)$ is the subgroup of elements of $H^1(K, E(\overline{K})_{\mathrm{tor}})$ which become trivial under the composite map $c_v \circ \lambda$ for all places v.

The Selmer group is closely related to the images of the Kummer maps $\kappa_v : E(K_v)\otimes\mathbb{Q}/\mathbb{Z} \to H^1(K_v, E(K_v)_{\mathrm{tor}})$. The relation

$$\mathrm{Sel}_E(K) = \ker\left(H^1(K, E(\overline{K})_{\mathrm{tor}}) \to \prod_v \frac{H^1(K_v, E(\overline{K}_v)_{\mathrm{tor}})}{\mathrm{im}(\kappa_v)}\right)$$

is evident from the above commutative diagram, and it follows that the p-primary subgroup of $\mathrm{Sel}_E(K)$, denoted $\mathrm{Sel}_E(K)_p$, fits into the exact sequence

$$0 \to \mathrm{Sel}_E(K)_p \to H^1(K, E[p^\infty]) \to \prod_v \frac{H^1(K_v, E[p^\infty])}{\mathrm{im}(\kappa_v)},$$

where $\kappa_v : E(K)\otimes\mathbb{Q}_p/\mathbb{Z}_p \to H^1(K_v, E[p^\infty])$ is the Kummer map corresponding to the p-primary subgroup $E[p^\infty]$ of E_{tor}.

The Selmer group is determined completely by the G_K-module $E[p^\infty]$ and the images of the Kummer maps κ_v. Assume E has good, ordinary reduction at p: So there is an exact sequence

$$0 \to \mathcal{F}[p^\infty] \to E[p^\infty] \xrightarrow{\pi} \tilde{E}[p^\infty] \to 0,$$

where $\pi : E[p^\infty] \to \tilde{E}[p^\infty]$ is the reduction map and $\mathcal{F}[p^\infty]$ is the kernel of the reduction map. Let $\epsilon_v : H^1(K_v, \mathcal{F}[p^\infty]) \to H^1(K_v, E[p^\infty])$ be the natural map induced by the inclusion $\mathcal{F}[p^\infty] \to E[p^\infty]$. The following proposition describes $\mathrm{im}(\kappa_v)$ in certain cases.

Proposition 2.1.

1. *Let E/K_v be an elliptic curve defined over an algebraic extension $K_v/\mathbb{Q}_l$ for a prime $l \neq p$. Then, $E(K_v)\otimes\mathbb{Q}_p/\mathbb{Z}_p = 0$.*
2. *Let E/K_v be an elliptic curve defined over $K_v = \mathbb{R}$ or $K_v = \mathbb{C}$. Then, $E(K_v)\otimes\mathbb{Q}_p/\mathbb{Z}_p = 0$.*
3. *Let E/K_v be an elliptic curve defined over a finite extension $K_v/\mathbb{Q}_p$. Suppose that E has good, ordinary reduction at v. Then, $\mathrm{im}(\kappa_v) = \mathrm{im}(\epsilon_v)_{\mathrm{div}}$.*
4. *Let K_v be an extension of $\mathbb{Q}_p$ with finite residue field. Assume further that the profinite degree of $K_v/\mathbb{Q}_p$ is divisible by p^∞ - so there are finite subextensions $L_v/\mathbb{Q}_p$ with degree divisible by p^n for n unbounded. Then, $\mathrm{im}(\kappa_v) = \mathrm{im}(\epsilon_v)$.*

Remark 2.2. In the course of showing (3), one can also show that $\mathrm{im}(\epsilon_v)/\,\mathrm{im}(\kappa_v)$ is a finite cyclic group whose order divides the size of $\tilde{E}(k_v)_p$, where k_v is the residue field of K_v, and $\tilde{E}$ is the reduction of E modulo v.

2.1. **Tate-Shafarevich Groups.** Let E be an elliptic curve defined over an algebraic extension $K/\mathbb{Q}$. The Tate-Shafarevich group $Ш_E(K)$ measures the failure of the local-global principle for principal homogeneous spaces of E. More precisely, we define the Tate-Shafarevich group as

$$Ш_E(K) = \ker\left(H^1(K, E(\overline{K})) \to \prod_v H^1(K_v, E(\overline{K}_v))\right).$$

This group fits into an exact sequence with the Selmer group:

$$0 \to E(K)\otimes\mathbb{Q}/\mathbb{Z} \to \mathrm{Sel}_E(K) \to Ш_E(K) \to 0.$$

Taking the p-parts of these groups, one has the short exact sequence

$$0 \to E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}_E(K)_p \to \text{Ш}_E(K)_p \to 0.$$

In particular, the finiteness of $\mathrm{Sel}_E(K)_p$ is equivalent to the finiteness of $E(K)$ and $\text{Ш}_E(K)_p$.

3. Λ-Modules

We shall denote by Λ the power series ring in one variable with coefficients in $\mathbb{Z}_p$: $\Lambda = \mathbb{Z}_p[[T]]$. Let $\mathfrak{m} = (p, T)$ be the unique maximal ideal of Λ. We consider Λ as a topological ring under the $\mathfrak{m}$-adic topology.

