UNIVERSITY OF CALIFORNIA
Los Angeles

Structure of various Lambda-adic arithmetic cohomology groups

A dissertation submitted in partial satisfaction
of the requirements for the degree
Doctor of Philosophy in Mathematics

by

Jaehoon Lee

2019

ABSTRACT OF THE DISSERTATION

Structure of various Lambda-adic
arithmetic cohomology groups

by

Jaehoon Lee
Doctor of Philosophy in Mathematics
University of California, Los Angeles, 2019
Professor Haruzo Hida, Chair

In this thesis, we study the structure of various arithmetic cohomology groups as Iwasawa modules, made out of two different p-adic variations. In the first part, for an abelian variety over a number field and a $\mathbb{Z}_p$-extension, we study the relation between structure of the Mordell-Weil, Selmer and Tate-Shafarevich groups over the $\mathbb{Z}_p$-extension as Iwasawa modules.

In the second part, we consider the tower of modular curves, which is an analogue of the $\mathbb{Z}_p$-extension in the first part. We study the structure of the ordinary parts of the arithmetic cohomology groups of modular Jacobians made out of this tower. We prove that the ordinary parts of Λ-adic Selmer groups coming from one chosen tower and its dual tower have almost the same Λ-module structures. This relation of the two Iwasawa modules explains well the functional equation of the corresponding p-adic L-function. We also prove the cotorsionness of Λ-adic Tate-Shafarevich group under mild assumptions.

The dissertation of Jaehoon Lee is approved.

Romyar Thomas Sharifi

Chandrashekhar Khare

Don M. Blasius

Haruzo Hida, Committee Chair

University of California, Los Angeles

2019

To my mother

TABLE OF CONTENTS

ACKNOWLEDGMENTS

I am grateful to Don Blasius, Chandrashekhar Khare, Romyar Sharifi and Haruzo Hida for being part of the thesis committee.

I am indebted to my advisor Haruzo Hida for his continuous guidance, encouragement and support. I've had the privilege of meeting with him every week and sitting in his classes and seminars. My view towards math has been heavily influenced by conversations with him. Without his patient guidance over the years, I wouldn't even be close to finishing this thesis. He has been very generous in sharing his ideas and intuition. It has been a great honour for being his student.

My sincere thanks also go to Chandrashekhar Khare and Romyar Sharifi, who taught me a great deal of mathematics and provided me not only mathematical ideas, but also advice and encouragement.

I also want to thank Ashay Burungale, Francesc Castella, Jaclyn Lang, Haesang Sun, Chan-Ho Kim and Gyujin Oh for their encouragement, advice and for the many interesting conversations.

Most importantly, I would like to thank my mother, for her unconditional love.

VITA

2013	B.S. (Mathematics), Seoul National University.
2015–2018	Teaching Assistant, Mathematics Department, UCLA.

PUBLICATIONS

Structure of Mordell-Weil groups over $\mathbb{Z}_p$*-extensions.* 2018, Submitted.

CHAPTER 1

Introduction

1.1 Iwasawa theory of abelian varieties

The Iwasawa theory of abelian varieties (elliptic curves) was initiated by Mazur in his seminal paper [Maz72], where he proved that the p^∞-Selmer groups of an abelian variety A defined over a number field K are "well-controlled" over $\mathbb{Z}_p$-extensions if A satisfies a certain reduction condition at places dividing p. More precisely, let K_∞ be a $\mathbb{Z}_p$-extension of K and K_n be the n-th layer. We identify $\mathbb{Z}_p[\![\mathrm{Gal}(K_\infty/K)]\!]$ with $\Lambda := \mathbb{Z}_p[\![T]\!]$ by fixing a generator γ of $\mathrm{Gal}(K_\infty/K)$ and identifying it with $1+T$. Let $\mathrm{Sel}_{K_n}(A)_p$ be the classical p^∞-Selmer group over K_n attached to A. For the natural restriction map

$$S_n^A : \mathrm{Sel}_{K_n}(A)_p \to \mathrm{Sel}_{K_\infty}(A)_p[(1+T)^{p^n} - 1],$$

we have the following celebrated theorem.

Theorem 1.1.1 (Control Theorem)**.** *If either*

- (Mazur, *[Maz72]*) *A has a good ordinary reduction at all places of K dividing p*

or

- (Greenberg, *[Gre99, Proposition 3.7]*) *$K = \mathbb{Q}$ and A is an elliptic curve having multiplicative reduction at p*

then $\mathrm{Coker}(S_n^A)$ *is finite and bounded independent of n.*

Here the word "control" means that the Selmer group $\mathrm{Sel}_{K_n}(A)_p$ at each layer K_n can be described by the *one* object. Hence we can expect that the each Selmer group over K_n should behave in a certain regular way governed by the "limit" Selmer group $\mathrm{Sel}_{K_\infty}(A)_p$. For instance, we have the following consequence of the above theorem.

Proposition 1.1.2. *Assume either one of the condition of Theorem 1.1.1 and also assume that both $A(K_n)$ and $Ш^1_{K_n}(A)_p$ are finite for all n. Then there exist μ, λ, ν such that*

$$|\mathrm{Sel}_{K_n}(A)_p| = |Ш^1_{K_n}(A)_p| = p^{e_n} \quad (n >> 0)$$

where

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

The value $p^n\mu + n\lambda + \nu$ in the Proposition 1.1.2 naturally appears from the structure theory of Λ-modules. For a finitely generated Λ-module M, there is a Λ-linear map

$$M \to \Lambda^r \oplus \left(\bigoplus_{i=1}^{n} \frac{\Lambda}{g_i^{e_i}} \right) \oplus \left(\bigoplus_{j=1}^{m} \frac{\Lambda}{p^{f_j}} \right)$$

with finite kernel and cokernel where $r, n, m \geq 0$, $e_1, \cdots, e_n, f_1, \cdots, f_m$ are positive integers, and $g_1, \cdots, g_n$ are distinguished irreducible polynomial of Λ. The quantities

$$r, e_1, \cdots, e_n, f_1, \cdots, f_m, g_1, \cdots, g_n$$

are uniquely determined, and we call

$$E(M) := \Lambda^r \oplus \left(\bigoplus_{i=1}^{n} \frac{\Lambda}{g_i^{e_i}} \right) \oplus \left(\bigoplus_{j=1}^{m} \frac{\Lambda}{p^{f_j}} \right)$$

as an *elementary module of M* following [NSW00, Page 292]. The λ-invariant $\lambda(M)$ is defined as $\sum_{i=1}^{n} e_i \cdot \deg g_i$ and the μ-invariant $\mu(M)$ is defined as $f_1 + \cdots + f_m$.

In Proposition 1.1.2, the constants λ and μ are indeed the λ and μ-invariants of the module $\mathrm{Sel}_{K_\infty}(A)_p^\vee$, respectively and hence we can say that the module $E\left(\mathrm{Sel}_{K_\infty}(A)_p^\vee\right)$ gives the information about the arithmetic of the A at each finite level at once. Hence it is quite natural to ask questions about the *shape* of the Λ-module $E\left(\mathrm{Sel}_{K_\infty}(A)_p^\vee\right)$. We can also consider the same question for the Mordell-Weil group and the Tate-Shafarevich group, which fit into a natural exact sequence

$$0 \to A(K_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}_{K_\infty}(A)_p \to Ш^1_{K_\infty}(A)_p \to 0.$$

Instead of the characteristic ideals of the modules above which are usually studied because of their connection with the Iwasawa Main Conjecture, we study their Λ-module *structure*. Naively, we can ask the following question:

Question 1.1.3. *Can we describe the structure of*

$$E\left((A(K_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)^\vee\right), E\left(\mathrm{Sel}_{K_\infty}(A)_p^\vee\right), E\left(Ш^1_{K_\infty}(A)_p^\vee\right)?$$

Or can we find some relations among these three modules?

In this thesis, under suitable assumptions, we will prove an isomorphism

$$E\left(\mathrm{Sel}_{K_\infty}(A)_p^\vee\right) \simeq E\left(\mathrm{Sel}_{K_\infty}(A^t)_p^\vee\right)^\iota$$

of Λ-modules where ι is an involution of Λ satisfying $\iota(T) = \frac{1}{1+T} - 1$. (Theorem 2.4.3)

1.2 Towers of modular curves

In this thesis, we consider one more p-adic variation of arithmetic cohomologies which we briefly introduce here. For simplicity, in this introduction let $X_{r/\mathbb{Q}}$ be the (compactified) modular curve classifying the triples

$$(E, \mu_N \overset{\phi_N}{\hookrightarrow} E, \mu_{p^r} \overset{\phi_{p^r}}{\hookrightarrow} E[p^r])_{/R}$$

where E is an elliptic curve defined over a $\mathbb{Q}$-algebra R. We then have a natural covering map $X_{r+1} \to X_r$ for all r, which gives rise to the tower

$$\cdots X_{r+1} \to X_r \to \cdots X_2 \to X_1$$

of modular curves, which is an analogue of $\mathbb{Z}_p$-extension introduced in the last section.

Let $J_{r/\mathbb{Q}}$ be the Jacobians of X_r. For a number field K, we have the Mordell-Weil group $J_r(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p$, (geometric) p-adic Selmer group $\mathrm{Sel}_K(J_r)_p$ and the p-adic Tate-Shafarevich group $Ш^1_K(J_r)_p$ of the Jacobian J_r. We can apply the idempotent $e := \lim_{n\to\infty} U(p)^{n!}$ to those groups to take ordinary parts $(J_r(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{ord}$, $\mathrm{Sel}_K(J_r)^{ord}_p$ and $Ш^1_K(J_r)^{ord}_p$. (See Definition 3.3.3 for the precise definition.), which gives rise to

- $(J_\infty(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{ord} := \varinjlim_r (J_r(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{ord}$
- $\mathrm{Sel}_K(J_\infty)^{ord}_p := \varinjlim_r \mathrm{Sel}_K(J_r)^{ord}_p$
- $Ш^1_K(J_\infty)^{ord}_p := \varinjlim_r Ш^1_K(J_r)^{ord}_p$

via Picard functoriality. They are naturally Λ-modules on which we will give discrete topology. We call them as the Λ-adic Mordell-Weil group, Λ-adic Selmer group and the Λ-adic Tate-Shafarevich group in order. For the Selmer groups, we have the natural map

$$s_r : \mathrm{Sel}_K(J_r)^{ord}_p \to \mathrm{Sel}_K(J_\infty)^{ord}_p[\omega_r]$$

induced by the restrictions whose kernel $\mathrm{Ker}(s_r)$ is finite and bounded independent of n. (See Lemma 5.2.2 and Remark 6.1.3-(3).) For the cokernel, we have the following theorem of Hida [Hid17, Theorem 10.4] which we refer as "Hida's control theorem" in this thesis.

Theorem 1.2.1. *(1)* $\mathrm{Ker}(s_r)$ *is finite and of bounded order as n varies.*

(2) [Hida] If X_r does not have split multiplicative reduction at all places of K dividing p, then $\mathrm{Coker}(s_r)$ *is finite. In particular,* $\mathrm{Coker}(s_r)$ *is finite for all $r \geq 2$.*

Hence the behavior of (the *ordinary* parts of) the Selmer groups made out of towers of modular curves are *controlled* by the one Λ-adic object $\mathrm{Sel}_K(J_\infty)^{ord}_p$ and it is natural to study the *structure* of $\mathrm{Sel}_K(J_\infty)^{ord}_p$ as a Λ-module (under the control theorem). More precisely, in this thesis, we want to study the elementary modules of

$$(J_\infty(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{ord}, (\mathrm{Sel}_K(J_\infty)^{ord}_p)^\vee, Ш^1_K(J_\infty)^{ord}_p$$

which will be an "*modular*" analogue of the result stated after Question 1.1.3.

1.3 Functors $\mathfrak{F}$ and $\mathfrak{G}$

To describe the Λ-module structure of Mordell-Weil and Tate-Shafarevich groups by using the Selmer group, we need two functors $\mathfrak{F}$ and $\mathfrak{G}$, which are key ingredients in this thesis. For a finitely generated Λ-module X, we define

$$\mathfrak{F}(X) := \left(\varinjlim_n \frac{X}{\omega_n X}[p^\infty] \right)^\vee, \quad \mathfrak{G}(X) := \varprojlim_n \left(\frac{X}{\omega_n X}[p^\infty] \right).$$

We have the following description of the functor $\mathfrak{G}$. For the proof, see Proposition 7.2.5.

- $\mathfrak{G}(\Lambda) = 0$. This shows that the $\mathfrak{G}(X)$ is a torsion Λ-module.
- $\mathfrak{G}(\frac{\Lambda}{g^e}) \simeq \frac{\Lambda}{g^e}$ if g is coprime to ω_n for all n.
- $$\mathfrak{G}(\frac{\Lambda}{\omega_{m+1,m}^e}) = \begin{cases} \frac{\Lambda}{\omega_{m+1,m}^{e-1}} & e \geq 2, \\ 0 & e = 1. \end{cases}$$
- $\mathfrak{G}$ is a covariant functor and preserves the pseudo-isomorphism.

We also have the similar description (Proposition 7.1.6) for the functor $\mathfrak{F}$.

The explicit description and the basic properties of those two functors are given in the last chapter (Chapter 7) of this thesis. The nice point of the functor $\mathfrak{G}$ is that under the finiteness assumption of Tate-Shafarevich groups, the functor $\mathfrak{G}$ relates the Selmer group and the Tate-Shafarevich group at each finite layer. By taking limits, we get relations between the Selmer and Tate-Shafarevich groups (Theorem 2.2.4 and Theorem 6.2.1).

1.4 Organization

This thesis is largely divided into two parts, namely, Chapter 2 and Chapters 3-6, in terms of the origin of p-adic variation. Chapter 2 is about the Iwasawa theory of an abelian variety over the cyclotomic variation. On the other hand, starting from Chapter 3, we deal with the case of the modular variation (tower of modular curves).

In Chapter 3, we define basic objects such as modular curves, ordinary Hecke algebra, limits of Jacobians (and their p^∞-torsion points) and record some basic facts following [Hid17].

Chapter 4 is technically important for the later Chapters 5 and 6. We define various perfect pairings between ordinary parts of arithmetic cohomology groups. This will give rise to the "algebraic functional equation" type result in the Chapter 6.

Chapter 5 is about the module structure, for local and global case both, of cohomologies coming from the p^∞-torsion group of (ordinary parts of) limits of Jacobians. For the definition of $\mathfrak{g}$, see Notation 3.3.6.

In Chapter 6, we prove the main results for the cohomology groups made out of tower of modular curves, which are analogues of the results in Chapter 2.

Lastly, definitions, basic properties and explicit descriptions of the functors $\mathfrak{F}$ and $\mathfrak{G}$ are given in Chapter 7.

1.5 Notations

We fix the following notations below throughout the paper.

- Notation 3.3.6, Convention 3.3.8 will be used from Chapter 3. Notation 6.1.2 will also be used in Chapter 6.
- We fix one rational odd prime p throughout this thesis.
- Except for Chapter 2, $\Lambda := W[\![T]\!]$ for a fixed ring W which is the integer ring of $Q(W)$, a finite **unramified** extension of $\mathbb{Q}_p$. In Chapter 2, we let $\Lambda := \mathbb{Z}_p[\![T]\!]$, the one variable power series ring over $\mathbb{Z}_p$. We also define $\omega_n = \omega_n(T) := (1+T)^{p^n} - 1$ and $\omega_{n+1,n} := \frac{\omega_{n+1}(T)}{\omega_n(T)}$ with $\omega_{0,-1} := T$. Note that $\omega_{n+1,n}$ is a distinguished irreducible polynomial in Λ (for both cases).

- For a locally compact Hausdorff continuous Λ-module M, we define

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

which is also a locally compact Hausdorff. $M^\vee$ becomes a continuous Λ-module via the action defined by $(f \cdot \phi)(m) := \phi(\iota(f) \cdot m)$ where $f \in \Lambda$, $m \in M$, $\phi \in M^\vee$. We also define M^ι to be the same underlying set M whose Λ-action is twisted by an involution $\iota : T \to \frac{1}{1+T} - 1$ of Λ.

- For a cofinitely generated $\mathbb{Z}_p$-module X, we define $X_{/div} := \frac{X}{X_{div}}$ where X_{div} is the maximal p-divisible subgroup of X. Note that

$$X_{/div} \simeq \varprojlim_n \frac{X}{p^n X} \quad \text{and} \quad \left(X_{/div}\right)^\vee \simeq X^\vee[p^\infty].$$

- For a finitely generated Λ-module M, there are prime elements $g_1, \cdots g_n$ of Λ, a non-negative integer r, positive integers $e_1, \cdots e_n$ and a pseudo-isomorphism

$$M \to \Lambda^r \oplus \left(\bigoplus_{i=1}^{n} \frac{\Lambda}{g_i^{e_i}} \right).$$

We call $E(M) := \Lambda^r \oplus \left(\bigoplus_{i=1}^{n} \frac{\Lambda}{g_i^{e_i}} \right)$ the **elementary module of** M following [NSW00, Page 292].

- For a ring R and an R-module M, we define $M[f] := \{m \in M | f \cdot m = 0\}$ for $f \in R$. If R is a domain, we define M_{R-tor} as the maximal R-torsion submodule of M.

CHAPTER 2

Structure of cohomology groups over cyclotomic towers

Let A be an abelian variety over a number field K, let K_∞ be a $\mathbb{Z}_p$-extension of K, and let K_n be the n-th layer. We identify $\mathbb{Z}_p[\![\mathrm{Gal}(K_\infty/K)]\!]$ with Λ by fixing a generator γ of $\mathrm{Gal}(K_\infty/K)$ and identifying it with $1+T$. The main goal of this chapter is is to describe (as precisely as possible) the structure of

$$E\left((A(K_\infty)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p)^\vee\right), \quad E\left(\mathrm{Sel}_{K_\infty}(A)_p^\vee\right), \quad E\left(\text{Ш}^1_{K_\infty}(A)_p^\vee\right).$$

More precisely, we can ask the following questions:

Question 2.0.1 (Describing the elementary modules)**.**

- *Can we find some relations among those three modules?*

Question 2.0.2 ("Smallness" of the Ш^1)**.** *Under the finiteness assumption of the groups* $\text{Ш}^1_{K_n}(A)_p$,

- *Is the group* $\text{Ш}^1_{K_\infty}(A)_p$ Λ*-cotorsion?*

- *Can we find an estimate (even conjecturally) of* $|\text{Ш}^1_{K_n}(A)_p|$ *in terms of* n*?*

Question 2.0.3 (Algebraic Functional Equation)**.** *If* A^t *is the dual abelian variety of* A*, then can we find any relation between*

- $E\left(\mathrm{Sel}_{K_\infty}(A)_p^\vee\right)$ and $E\left(\mathrm{Sel}_{K_\infty}(A^t)_p^\vee\right)$?

- $E\left(\text{Ш}^1_{K_\infty}(A)_p^\vee\right)$ and $E\left(\text{Ш}^1_{K_\infty}(A^t)_p^\vee\right)$?

- $E\left((A(K_\infty)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p)^\vee\right)$ and $E\left((A^t(K_\infty)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p)^\vee\right)$?

We will try to answer these questions in this chapter.

2.1 Structure of limit Mordell-Weil groups

In this section, we study the structure of the Λ-adic Mordell-Weil group and prove our first main theorem (Theorem 2.1.2). We first start with a lemma.

Lemma 2.1.1. *Let F be a finite extension of $\mathbb{Q}$ or $\mathbb{Q}_l$ for some prime l and let A be an abelian variety defined over F. Take any $\mathbb{Z}_p$-extension F_∞ and consider the module $X := (A(F_\infty)[p^\infty])^\vee$.*

(1) X is a finitely generated torsion Λ-module with $\mu(X) = 0$, and $\mathrm{char}_\Lambda X$ is coprime to ω_n for all n.

(2) The modules $\frac{A(F_\infty)[p^\infty]}{p^n A(F_\infty)[p^\infty]}$ and $\frac{A(F_\infty)[p^\infty]}{\omega_n A(F_\infty)[p^\infty]}$ are finite and bounded independent of n.

(3) For the natural maps

$$MW_n^A : A(F_n) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p \to A(F_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p[\omega_n]$$

and

$$S_n^A : \mathrm{Sel}_{F_n}(A)_p \to \mathrm{Sel}_{F_\infty}(A)_p[\omega_n],$$

the groups $\mathrm{Ker}(MW_n^A)$ and $\mathrm{Ker}(S_n^A)$ are finite and bounded independent of n.

We first remark that (2) is a direct consequence of (1) by the structure theorem of the finitely generated Λ-modules. Hence we prove (1) and (3) only.