Let Γ denote the additive (topological) group $\mathbb{Z}_p$, and fix a topological generator γ_0 of Γ. Let A be a p-primary, abelian group (hence a $\mathbb{Z}_p$-module) with a continuous action of Γ. The group $\widehat{A} = \mathrm{Hom}(A, \mathbb{Q}_p/\mathbb{Z}_p)$ along with the compact-open topology (when $\mathbb{Q}_p/\mathbb{Z}_p$ is given the discrete topology) is called the Pontryagin dual of A. The Pontryagin dual $\widehat{A}$ is a pro-p group. If B is a pro-p group, then the Pontryagin dual $\widehat{B} = \mathrm{Hom}_{\mathrm{cont}}(B, \mathbb{Q}_p/\mathbb{Z}_p)$ of B is a discrete, p-primary abelian group. We can turn A and $\widehat{A}$ into $\mathbb{Z}_p[T]$-modules by letting T act as $\gamma_0 - 1$. In fact, this action turns A into a Λ-module, as is captured by the result below.

Proposition 3.1. *We have an isomorphism of topological rings*

$$\mathbb{Z}_p[[T]] = \mathbb{Z}_p[[\Gamma]] = \varprojlim \mathbb{Z}_p[\Gamma/\Gamma^{p^n}],$$

given by $T \mapsto \gamma_0 - 1$ for some fixed topological generator γ_0 of Γ.

Although Λ is not a PID, there is a structure theorem for Λ-modules.

Theorem 3.2. *Let X be a finitely generated Λ-module. Then there exist irreducible elements $f_1(T), \ldots, f_n(T)$, and integers $r, e_1, \ldots, e_n \geq 0$, and a Λ-module homomorphism*

$$\varphi : X \to \Lambda^r \oplus (\oplus_{i=1}^n \Lambda/(f_i(T)^{e_i}))$$

with finite kernel and cokernel. The integers $r, e_1, \ldots, e_n$, and the ideals $(f_i(T))$ are uniquely determined by X.

Remark 3.3. Such a homomorphism with finite kernel and cokernel is called a *pseudo-isomorphism*. The existence of a pseudo-isomorphism between two finitely generated Λ-modules is not an equivalence relation, although it becomes an equivalence when we restrict ourselves to finitely generated, torsion Λ-modules.

There is an analogue of Nakayama's lemma for Λ-modules.

Lemma 3.4. *Let X be a Λ-module. Then*

(1) X is finitely generated if and only if $X/\mathfrak{m}X$ is finite.
(2) X is torsion if X/TX is finite.

We will denote the elements $(1+T)^{p^n} - 1$ in Λ by ω_n. Let X be a torsion Λ-module, so we have a pseudo-isomorphism

$$X \to \oplus_{i=1}^n \Lambda/(f_i(T)^{e_i}),$$

where we may take the elements f_i to be either p or distinguished polynomials. The ideal generated by the element $f_X(T) = \prod f_i(T)^{e_i}$ is called the *characteristic ideal* of X. This ideal is important in the context of Iwasawa Main Conjectures. We define the Iwasawa λ-invariant λ_X to be the degree of $f_X(T)$, and the Iwasawa μ-invariant μ_X to be the maximum μ such that $f_X(T)$ is divisible by p^μ. An ingredient in Iwasawa's proof of Theorem 1.1 is the following.

Proposition 3.5. *Let X be a finitely generated, torsion Λ-module. Suppose that $X/\omega_n X$ is finite for all n. Let μ, λ be the Iwasawa invariants of X. Then,*

$$|X/\omega_n X| = p^{\mu p^n + \lambda n + O(1)}$$

for all $n >> 0$.

4. Mazur's Control Theorem

Theorem 4.1 (Mazur's Control Theorem)**.** *Let F be a number field, and let E/F be an elliptic curve. Suppose p is a prime, and that E has good, ordinary reduction on all primes of F above p. Let $F_\infty = \bigcup_n F_n$ be a $\mathbb{Z}_p$-extension of F. Then, the natural maps*

$$\mathrm{Sel}_E(F_n)_p \to \mathrm{Sel}_E(F_\infty)_p^{\mathrm{Gal}(F_\infty/F_n)}$$

have finite kernel and cokernels. Their orders are bounded as $n \to \infty$.

We say a Λ-module A is Λ-cotorsion if its Pontryagin dual $\widehat{A}$ is a torsion Λ-module.