Proof. For (1), it suffices to show that $\frac{X}{pX}$ and $\frac{X}{\omega_n X}$ are finite. Since we have isomorphisms

$$\frac{X}{pX} \simeq (A(F_\infty)[p])^\vee, \quad \frac{X}{\omega_n X} \simeq (A(F_n)[p^\infty])^\vee$$

and the groups $A(F_\infty)[p], A(F_n)[p^\infty]$ are finite, we get (1).

For (3), by the definition of the Selmer group, we have injections

$$\mathrm{Ker}(MW_n^A) \hookrightarrow \mathrm{Ker}(S_n^A) \hookrightarrow \frac{A(F_\infty)[p^\infty]}{\omega_n A(F_\infty)[p^\infty]}.$$

Hence (3) follows from (2). □

We first recall a functor $\mathfrak{G}$ whose detailed explanation is given in the Chapter 7. For a finitely generated Λ-module X, we define

$$\mathfrak{G}(X) := \varprojlim_n \left(\frac{X}{\omega_n X}[p^\infty] \right).$$

We have the following description of the functor $\mathfrak{G}$. For the proof, see Proposition 7.2.5.

- $\mathfrak{G}(\Lambda) = 0$. This shows that $\mathfrak{G}(X)$ is a torsion Λ-module.
- $\mathfrak{G}(\frac{\Lambda}{g^e}) \simeq \frac{\Lambda}{g^e}$ if g is coprime to ω_n for all n.
- For $m \geq -1$,

$$\mathfrak{G}(\frac{\Lambda}{\omega_{m+1,m}^e}) = \begin{cases} \frac{\Lambda}{\omega_{m+1,m}^{e-1}} & e \geq 2, \\ 0 & e = 1. \end{cases}$$

- $\mathfrak{G}$ is a covariant functor and preserves pseudo-isomorphisms.

Theorem 2.1.2. *Let F be a finite extension of $\mathbb{Q}$ or $\mathbb{Q}_p$, and let F_∞ be any $\mathbb{Z}_p$-extension of F. We identify $\mathbb{Z}_p[\![\mathrm{Gal}(F_\infty/F)]\!]$ with Λ by fixing a generator γ of $\mathrm{Gal}(F_\infty/F)$ and identifying it with $1+T$. Then we have:*

(1) $\mathfrak{G}\left((A(F_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)^\vee\right) = 0.$

(2) There is a Λ-linear injection

$$(A(F_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)^\vee \hookrightarrow \Lambda^r \oplus \left(\bigoplus_{n=1}^{t} \frac{\Lambda}{\omega_{b_n, b_n - 1}} \right)$$

with finite cokernel for some non-negative integers $r, b_1, \cdots b_n$.

We call $A(F_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p$ the limit Mordell-Weil group.

Remark 2.1.3. (1) Hence the direct factors of $E\left((A(F_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)^\vee\right)_{\Lambda-tor}$ are only of the form $\frac{\Lambda}{\omega_{k+1,k}}$ for some k.

(2) If F is a number field, then for any integer e and any irreducible distinguished polynomial $h \in \Lambda$ coprime to ω_n for all n, the natural injection

$$Ш^1_{F_\infty}(A)_p^\vee[h^e] \hookrightarrow \mathrm{Sel}_{F_\infty}(A)_p^\vee[h^e]$$

has a finite cokernel.

(3) As it will be clear in the proof, Theorem 2.1.2 holds for any p-adic local field F also. This produces one consequence about the finiteness of the p^∞-torsion of an abelian variety $A_{/F}$ over a $\mathbb{Z}_p$-extension. (See Theorem 2.1.7)

Note that $(A(F_\infty)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p)^\vee$ has no non-trivial finite Λ-submodule since it is $\mathbb{Z}_p$-torsion-free. Due to Proposition 7.2.5, it is enough to show the assertion (1) only. As a preparation for the proof, we record the following lemma.

Lemma 2.1.4. *(1) Let R be an integral domain and $Q(R)$ be the quotient field of R. Consider an exact sequence of R-modules $0 \to A \to B \to C \to 0$ where A is a R-torsion module. Then we have a short exact sequence $0 \to A_{R-\mathrm{tor}} \to B_{R-\mathrm{tor}} \to C_{R-\mathrm{tor}} \to 0$.*

(2) Let $0 \to A \to B \to C \to 0$ be a short exact sequence of finitely generated $\mathbb{Z}_p$-modules. If A has finite cardinality, then we have a short exact sequence $0 \to A = A[p^\infty] \to B[p^\infty] \to C[p^\infty] \to 0$.

(3) If $0 \to X \to Y \to Z \to W \to 0$ is an exact sequence of cofinitely generated $\mathbb{Z}_p$-modules with finite W, then the sequence $X_{/div} \to Y_{/div} \to Z_{/div} \to W \to 0$ is exact.

Proof. We prove (1) and (3) only, since (2) is a direct consequence of (1). Note that for an R-module M, we have $\mathrm{Tor}_1^R(M, Q(R)/R) \simeq M_{R-\mathrm{tor}}$. Since A is a R-torsion module, we have $A \otimes_R Q(R)/R = 0$. Now (1) follows from the long exact sequence associated with functor $\mathrm{Tor}_1^R(-, Q(R)/R)$.

For (3), break up the sequence to $0 \to X \to Y \to T \to 0$ and $0 \to T \to Z \to W \to 0$. Applying the p^∞-torsion functor to the Pontryagin dual of the first short exact sequence gives $X_{/div} \to Y_{/div} \to T_{/div} \to 0$. By (2), we get $0 \to T_{/div} \to Z_{/div} \to W_{/div} \to 0$. Combining these two sequences proves the assertion. ∎

Proof of Theorem 2.1.2. Let C_n be the cokernel of the natural map

$$MW_n^A : A(F_n) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p \to A(F_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p[\omega_n].$$

Since $\varinjlim_n A(F_n) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p = A(F_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p$ by definition, we get $\varinjlim_n C_n = 0$ and $\varinjlim_n (C_n)_{/div} = 0$.

From the exact sequence

$$A(F_n) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p \to A(F_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p[\omega_n] \to C_n \to 0,$$

we have

$$0 = (A(F_n) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)_{/div} \to (A(F_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p[\omega_n])_{/div} \to (C_n)_{/div} \to 0$$

by Lemma 2.1.4-(3). Taking the direct limit of this sequence shows

$$\varinjlim_n (A(F_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p[\omega_n])_{/div} = 0$$

since $\varinjlim_n (C_n)_{/div} = 0$. If we take the Pontryagin dual, we get

$$\varprojlim_n \frac{(A(F_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)^\vee}{\omega_n (A(F_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)^\vee}[p^\infty] = 0.$$

Hence we get

$$\mathfrak{G}\left((A(F_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)^\vee\right) := \varprojlim_n \frac{(A(F_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)^\vee}{\omega_n (A(F_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)^\vee}[p^\infty] = 0.$$

□

Next we state the control result on the limit of Mordell-Weil groups under the Λ-cotorsion assumption. For the second statement about the λ-invariant, we need to use Theorem 2.1.2.

Theorem 2.1.5. *Let F be a number field, F_∞ be a $\mathbb{Z}_p$-extension of F and F_n be the n-th layer. The following two assertions are equivalent:*

- *The sequence $\{\mathrm{rank}_{\mathbb{Z}} A(F_n)\}_{n \geq 0}$ is bounded.*
- *$A(F_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p$ is a cotorsion Λ-module.*

If these equivalent conditions hold, the natural map

$$A(F_n)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p \to A(F_\infty)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p[\omega_n]$$

is surjective for almost all n and $\mathrm{rank}_{\mathbb{Z}}A(F_n)$ *stabilizes to* $\lambda\left((A(F_\infty)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p)^\vee\right)$.

Proof. By Lemma 2.1.1, the natural map $A(F_n)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p \to A(F_\infty)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p[\omega_n]$ has finite kernel for all n. If $A(F_\infty)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p$ is a cotorsion Λ-module, then by the Λ-module theory, the $\mathbb{Z}_p$-coranks of the modules $A(F_\infty)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p[\omega_n]$ are bounded, and hence $\mathrm{rank}_{\mathbb{Z}}A(F_n)$ is bounded.

Conversely, assume that $\mathrm{rank}_{\mathbb{Z}}A(F_n)$ is bounded and take n so that

$$\mathrm{rank}_{\mathbb{Z}}A(F_{n+k}) = \mathrm{rank}_{\mathbb{Z}}A(F_n)$$

for all $k\geq 0$. Now consider the following diagram:

$$\begin{array}{ccc}
A(F_n)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p & \xrightarrow{\quad r \quad} & A(F_{n+k})\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p \\
\downarrow{\scriptstyle s} & & \downarrow{\scriptstyle t} \\
A(F_\infty)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p[\omega_n] & \hookrightarrow & A(F_\infty)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p[\omega_{n+1}]
\end{array}$$

Since the map s has finite kernel, $\mathrm{Ker}(r)$ is also finite. Considering the $\mathbb{Z}_p$-corank shows that r is surjective. By taking the direct limit, we get a surjection

$$A(F_n)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p \twoheadrightarrow A(F_\infty)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p.$$

Since this map factors through the natural inclusion

$$A(F_\infty)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p[\omega_n] \hookrightarrow A(F_\infty)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p,$$

the above inclusion is an isomorphism indeed, and hence $A(F_\infty)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p$ is a cotorsion Λ-module. This also proves the assertion about the stabilized value of the sequence $\{\mathrm{rank}_{\mathbb{Z}}A(F_n)\}_{n\geq 0}$. □

Remark 2.1.6. (1) In above theorem, the condition that $A(F_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p$ is a cotorsion Λ-module is *not* enough to guarantee that

$$\mathrm{rank}_{\mathbb{Z}} A(F_n) = \lambda\left((A(F_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)^\vee\right) \quad (n >> 0).$$

Indeed, we need to use Theorem 2.1.2 that the direct factors of $E\left((F(K_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)^\vee\right)_{\Lambda-tor}$ are only of the form $\frac{\Lambda}{\omega_{k+1,k}}$ for some k.

(2) If F is a number field, consider a Λ-linear injection

$$(A(F_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)^\vee \hookrightarrow \Lambda^r \oplus \left(\bigoplus_{n=1}^{t} \frac{\Lambda}{\omega_{b_n+1,b_n}}\right)$$

in Theorem 2.1.2. Assume that $\mathrm{Coker}(S_n^A)$ and $\text{Ш}^1_{F_n}(A)_p$ are finite for all n. Then by the snake lemma, the natural map

$$A(F_n) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p \to A(F_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p[\omega_n]$$

has finite kernel and cokernel for all n. By comparing the $\mathbb{Z}_p$-coranks of the two modules, we get

$$r = \lim_{n \longrightarrow \infty} \frac{\mathrm{rank}_{\mathbb{Z}} A(F_n)}{p^n}, \quad a_n = \frac{\mathrm{rank}_{\mathbb{Z}} A(F_n) - \mathrm{rank}_{\mathbb{Z}} A(F_{n-1})}{p^{n-1}(p-1)} - r \quad (n \geq 1)$$

where a_n is defined as the number of $1 \leq i \leq t$ satisfying $b_i = n-1$. Hence for this case, we can describe $E\left((A(F_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)^\vee\right)$ by using the sequence $\{\mathrm{rank}_{\mathbb{Z}} A(F_n)\}_{n \geq 0}$.

We prove one interesting consequence of Theorem 2.1.2 about the finiteness of the p^∞-torsion group of an abelian variety over a p-adic local field. Let L be a finite extension of $\mathbb{Q}_p$, L_∞ be a $\mathbb{Z}_p$-extension of L, L_n be a n-th layer, and A be an abelian variety defined over L.

We consider $A(L_\infty)[p^\infty]$, which is a cofinitely generated cotorsion Λ-module by Lemma 2.1.1. If A has (potentially) good reduction over L, Imai [Ima75] proved that the torsion subgroup of the $A(L(\mu_{p^\infty}))$ is finite. By using Theorem 2.1.2, we prove that if A has potentially supersingular reduction, $A(L_\infty)[p^\infty]$ is finite for the general ramified $\mathbb{Z}_p$-extension L_∞/L.

Theorem 2.1.7. *If $A_{/L}$ has potentially supersingular reduction and L_∞/L is a ramified $\mathbb{Z}_p$-extension, then $A(L_\infty)[p^\infty]$ is finite.*

Proof. We may assume that A has supersingular reduction over L. Let $\mathcal{F}$ be a formal group of A. Since $A_{/L}$ has supersingular reduction, we have an isomorphism

$$H^1(L_\infty, \mathcal{F}) \simeq H^1(L_\infty, A)[p^\infty].$$

Since L_∞/L is a ramified $\mathbb{Z}_p$-extension, by [CG96, Proposition 2.10, Theorem 2.13] we have

$$H^1(L_\infty, \mathcal{F}) = 0.$$

Hence from the Kummer sequence, we have an isomorphism

$$H^1(L_\infty, A[p^\infty])^\vee \simeq (A(L_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)^\vee.$$

Since Λ-torsion part of $H^1(L_\infty, A[p^\infty])^\vee$ is pseudo-isomorphic to $(A^t(L_\infty)[p^\infty])^\vee$ by [Gre89, Proposition 3.1] (up to twisting by ι), combining Theorem 2.1.2 and Lemma 2.1.1 shows the desired assertion. □

Remark 2.1.8. In the proof of the above Theorem, we have also proved that

$$(A(L_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)^\vee$$

is a torsion-free Λ-module.

2.2 Selmer groups and Tate-Shafarevich groups

We study the Selmer group and the Tate-Shafarevich group in this section. We will describe the Λ-adic Tate-Shafarevich group by the Λ-adic Selmer group under mild assumptions. (See Theorem 2.2.4.)

Definition 2.2.1. Let F be a number field and A be an abelian variety over F. Let S be a finite set of places of F containing the places over p, infinite places and places of bad reduction of A. We define the Selmer group and the Tate-Shafarevich group as follows:

(1) $\mathrm{Sel}_F(A)_p := \mathrm{Ker}\left(H^1(F^S/F, A[p^\infty]) \to \prod_{v\in S} H^1(F_v, A)\right)$.

(2) $\text{Ш}^1_F(A)_p := \mathrm{Ker}\left(H^1(F^S/F, A)[p^\infty] \to \prod_{v\in S} H^1(F_v, A)[p^\infty]\right)$.

Remark 2.2.2. By [Mil06, Corollary I.6.6], this definition is independent of the choice of S as long as S contains infinite places, primes over p and primes of bad reduction of A. Moreover, all modules in the above definition are cofinitely generated $\mathbb{Z}_p$-modules.

Notation 2.2.3. *In this chapter, hereafter,*

(1) we let A be an abelian variety over a number field K and let S be a finite set of places of K containing the places over p, infinite places and places of bad reduction of A. We fix a $\mathbb{Z}_p$-extension K_∞ of K,

(2) we identify $\mathbb{Z}_p[\![\mathrm{Gal}(K_\infty/K)]\!]$ with Λ by fixing a generator γ of $\mathrm{Gal}(K_\infty/K)$ and identifying it with $1+T$,

(3) we let

$$S_n^A : \mathrm{Sel}_{K_n}(A)_p \to \mathrm{Sel}_{K_\infty}(A)_p[\omega_n]$$

be the natural restriction map.

Next we state the result that under the control of Selmer groups and the Tate-Shafarevich conjecture, $\text{Ш}^1_{K_\infty}(A)_p$ is a cotorsion Λ-module. This can be regarded as a Λ-adic analogue of the Tate-Shafarevich conjecture. (Recall that $\mathfrak{G}(X) = \varprojlim_n \left(\frac{X}{\omega_n X}[p^\infty]\right)$.)

Theorem 2.2.4. *If $\mathrm{Coker}(S_n^A)$ and $\text{Ш}^1_{K_n}(A)_p$ are finite for all n, then we have an isomorphism*

$$\text{Ш}^1_{K_\infty}(A)_p^\vee \simeq \mathfrak{G}\left(\mathrm{Sel}_{K_\infty}(A)_p^\vee\right)$$

of Λ-modules. In particular, $\text{Ш}^1_{K_\infty}(A)_p$ is a cotorsion Λ-module.

Proof. We start from the natural map $S_n^A : \mathrm{Sel}_{K_n}(A)_p \to \mathrm{Sel}_{K_\infty}(A)_p[\omega_n]$. Note that

$$\varinjlim_n \mathrm{Ker}(S_n^A) = \varinjlim_n \mathrm{Coker}(S_n^A) = 0$$

by definition. Hence we get

$$\varprojlim_n \mathrm{Ker}(S_n^A)^\vee[p^\infty] = \varprojlim_n \mathrm{Coker}(S_n^A)^\vee[p^\infty] = 0.$$

On the other hand, since $\mathrm{Coker}(S_n^A)$ is finite, by Lemma 2.1.4-(3) we get an exact sequence

$$0 \to \mathrm{Coker}(S_n^A)^\vee[p^\infty] \to \frac{\mathrm{Sel}_{K_\infty}(A)_p^\vee}{\omega_n \mathrm{Sel}_{K_\infty}(A)_p^\vee}[p^\infty] \to \mathrm{Sel}_{K_n}(A)_p^\vee[p^\infty] \to \mathrm{Ker}(S_n^A)^\vee[p^\infty]$$

where $\mathrm{Sel}_{K_n}(A)_p^\vee[p^\infty]$ is isomorphic to $Ш^1_{K_n}(A)_p^\vee$ since $Ш^1_{K_n}(A)_p$ is finite. Now taking the projective limit of the above sequence gives

$$\mathfrak{G}\left(\mathrm{Sel}_{K_\infty}(A)_p^\vee\right) := \varprojlim_n \frac{\mathrm{Sel}_{K_\infty}(A)_p^\vee}{\omega_n \mathrm{Sel}_{K_\infty}(A)_p^\vee}[p^\infty] \simeq Ш^1_{K_\infty}(A)_p^\vee.$$

□

Under the same conditions with the above theorem, we can *separate* the Mordell-Weil group and the Tate-Shafarevich group from the Selmer group. More precisely, we describe the elementary modules of the Mordell-Weil group and the Tate-Shafarevich group by using the elementary module of the Selmer group.

Corollary 2.2.5. *Suppose that* $\mathrm{Coker}(S_n^A)$ *and* $Ш^1_{K_n}(A)_p$ *are finite for all* n *and let*

$$E\left(\mathrm{Sel}_{K_\infty}(A)_p^\vee\right) \simeq \Lambda^r \oplus \left(\bigoplus_{i=1}^d \frac{\Lambda}{g_i^{l_i}}\right) \oplus \left(\bigoplus_{\substack{m=1 \\ e_1,\dots,e_f \geq 2}}^f \frac{\Lambda}{\omega_{a_m+1,a_m}^{e_m}}\right) \oplus \left(\bigoplus_{n=1}^t \frac{\Lambda}{\omega_{b_n+1,b_n}}\right)$$

where $r \geq 0$, $g_1, \dots, g_d$ *are prime elements of* Λ *which are coprime to* ω_n *for all* n, $d \geq 0$, $l_1, \dots, l_d \geq 1$, $f \geq 0$, $e_1, \dots, e_f \geq 2$ *and* $t \geq 0$. *Then we have isomorphisms*

$$E\left(Ш^1_{K_\infty}(A)_p^\vee\right) \simeq \left(\bigoplus_{i=1}^d \frac{\Lambda}{g_i^{l_i}}\right) \oplus \left(\bigoplus_{\substack{m=1 \\ e_1,\dots,e_f \geq 2}}^f \frac{\Lambda}{\omega_{a_m+1,a_m}^{e_m-1}}\right)$$

and

$$E\left((A(K_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)^\vee\right) \simeq \Lambda^r \oplus \left(\bigoplus_{\substack{m=1 \\ e_1,\dots,e_f \geq 2}}^f \frac{\Lambda}{\omega_{a_m+1,a_m}}\right) \oplus \left(\bigoplus_{n=1}^t \frac{\Lambda}{\omega_{b_n+1,b_n}}\right).$$

Proof. The isomorphism for $Ш^1_{K_\infty}(A)_p^\vee$ is a direct consequence of Theorem 2.2.4. For the second isomorphism, since $Ш^1_{K_\infty}(A)_p^\vee$ is a torsion Λ-module by Theorem 2.2.4, the exact sequence

$$0 \to Ш^1_{K_\infty}(A)_p^\vee \to \mathrm{Sel}_{K_\infty}(A)_p^\vee \to (A(K_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)^\vee \to 0$$

induces another exact sequence

$$0 \to \left(Ш^1_{K_\infty}(A)_p^\vee\right)_{\Lambda-\mathrm{tor}} \to \left(\mathrm{Sel}_{K_\infty}(A)_p^\vee\right)_{\Lambda-\mathrm{tor}} \to \left(A(K_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p\right)^\vee_{\Lambda-\mathrm{tor}} \to 0$$

by Lemma 2.1.4-(1). Now the first part of Theorem 2.2.4 shows the desired isomorphism. □

2.3 Estimates on the size of $Ш^1$

Now we find an estimate of $\left|Ш^1_{K_n}(A)_p\right|$, which is an analogue of the Iwasawa's class number formula [Gre99, Theorem 1.1].