Corollary 4.2. *Assume that $\mathrm{Sel}_E(F)_p$ is finite. Then $\mathrm{Sel}_E(F_\infty)_p$ is Λ-cotorsion. Consequently, the rank of $E(F_n)$ is bounded as n varies.*

Proof. Let $X = \mathrm{Hom}(\mathrm{Sel}_E(F_\infty)_p, \mathbb{Q}_p/\mathbb{Z}_p)$ be the Pontryagin dual of $\mathrm{Sel}_E(F_\infty)_p$. The finiteness of $\mathrm{Sel}_E(F)_p$ and Mazur's Control Theorem imply that $\mathrm{Sel}_E(F_\infty)_p^\Gamma$ is finite. The Pontryagin dual of the finite group $\mathrm{Sel}_E(F_\infty)_p^\Gamma$ is X/TX, the maximal quotient of X on which Γ acts trivially. By Nakayama's lemma for Λ-modules, X is a finitely generated, torsion Λ-module. It follows that the divisible part of $\mathrm{Sel}_E(F_\infty)_p$ is $(\mathbb{Q}_p/\mathbb{Z}_p)^\lambda$, so λ serves as an upper bound of the ranks of the Mordell-Weil groups $E(F_n)$. ☐

Remark 4.3. Without the assumption that $\mathrm{Sel}_E(F)_p$ is finite, Mazur conjectured that $\mathrm{Sel}_E(F_\infty)_p$ is Λ-cotorsion when F_∞/F is the cyclotomic $\mathbb{Z}_p$-extension of F. This result is known to be true (due to Kato) when $F/\mathbb{Q}$ is abelian and $E/\mathbb{Q}$ is a modular elliptic curve.

We have an analogue of Iwasawa's theorem for the growth of the Tate-Shafarevich groups.

Corollary 4.4. *Assume that $E(F_n)$ and $\text{Ш}_E(F_n)_p$ are finite for all n. Then, there exist integers $\lambda, \mu \geq 0$ depending only on E and F_∞/F, such that*

$$|\text{Ш}_E(F_n)_p| = p^{\lambda n + \mu p^n + O(1)}$$

for all $n >> 0$.

Proof. As usual, let $\omega_n = (1+T)^{p^n} - 1$. Let X be the Pontryagin dual of $\mathrm{Sel}_E(F_\infty)_p$. Akin to the previous proof, $X/\omega_n X$ is the Pontryagin dual of $\mathrm{Sel}_E(F_\infty)_p^{\Gamma_n}$, so they have the same order. By Mazur's control theorem, the quantity $|\mathrm{Sel}_E(F_n)_p|/|X/\omega_n X|$ is bounded as n varies. Therefore, X is a finitely generated, torsion Λ-module such that $X/\omega_n X$ is finite for all n. By Proposition 3.5, if λ, μ are the Iwasawa invariants of X, then we have

$$|\text{Ш}_E(F_n)_p| = |\mathrm{Sel}_E(F_n)_p| = |X/\omega_n X| = p^{\lambda n + \mu p^n + O(1)}$$

for all $n >> 0$. ☐

We conclude with an outline of the proof of Theorem 4.1. Let

$$\mathcal{G}_E(K) = \mathrm{im}(H^1(K, E[p^\infty]) \to \prod_v H^1(K_v, E[p^\infty])/\mathrm{im}(\kappa_v)).$$

The kernel of this map is $\mathrm{Sel}_E(K)_p$. Since taking invariants is left exact, one has the commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & Sel_E(F_n)_p & \longrightarrow & H^1(F_n, E[p^\infty]) & \longrightarrow & \mathcal{G}_E(F_n) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle s_n} & & \downarrow{\scriptstyle h_n} & & \downarrow{\scriptstyle g_n} & & \\
0 & \longrightarrow & Sel_E(F_\infty)_p^{\Gamma_n} & \longrightarrow & H^1(F_\infty, E[p^\infty])^{\Gamma_n} & \longrightarrow & \mathcal{G}_E(F_\infty)^{\Gamma_n}. & &
\end{array}$$

The snake lemma yields the exact sequence

$$0 \to \ker(s_n) \to \ker(h_n) \to \ker(g_n) \to \mathrm{coker}(s_n) \to \mathrm{coker}(h_n). \tag{4.1}$$

Based on the description of the images of κ_v in Proposition 2.1, one can show the following.

(1) $\ker(h_n)$ *is finite of bounded order as n varies.*
(2) $\mathrm{coker}(h_n) = 0$.
(3) $\ker(g_n)$ *is finite of bounded order as n varies.*

From the sequence 4.1, it is now clear that $\ker(s_n)$ and $\mathrm{coker}(s_n)$ are finite, and their orders are bounded as n varies. ☐

References

[1] R. Greenberg, *Iwasawa theory for elliptic curves*, Lecture Notes in Mathematics-Springer Verlag-, (1999), pp. 51–144.
[2] ———, *Introduction to iwasawa theory for elliptic curves*, Arithmetic algebraic geometry (Park City, UT, 1999), 9 (2001), pp. 407–464.
[3] ———, *Iwasawa theory—past and present*, in Class field theory–its centenary and prospect, vol. 30, Mathematical Society of Japan, 2001, pp. 335–386.
[4] J. Neukirch and J. Neukirch, *Local class field theory*, Class Field Theory, (1986), pp. 37–71.
[5] R. Sharifi, *Iwasawa theory: a climb up the tower*, Notices of the American Mathematical Society, 66 (2019).