Theorem 2.3.1. *Suppose that* $\mathrm{Coker}(S_n^A)$ *is finite and bounded independent of* n *and also suppose that* $Ш^1_{K_n}(A)_p$ *is finite for all* n*. Then there exists an integer* ν *independent of* n *such that*

$$\left|Ш^1_{K_n}(A)_p\right| = p^{e_n} \quad (n >> 0)$$

where

$$e_n = p^n\mu\left(Ш^1_{K_\infty}(A)_p^\vee\right) + n\lambda\left(Ш^1_{K_\infty}(A)_p^\vee\right) + \nu.$$

Remark 2.3.2. (1) This theorem can be an evidence for the control of the Tate-Shafarevich group over the tower of fields $\{K_n\}_{n\geq 0}$. More precisely, if the characteristic ideal of $Ш^1_{K_\infty}(A)_p^\vee$ is coprime to ω_n for all n (noting that by Theorem 2.2.4, $Ш^1_{K_\infty}(A)_p^\vee$ is a Λ-torsion under the assumption of Theorem 2.3.1), then by the Λ-module theory, we get

$$\left|Ш^1_{K_\infty}(A)_p[\omega_n]\right| = p^{e_n}$$

for the same e_n appearing in the above theorem. Hence we could expect the natural map

$$Ш^1_{K_n}(A)_p \to Ш^1_{K_\infty}(A)_p[\omega_n]$$

to have finite, bounded kernel and cokernel.

(2) This theorem improves [Gre99, Theorem 1.10] by removing the cotorsionness assumption of $\mathrm{Sel}_{K_\infty}(A)_p$. If Selmer group is a Λ-cotorsion, then our formula recovers that of [Gre99, Theorem 1.10]. We give a brief explanation here.

In [Gre99, Theorem 1.10], Greenberg's formula was

$$\left|Ш^1_{K_n}(A)_p\right| = p^{f_n} \quad (n >> 0)$$

for $f_n = p^n \mu_A + n \cdot (\lambda_A - \lambda_A^{MW}) + \nu$ where

- μ_A is a μ-invariant of the Selmer group $\mathrm{Sel}_{K_\infty}(A)_p^\vee$.
- λ_A is a λ-invariant of the Selmer group $\mathrm{Sel}_{K_\infty}(A)_p^\vee$.
- λ_A^{MW} is the stabilized value of $\{\mathrm{rank}_{\mathbb{Z}} A(K_n)\}_{n\geq 0}$.

Since $(A(K_\infty)\otimes \mathbb{Q}_p/\mathbb{Z}_p)^\vee$ is a Λ-torsion for this case, λ_A^{MW} is same as the λ-invariant of $(A(K_\infty)\otimes \mathbb{Q}_p/\mathbb{Z}_p)^\vee$ by Theorem 2.1.5. Hence by the multiplicative property of characteristic ideals, we get

$$\lambda_A - \lambda_A^{MW} = \lambda\left(Ш^1_{K_\infty}(A)_p^\vee\right).$$

For the μ-invariant, by Theorem 2.1.2, $(A(K_\infty)\otimes \mathbb{Q}_p/\mathbb{Z}_p)^\vee$ has μ-invariant zero. Hence we get

$$\mu_A = \mu\left(Ш^1_{K_\infty}(A)_p^\vee\right)$$

which justifies the claim.

Proof of Theorem 2.3.1. By a straightforward calculation, we can check that for a finitely generated Λ-module Y, we have

$$\log_p\left|\frac{Y}{\omega_n Y}[p^\infty]\right| = p^n\mu\left(\mathfrak{G}(Y)\right) + n\lambda\left(\mathfrak{G}(Y)\right) + \nu$$

for all $n >> 0$.

If we let $Y = \mathrm{Sel}_{K_\infty}(A)_p^\vee$, this gives an estimate for the group $\frac{\mathrm{Sel}_{K_\infty}(A)_p^\vee}{\omega_n \mathrm{Sel}_{K_\infty}(A)_p^\vee}[p^\infty]$. Since $\mathrm{Ker}(S_n^A)$ and $\mathrm{Coker}(S_n^A)$ are bounded independent of n, we get the desired assertion since we have isomorphisms

$$\mathrm{Sel}_{K_n}(A)_p^\vee[p^\infty] \simeq \text{Ш}^1_{K_n}(A)_p^\vee \quad \text{and} \quad \text{Ш}^1_{K_\infty}(A)_p^\vee \simeq \mathfrak{G}\left(\mathrm{Sel}_{K_\infty}(A)_p^\vee\right).$$

The second isomorphism holds due to Theorem 2.2.4. □

2.4 Algebraic functional equation

In this section, we want to compare two modules $E\left(\mathrm{Sel}_{K_\infty}(A)_p^\vee\right)$ and $E\left(\mathrm{Sel}_{K_\infty}(A^t)_p^\vee\right)^\iota$ under the control of the Selmer groups of A and A^t. Our strategy is the following:

- By using the Greenberg-Wiles formula [DDT95, Theorem 2.19], we compare the $\mathbb{Z}_p$-corank of Selmer groups of A and A^t at each finite layer K_n.
- Using two functors $\mathfrak{F}$ and $\mathfrak{G}$, we can lift the duality between Selmer groups of A and A^t (induced by Flach's pairing) to the Λ-adic setting.

2.4.1 The Greenberg-Wiles formula

We recall the Greenberg-Wiles formula in [DDT95, Theorem 2.19], which compares the cardinalities of two finite Selmer groups. We define $\mathrm{Sel}_{K_n,p^m}(A)$ as the kernel of the natural restriction map

$$H^1(K^S/K_n, A[p^m]) \to \prod_v H^1(K_n, A)$$

where v runs through the primes of K_n over the primes in S.

Proposition 2.4.1. *(1) (Greenberg-Wiles formula) For a fixed n, $\frac{|\mathrm{Sel}_{K_n,p^m}(A)|}{|\mathrm{Sel}_{K_n,p^m}(A^t)|}$ becomes stationary as $m \to \infty$.*

(2) We have $\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_{K_n}(A)_p = \mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_{K_n}(A^t)_p$ *for all n.*

Proof. For the proof of (1), see [DDT95, Theorem 2.19]. For (2), consider the following two natural exact sequences :

$$0 \to \frac{A(K_n)[p^\infty]}{p^m A(K_n)[p^\infty]} \to \mathrm{Sel}_{K_n,p^m}(A) \to \mathrm{Sel}_{K_n}(A)_p[p^m] \to 0$$
$$0 \to \frac{A^t(K_n)[p^\infty]}{p^m A^t(K_n)[p^\infty]} \to \mathrm{Sel}_{K_n,p^m}(A^t) \to \mathrm{Sel}_{K_n}(A^t)_p[p^m] \to 0$$

Since $A(K_n)[p^\infty]$ and $A^t(K_n)[p^\infty]$ are finite groups, the sizes of the groups

$$\frac{A(K_n)[p^\infty]}{p^m A(K_n)[p^\infty]}, \frac{A^t(K_n)[p^\infty]}{p^m A^t(K_n)[p^\infty]}$$

are of bounded order as m varies. If we consider the ratio between two groups $\mathrm{Sel}_{K_n,p^m}(A)$ and $\mathrm{Sel}_{K_n,p^m}(A^t)$, we get (2) from (1). □

2.4.2 Flach's pairing on Selmer groups

We briefly recall properties of the pairing of Flach.

For any finite extension $\mathfrak{k}$ of K contained in K^S, Flach [Fla90] constructed a $\mathrm{Gal}(\mathfrak{k}/K)$-equivariant bilinear pairing

$$F_{\mathfrak{k}} : \mathrm{Sel}_{\mathfrak{k}}(A)_p \times \mathrm{Sel}_{\mathfrak{k}}(A^t)_p \to \mathbb{Q}_p/\mathbb{Z}_p$$

whose left kernel (resp. right kernel) is the maximal p-divisible subgroup of $\mathrm{Sel}_{\mathfrak{k}}(A)_p$ (resp. $\mathrm{Sel}_{\mathfrak{k}}(A^t)_p$). Here $\mathrm{Gal}(\mathfrak{k}/K)$-equivariance means the property

$$F_{\mathfrak{k}}(g \cdot x, g \cdot y) = F_{\mathfrak{k}}(x, y)$$

for all $g \in \mathrm{Gal}(\mathfrak{k}/K)$ and $x \in \mathrm{Sel}_{\mathfrak{k}}(A)_p, y \in \mathrm{Sel}_{\mathfrak{k}}(A^t)_p$.

If we have two finite extensions $\mathfrak{k}_1 \geq \mathfrak{k}_2$ of K in K^S, we have the following functorial diagram:

$$\begin{array}{ccccc} \mathrm{Sel}_{\mathfrak{k}_2}(A)_p & \times & \mathrm{Sel}_{\mathfrak{k}_2}(A^t)_p & \xrightarrow{F_{\mathfrak{k}_2}} & \\ \uparrow{\scriptstyle \mathrm{Cor}} & & \downarrow{\scriptstyle \mathrm{Res}} & & \mathbb{Q}_p/\mathbb{Z}_p \\ \mathrm{Sel}_{\mathfrak{k}_1}(A)_p & \times & \mathrm{Sel}_{\mathfrak{k}_1}(A^t)_p & \xrightarrow{F_{\mathfrak{k}_1}} & \end{array}$$

By this functoriality, we get a perfect pairing

$$\varprojlim_n (\mathrm{Sel}_{K_n}(A)_p)_{/div} \times \varinjlim_n (\mathrm{Sel}_{K_n}(A^t)_p)_{/div} \to \mathbb{Q}_p/\mathbb{Z}_p$$

which is Λ-equivariant. Hence we have an isomorphism

$$\varprojlim_n (\mathrm{Sel}_{K_n}(A)_p)_{/div} \simeq \varprojlim_n \left(\mathrm{Sel}_{K_n}(A^t)_p^\vee[p^\infty]\right)$$

of Λ-modules.

2.4.3 Results on functional equation

We first mention two technical lemmas without proof. These can be proved by using the explicit description of the functors $\mathfrak{F}$ and $\mathfrak{G}$. (See Proposition 7.1.6 and Proposition 7.2.5.)

Lemma 2.4.2. *(1) Let M and N be finitely generated torsion Λ-modules. If there are Λ-linear maps $\phi : M \to N$ and $\psi : N \to M$ with finite kernels, then M and N are pseudo-isomorphic.*

(2) Let X and Y be finitely generated Λ-modules. Suppose that $\mathrm{rank}_{\mathbb{Z}_p} \frac{X}{\omega_n X} = \mathrm{rank}_{\mathbb{Z}_p} \frac{Y}{\omega_n Y}$ holds for all n, and that there are two Λ-linear maps $\mathfrak{G}(X) \to \mathfrak{F}(Y), \mathfrak{G}(Y) \to \mathfrak{F}(X)$ with finite kernels. Then $E(X)$ and $E(Y)^\iota$ are isomorphic as Λ-modules.

Greenberg [Gre99, Theorem 1.14] proved the equality of characteristic ideals between $\mathrm{Sel}_{K_\infty}(A)_p^\vee$ and $\left(\mathrm{Sel}_{K_\infty}(A^t)_p^\vee\right)^\iota$ under the additional assumption that $\mathrm{Sel}_{K_\infty}(A)_p^\vee$ is a cotorsion Λ-module. Their Λ-module structures will be proven to be identical up to twisting by ι by the following theorem. Note that we do not assume the cotorsionness of the Selmer group.

Theorem 2.4.3. *If $\mathrm{Coker}(S_n^A)$ and $\mathrm{Coker}(S_n^{A^t})$ are finite for all n, then we have an isomorphism*

$$E\left(\mathrm{Sel}_{K_\infty}(A)_p^\vee\right) \simeq E\left(\mathrm{Sel}_{K_\infty}(A^t)_p^\vee\right)^\iota$$

of Λ-modules. Here ι is an involution of Λ satisfying $\iota(T) = \frac{1}{1+T} - 1$.

Proof of Theorem 2.4.3. By Lemma 2.4.2, it suffices to show the following two assertions:

- $\mathrm{Sel}_{K_\infty}(A)_p[\omega_n]$ and $\mathrm{Sel}_{K_\infty}(A^t)_p[\omega_n]$ have same $\mathbb{Z}_p$-corank for all n.

- There is a Λ-linear map $\mathfrak{G}\left(\mathrm{Sel}_{K_\infty}(A^t)_p^\vee\right) \to \mathfrak{F}\left(\mathrm{Sel}_{K_\infty}(A)_p^\vee\right)$ with finite kernel.

The first assertion follows from our assumption on the finiteness of $\mathrm{Coker}(S_n^A)$, $\mathrm{Coker}(S_n^{A^t})$ and Proposition 2.4.1. Now we prove the second statement by using Flach's pairing.

By the same method as the proof of Theorem 2.2.4, we have an exact sequence

$$0 \to \mathrm{Coker}(S_n^{A^t})^\vee[p^\infty] \to \frac{\mathrm{Sel}_{K_\infty}(A^t)_p^\vee}{\omega_n \mathrm{Sel}_{K_\infty}(A^t)_p^\vee}[p^\infty] \to \mathrm{Sel}_{K_n}(A^t)_p^\vee[p^\infty] \to \mathrm{Ker}(S_n^{A^t})^\vee[p^\infty],$$

and isomorphisms

$$\varprojlim_n \mathrm{Ker}(S_n^{A^t})^\vee[p^\infty] = \varprojlim_n \mathrm{Coker}(S_n^{A^t})^\vee[p^\infty] = 0.$$

(Note that for the exact sequence, we used the finiteness of $\mathrm{Coker}(S_n^{A^t})$.) Now taking the projective limit of the above sequence gives an isomorphism

$$\mathfrak{G}\left(\mathrm{Sel}_{K_\infty}(A^t)_p^\vee\right) := \varprojlim_n \frac{\mathrm{Sel}_{K_\infty}(A^t)_p^\vee}{\omega_n \mathrm{Sel}_{K_\infty}(A)_p^\vee}[p^\infty] \simeq \varprojlim_n \mathrm{Sel}_{K_n}(A^t)_p^\vee[p^\infty]. \tag{2.1}$$

Now consider a natural exact sequence

$$0 \to \mathrm{Ker}(S_n^A) \to \mathrm{Sel}_{K_n}(A)_p \to \mathrm{Sel}_{K_\infty}(A)_p[\omega_n] \to \mathrm{Coker}(S_n^A) \to 0.$$

By Lemma 2.1.4-(3) and the finiteness of the $\mathrm{Coker}(S_n^A)$, we get another exact sequence

$$\mathrm{Ker}(S_n^A) \to (\mathrm{Sel}_{K_n}(A)_p)_{/div} \to (\mathrm{Sel}_{K_\infty}(A)_p[\omega_n])_{/div} \to \mathrm{Coker}(S_n^A) \to 0.$$

(Note that $\mathrm{Coker}(S_n^A)$ is finite.) By taking the projective limit, we get an exact sequence

$$\varprojlim_n \mathrm{Ker}(S_n^A) \to \varprojlim_n (\mathrm{Sel}_{K_n}(A)_p)_{/div} \to \varprojlim_n (\mathrm{Sel}_{K_\infty}(A)_p[\omega_n])_{/div}. \tag{2.2}$$

Here we use the fact that the projective limits of the compact modules are exact functors. We now analyze the three terms in this sequence (2.2).

- By the proof of Lemma 2.1.1, the first term $\varprojlim_n \mathrm{Ker}(S_n^A)$ injects into $\varprojlim_n \dfrac{A(K_\infty)[p^\infty]}{\omega_n A(K_\infty)[p^\infty]}$ which is a finite group. (This follows from the structure theorem of Λ-modules and Lemma 2.1.1-(1).)

- The middle term in (2.2) is isomorphic to $\varprojlim_n \left(\mathrm{Sel}_{K_n}(A^t)_p^\vee[p^\infty]\right)$ by the remark mentioned before this subsection (the functorial property of the Flach's pairing), which is also isomorphic to $\mathfrak{G}\left(\mathrm{Sel}_{K_\infty}(A^t)_p^\vee\right)$ by (2.1).

- Lastly, the third term in (2.2) is isomorphic to $\mathfrak{F}\left(\mathrm{Sel}_{K_\infty}(A)_p^\vee\right)$ by definition.

Hence the sequence (2.2) becomes a Λ-linear map $\mathfrak{G}\left(\mathrm{Sel}_{K_\infty}(A^t)_p^\vee\right) \to \mathfrak{F}\left(\mathrm{Sel}_{K_\infty}(A)_p^\vee\right)$ with the finite kernel. □

Proposition 2.4.4. *Suppose that* $\mathrm{Coker}(S_n^A)$, $\mathrm{Coker}(S_n^{A^t})$ *are finite for all* n. *If* $\text{Ш}^1_{K_n}(A)_p$ *is finite for all* n*, then we have isomorphisms*

$$E\left(\text{Ш}^1_{K_\infty}(A)_p^\vee\right) \simeq E\left(\text{Ш}^1_{K_\infty}(A^t)_p^\vee\right)^\iota$$

and

$$E\left((A(K_\infty)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p)^\vee\right) \simeq E\left((A^t(K_\infty)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p)^\vee\right)^\iota$$

of Λ*-modules.*

We remark here that the finiteness of $\text{Ш}^1_{K_n}(A)_p$ implies the finiteness of $\text{Ш}^1_{K_n}(A^t)_p$ by [Mil06, Lemma I.7.1].

Proof. This follows from Corollary 2.2.5 and Theorem 2.4.3. □

As a consequence of Theorem 2.4.3, we can compare the sizes of $\text{Ш}^1_{K_n}(A)_p$ and $\text{Ш}^1_{K_n}(A^t)_p$ over the tower of fields $\{K_n\}_{n\geq 0}$.

Theorem 2.4.5. *Suppose that* $\mathrm{Coker}(S_n^A)$, $\mathrm{Coker}(S_n^{A^t})$ *are finite and bounded independent of* n. *If* $\text{Ш}^1_{K_n}(A)_p$ *are finite for all* n*, then the ratios* $\frac{|\text{Ш}^1_{K_n}(A)_p|}{|\text{Ш}^1_{K_n}(A^t)_p|}$ *and* $\frac{|\text{Ш}^1_{K_n}(A^t)_p|}{|\text{Ш}^1_{K_n}(A)_p|}$ *become stationary as* n *goes to infinity.*

Proof. By Proposition 2.4.4, we have

$$\mu\left(\text{Ш}^1_{K_\infty}(A)_p^\vee\right) = \mu\left(\text{Ш}^1_{K_\infty}(A^t)_p^\vee\right)$$
$$\lambda\left(\text{Ш}^1_{K_\infty}(A)_p^\vee\right) = \lambda\left(\text{Ш}^1_{K_\infty}(A^t)_p^\vee\right).$$

Now applying the estimate of Theorem 2.3.1 to both groups $Ш^1_{K_n}(A)_p$ and $Ш^1_{K_n}(A^t)_p$ gives the desired assertion. □

CHAPTER 3

Tower of modular curves and Hecke algebra

3.1 Various modular curves

We define and analyze some properties of our main geometric objects in this section.

3.1.1 Congruence Subgroups

For $(\alpha, \delta) \in \mathbb{Z}_p \times \mathbb{Z}_p$ satisfying $\alpha\mathbb{Z}_p + \delta\mathbb{Z}_p = \mathbb{Z}_p$, define a map

$$\pi_{\alpha,\delta} : \Gamma \times \Gamma \to \Gamma$$

by

$$\pi_{\alpha,\delta}(x, y) = x^{\alpha} y^{-\delta}$$

where $\Gamma = 1 + p\mathbb{Z}_p$, and let $\Lambda_{\alpha,\delta} := W[\![(\Gamma \times \Gamma)/\mathrm{Ker}(\pi_{\alpha,\delta})]\!]$ be the completed group ring.

Let μ be the maximal torsion subgroup of $\mathbb{Z}_p^\times$. Pick a character $\xi : \mu \times \mu \to \mu$ and define another character $\xi' : \mu \times \mu \to \mu$ by $\xi'(a, b) := \xi(b, a)$. Consider $\mathrm{Ker}(\xi) \times \mathrm{Ker}(\pi_{\alpha,\delta})$ as a subgroup of $\mathbb{Z}_p^\times \times \mathbb{Z}_p^\times$ and let $H_{\alpha,\delta,\xi,r}$ be the image of $\mathrm{Ker}(\xi) \times \mathrm{Ker}(\pi_{\alpha,\delta})$ in $(\mathbb{Z}_p^\times)^2/(\Gamma^{p^{r-1}})^2$.

Definition 3.1.1. Let $\widehat{\mathbb{Z}} = \prod_{l:\text{prime}} \mathbb{Z}_l$ and N be a positive integer prime to p. For a positive integer r, we define the following congruence subgroups:

(1) $\widehat{\Gamma}_0(Np^r) := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\widehat{\mathbb{Z}}) \mid c \in Np^r\widehat{\mathbb{Z}} \right\}$. Let $\Gamma_0(Np^r) = \widehat{\Gamma}_0(Np^r) \cap \mathrm{SL}_2(\mathbb{Q})$.

(2) $\widehat{\Gamma}_{\alpha,\delta,\xi}(Np^r) := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \widehat{\Gamma}_0(Np^r) \mid (a_p, d_p) \in H_{\alpha,\delta,\xi,r}, d - 1 \in N\widehat{\mathbb{Z}} \right\}$.

Also let

$$\Gamma_{\alpha,\delta,\xi}(Np^r) = \widehat{\Gamma}_{\alpha,\delta,\xi}(Np^r) \cap \mathrm{SL}_2(\mathbb{Q}).$$

(3) $\widehat{\Gamma}_1^1(Np^r) := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \widehat{\Gamma}_0(Np^r) \mid c, d-1 \in Np^r\widehat{\mathbb{Z}}, a-1 \in p^r\widehat{\mathbb{Z}} \right\}$.

Remark 3.1.2. We have an isomorphism

$$(\mathbb{Z}/N\mathbb{Z})^\times \times \mathbb{Z}_p^\times \times \mathbb{Z}_p^\times \simeq \varprojlim_r \left(\widehat{\Gamma}_0(Np^r)/\widehat{\Gamma}_1^1(Np^r)\right)$$

sending (u, a, d) to the matrix whose p-component is $\left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right)$, and whose l-component is $\left(\begin{smallmatrix} 1 & 0 \\ 0 & u \end{smallmatrix}\right)$ for $l \mid N$ and trivial for $l \nmid Np$. This isomorphism induces two isomorphisms

$$\mathrm{Ker}(\xi) \times H_{\alpha,\delta,\xi,r} \simeq \widehat{\Gamma}_{\alpha,\delta,\xi}(Np^r)/\widehat{\Gamma}_1^1(Np^r),$$
$$(\mathbb{Z}/N\mathbb{Z})^\times \times \mathrm{Im}(\xi) \times \Gamma/\Gamma^{p^{r-1}} \simeq \widehat{\Gamma}_0(Np^r)/\widehat{\Gamma}_{\alpha,\delta,\xi}(Np^r).$$

3.1.2 Modular Curves

Following [Hid17, Section 3], we study various modular curves arising from congruence subgroups we defined in the previous subsection. Consider the moduli problem over $\mathbb{Q}$ classifying the triples

$$(E, \mu_N \xhookrightarrow{\phi_N} E, \mu_{p^r} \xhookrightarrow{\phi_{p^r}} E[p^r] \xrightarrow{\varphi_{p^r}} \mathbb{Z}/p^r\mathbb{Z})$$

where E is an elliptic curve defined over a $\mathbb{Q}$-algebra R and the sequence

$$\mu_{p^r} \xhookrightarrow{\phi_{p^r}} E[p^r] \xrightarrow{\varphi_{p^r}} \mathbb{Z}/p^r\mathbb{Z}$$

is exact in the category of finite flat group schemes. The triples are classified by a modular curve $U_{r/\mathbb{Q}}$, and we let $X_1^1(Np^r)_{/\mathbb{Q}}$ be the compactification of U_r smooth at cusps.

Note that $(\mathbb{Z}/N\mathbb{Z})^\times \times \mathbb{Z}_p^\times \times \mathbb{Z}_p^\times$ naturally acts on $X_1^1(Np^r)_{/\mathbb{Q}}$: $(u, a, d) \in (\mathbb{Z}/N\mathbb{Z})^\times \times \mathbb{Z}_p^\times \times \mathbb{Z}_p^\times$ sends

$$(E, \mu_N \xhookrightarrow{\phi_N} E, \mu_{p^r} \xhookrightarrow{\phi_{p^r}} E[p^r] \xrightarrow{\varphi_{p^r}} \mathbb{Z}/p^r\mathbb{Z})$$

to

$$(E, \mu_N \xhookrightarrow{\phi_N \circ u} E, \mu_{p^r} \xhookrightarrow{\phi_{p^r} \circ a} E[p^r] \xrightarrow{d \circ \varphi_{p^r}} \mathbb{Z}/p^r\mathbb{Z}).$$

We now define our main geometric objects.

Definition 3.1.3. We define the following two curves:

$$X_{\alpha,\delta,\xi}(Np^r)_{/\mathbb{Q}} := X_1^1(Np^r)_{/\mathbb{Q}}/\left(\mathrm{Ker}(\xi)\times \mathrm{Ker}(\pi_{\alpha,\delta})\right)$$
$$X_0(Np^r)_{/\mathbb{Q}} := X_1^1(Np^r)_{/\mathbb{Q}}/\left((\mathbb{Z}/N\mathbb{Z})^\times \times \mathbb{Z}_p^\times \times \mathbb{Z}_p^\times\right).$$

Remark 3.1.4. (1) Since $p \geq 5$, the above curves are smooth projective curves over $\mathbb{Q}$. Therefore, the natural projection maps

$$\pi_{1/\mathbb{Q}} : X_1^1(Np^r)_{/\mathbb{Q}} \to X_{\alpha,\delta,\xi}(Np^r)_{/\mathbb{Q}} \quad \text{and} \quad \pi_{2/\mathbb{Q}} : X_{\alpha,\delta,\xi}(Np^r)_{/\mathbb{Q}} \to X_0(Np^r)_{/\mathbb{Q}}$$

are finite flat.

(2) We have the following isomorphisms of geometric Galois groups:

$$\mathrm{Gal}(X_1^1(Np^r)/X_{\alpha,\delta,\xi}(Np^r)) \simeq \mathrm{Ker}(\xi)\times H_{\alpha,\delta,\xi,r} \simeq \hat{\Gamma}_{\alpha,\delta,\xi}(Np^r)/\hat{\Gamma}_1^1(Np^r)$$

$$\mathrm{Gal}(X_{\alpha,\delta,\xi}(Np^r)/X_0(Np^r)) \simeq (\mathbb{Z}/N\mathbb{Z})^\times \times \mathrm{Im}(\xi)\times \Gamma/\Gamma^{p^{r-1}} \simeq \hat{\Gamma}_0(Np^r)/\hat{\Gamma}_{\alpha,\delta,\xi}(Np^r).$$

(3) The complex points of these curves are given by

$$X_1^1(Np^r)(\mathbb{C}) - \{\text{cusps}\} \simeq \mathrm{GL}_2(\mathbb{Q})\backslash \mathrm{GL}_2(\mathbb{A})/\hat{\Gamma}_1^1(Np^r)\mathbb{R}^+\mathrm{SO}_2(\mathbb{R})$$
$$X_{\alpha,\delta,\xi}(Np^r)(\mathbb{C}) - \{\text{cusps}\} \simeq \mathrm{GL}_2(\mathbb{Q})\backslash \mathrm{GL}_2(\mathbb{A})/\hat{\Gamma}_{\alpha,\delta,\xi}(Np^r)\mathbb{R}^+\mathrm{SO}_2(\mathbb{R})$$
$$X_0(Np^r)(\mathbb{C}) - \{\text{cusps}\} \simeq \mathrm{GL}_2(\mathbb{Q})\backslash \mathrm{GL}_2(\mathbb{A})/\hat{\Gamma}_0(Np^r)\mathbb{R}^+\mathrm{SO}_2(\mathbb{R}).$$

Hence $X_1^1(Np^r), X_{\alpha,\delta,\xi}(Np^r), X_0(Np^r)$ are reduced over $\mathbb{Q}$. Moreover, the projection maps

$$\pi_1 : X_1^1(Np^r) \to X_{\alpha,\delta,\xi}(Np^r) \quad \text{and} \quad \pi_2 : X_{\alpha,\delta,\xi}(Np^r) \to X_0(Np^r)$$

have constant degree, since the degree is invariant under the flat base change.

3.2 Big Ordinary Hecke algebra

Following [Hid17, Section 4], we define Hecke algebras associated to the modular curves $X_{\alpha,\delta,\xi}(Np^r)$ in this subsection. For each rational prime l, consider $\varpi_l = \left(\begin{smallmatrix} 1 & 0 \\ 0 & l \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{A})$ whose component at prime $q \neq l$ is identity matrix. The group

$$\Theta_r = \varpi_l^{-1}\widehat{\Gamma}_{\alpha,\delta,\xi}(Np^r)\varpi_l \cap \widehat{\Gamma}_{\alpha,\delta,\xi}(Np^r)$$

gives rise to the modular curve $X(\Theta_r)$ whose complex points are given by

$$X(\Theta_r)(\mathbb{C}) - \{\text{cusps}\} \simeq \mathrm{GL}_2(\mathbb{Q})\backslash\mathrm{GL}_2(\mathbb{A})/\Theta_r\mathbb{R}^+\mathrm{SO}_2(\mathbb{R}).$$

We have two projection maps

$$\pi_{l,1} : X(\Theta_r) \to X_{\alpha,\delta,\xi}(Np^r) \quad \text{and} \quad \pi_{l,2} : X(\Theta_r) \to X_{\alpha,\delta,\xi}(Np^r)$$

defined by $\pi_{l,1}(z) = z$ and $\pi_{l,2}(z) = z/l$ for $z \in \mathbb{H}$. Now an embedding

$$X(\Theta_r) \xrightarrow{\pi_{l,1}\times\pi_{l,2}} X_{\alpha,\delta,\xi}(Np^r) \times X_{\alpha,\delta,\xi}(Np^r)$$

defines a modular correspondence. We write this correspondence as $T(l)$ if $l \nmid Np$ and $U(l)$ if $l \mid Np$. Hence we get endomorphisms

$$T(l) \quad (l \nmid Np) \quad \text{and} \quad U(l) \quad (l \mid Np)$$

of the Jacobian of $X_{\alpha,\delta,\xi}(Np^r)$ which we denote as $J_{\alpha,\delta,\xi,r}$. (See [Hid17, Section 4] for the details.) This $J_{\alpha,\delta,\xi,r}$ admits a geometric Galois action of $(\mathbb{Z}/N\mathbb{Z})^\times \times (\Gamma \times \Gamma)/\mathrm{Ker}(\pi_{\alpha,\delta})$ acts on $J_{\alpha,\delta,\xi,r}$ via Picard functoriality.

Definition 3.2.1. We define $h_{\alpha,\delta,\xi,r}(\mathbb{Z})$ by the subalgebra of $\mathrm{End}(J_{\alpha,\delta,\xi,r})$ generated by $T(l)$ for $l \nmid Np$, $U(l)$ for $l \mid Np$, and the action of $(\mathbb{Z}/N\mathbb{Z})^\times \times (\Gamma \times \Gamma)/\mathrm{Ker}(\pi_{\alpha,\delta})$. We let $h_{\alpha,\delta,\xi,r}(R) := h_{\alpha,\delta,\xi,r}(\mathbb{Z}) \otimes_{\mathbb{Z}} R$ for a commutative ring R and define $\mathbf{h}_{\alpha,\delta,\xi,r} := e(h_{\alpha,\delta,\xi,r}(W))$ where $e := \lim_{n\to\infty} U(p)^{n!}$ is the ordinary projector.

Remark 3.2.2. (1) Since $h_{\alpha,\delta,\xi,r}(W)$ is a finitely generated W-module, the ordinary projector e and $\mathbf{h}_{\alpha,\delta,\xi,r}$ are well-defined.

(2) For all r, $\mathbf{h}_{\alpha,\delta,\xi,r}$ is a $\Lambda_{\alpha,\delta}$-algebra. For $r \leq s$, we have a natural $\Lambda_{\alpha,\delta}$-equivariant surjection

$$\mathbf{h}_{\alpha,\delta,\xi,s} \twoheadrightarrow \mathbf{h}_{\alpha,\delta,\xi,r}.$$

Definition 3.2.3. Define the one variable big ordinary Hecke algebra $\mathbf{h}_{\alpha,\delta,\xi}(N) := \varprojlim_r \mathbf{h}_{\alpha,\delta,\xi,r}$ where the inverse limit is taken with respect to the natural surjections $\mathbf{h}_{\alpha,\delta,\xi,s} \twoheadrightarrow \mathbf{h}_{\alpha,\delta,\xi,r}$ for $r \leq s$. By Remark 3.2.2, $\mathbf{h}_{\alpha,\delta,\xi}(N)$ is a $\Lambda_{\alpha,\delta}$-algebra.

We quote some facts about structure of the big ordinary Hecke algebra. For the proofs of the following theorems, see [Hid12, Corollary 4.31].

Theorem 3.2.4. *(1) Fix a generator* γ *of* $(\Gamma \times \Gamma)/\mathrm{Ker}(\pi_{\alpha,\delta})$*. Then we have an isomorphism*

$$\frac{\boldsymbol{h}_{\alpha,\delta,\xi}(N)}{(\gamma^{p^{r-1}} - 1)\boldsymbol{h}_{\alpha,\delta,\xi}(N)} \simeq \boldsymbol{h}_{\alpha,\delta,\xi,r}.$$

(2) $\boldsymbol{h}_{\alpha,\delta,\xi}(N)$ *is a* $\Lambda_{\alpha,\delta}$*-free module of finite rank.*

3.3 Limit Mordell-Weil groups and limit Barsotti-Tate groups

3.3.1 Sheaves attached to abelian varieties

Definition 3.3.1. Let K be a finite extension of $\mathbb{Q}$ or $\mathbb{Q}_l$ and A be an abelian variety over K.

(1) For a finite extension F/K, define a finitely generated W-module

$$\widehat{A}(F) := \left(\varprojlim_n \frac{A(F)}{p^n A(F)} \right) \otimes_{\mathbb{Z}_p} W$$

.

(2) For an algebraic extension E/K, define $\widehat{A}(E) := \varinjlim_F \widehat{A}(F)$ where direct limit is taken over finite extensions F of K in E with respect to the natural inclusions.

Note that if F is a finite extension of $\mathbb{Q}_l$ with $l \neq p$, then $\widehat{A}(F) = A(F)[p^\infty]$ is a finite module.

We record (without proof) one lemma [Hid17, Lemma 7.2] regarding the Galois cohomology of $\widehat{A}$.

Lemma 3.3.2. *Let* K *be a finite extension of* $\mathbb{Q}$ *or* $\mathbb{Q}_l$*,* A *be an abelian variety defined over* K*, and* q *be a positive integer.*

(1) If K *is a number field, let* S *be finite set of places containing infinite places, primes over* p *and primes of bad reduction of* A*. Then* $H^q(K^S/K, \widehat{A}) \simeq H^q(K^S/K, A)[p^\infty]$*.*

(2) If K *is a local field, then* $H^q(K, \widehat{A}) \simeq H^q(K, A)[p^\infty]$*.*

Now we define the Selmer group and the Tate-Shafarevich group for $\widehat{A}$.

Definition 3.3.3. Let K be a number field, A be an abelian variety defined over K, and S be a finite set of places of K containing infinite places, primes over p and primes of bad reduction of A.

(1) $\mathrm{Sel}_K(\widehat{A}) := \mathrm{Ker}\left(H^1(K^S/K, \widehat{A}[p^\infty]) \to \prod_{v\in S} H^1(K_v, \widehat{A})\right)$

(2) $Ш^1_K(\widehat{A}) := \mathrm{Ker}\left(H^1(K^S/K, \widehat{A}) \to \prod_{v\in S} H^1(K_v, \widehat{A})\right)$

(3) $Ш^i_K(\widehat{A}[p^\infty]) := \mathrm{Ker}\left(H^i(K^S/K, \widehat{A}[p^\infty]) \to \prod_{v\in S} H^i(K_v, \widehat{A}[p^\infty])\right)$ for $i = 1, 2$

Remark 3.3.4. (1) By [Mil06, Corollary I.6.6], this definition is independent of the choice of S as long as S contains infinite places, primes over p and primes of bad reduction of A. Moreover, all three modules in the above definition are cofinitely generated W-modules.

(2) If we consider the usual classical p-adic Selmer group

$$\mathrm{Sel}_K(A) := \mathrm{Ker}(H^1(K^S/K, A[p^\infty]) \to \prod_{v\in S} H^1(K_v, A)),$$

then $\mathrm{Sel}_K(\widehat{A})$ is isomorphic to $\mathrm{Sel}_K(A)_p$ by Lemma 3.3.2. The same assertion holds for the Tate-Shafarevich groups.

(3) Since $A[p^\infty] \simeq \widehat{A}[p^\infty]$, we get $Ш^1_K(\widehat{A}[p^\infty]) = Ш^1_K(A[p^\infty])$ and $Ш^2_K(\widehat{A}[p^\infty]) = Ш^2_K(A[p^\infty])$.

3.3.2 Control sequences

Note that the $U(p)$-operator acts on sheaf $\hat{J}_{\alpha,\delta,\xi,r/\mathbb{Q}}$, where $J_{\alpha,\delta,\xi,r/\mathbb{Q}}$ is the Jacobian of the modular curve $X_{\alpha,\delta,\xi}(Np^r)_{/\mathbb{Q}}$. By considering the idempotent $e := \lim_{n\to\infty} U(p)^{n!}$, we define

$$\hat{J}^{ord}_{\alpha,\delta,\xi,r/\mathbb{Q}} := e(\hat{J}_{\alpha,\delta,\xi,r/\mathbb{Q}}).$$

Definition 3.3.5. We define the following Λ-adic Mordell-Weil group and Λ-adic Barsotti-Tate group as injective limits of sheaves:

(1) $J^{ord}_{\alpha,\delta,\xi,\infty/\mathbb{Q}} := \varinjlim_n \hat{J}^{ord}_{\alpha,\delta,\xi,n/\mathbb{Q}}$ (2) $G_{\alpha,\delta,\xi/\mathbb{Q}} := \varinjlim_n \hat{J}^{ord}_{\alpha,\delta,\xi,n}[p^\infty]_{/\mathbb{Q}}$

Notation 3.3.6. *Hereafter, we fix the following notations about the Jacobians and the Barsotti-Tate groups. For* $\alpha, \delta \in \mathbb{Z}_p$ *with* $\alpha\mathbb{Z}_p + \delta\mathbb{Z}_p = \mathbb{Z}_p$ *and a character* $\xi : \mu_{p-1} \times \mu_{p-1} \to \mu_{p-1}$*, we let*

- $J_n = J_{\alpha,\delta,\xi,n}$ *and* $J'_n = J_{\delta,\alpha,\xi',n}$.
- $\hat{J}_n^{ord} = \hat{J}_{\alpha,\delta,\xi,n}^{ord}$ *and* $\hat{J'}_n^{ord} = \hat{J}_{\delta,\alpha,\xi',n}^{ord}$.
- $J_\infty^{ord} = J_{\alpha,\delta,\xi,\infty}^{ord}$ *and* $J'^{ord}_\infty = J_{\delta,\alpha,\xi',\infty}^{ord}$
- $\mathfrak{g} = G_{\alpha,\delta,\xi}$ *and* $\mathfrak{g}' = G_{\delta,\alpha,\xi'}$.

Remark 3.3.7. (1) Note that the natural map

$$J_{n/\mathbb{Q}} \to J_{n+1/\mathbb{Q}}$$

induced from projection map $X_{\alpha,\delta,\xi}(Np^{n+1})_{/\mathbb{Q}} \twoheadrightarrow X_{\alpha,\delta,\xi}(Np^n)_{/\mathbb{Q}}$ via Picard functoriality is Hecke-equivariant. Hence we have an induced map

$$P_{n,n+1} : \hat{J}^{ord}_{n/\mathbb{Q}} \to \hat{J}^{ord}_{n+1/\mathbb{Q}}.$$

In Definition 3.3.5, direct limit is taken with respect to this $P_{n,n+1}$.

(2) If K is an algebraic extension of $\mathbb{Q}$ or $\mathbb{Q}_l$, we give discrete topology on

$$\mathfrak{g}(K) \quad \text{and} \quad \hat{J}_r^{ord}(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p$$

including $r = \infty$ which makes these two modules continuous Λ-modules. They are also $\mathbf{h}_{\alpha,\delta,\xi}(N)$-modules since the maps $P_{n,n+1}$ are Hecke-equivariant.

We use the following convention hereafter.

Convention 3.3.8 (Identification)**.** *We can find two elements* $\gamma_1 = (a, d)$ *and* $\gamma_2 = (d, a)$ *of* $\Gamma \times \Gamma$ *so that they generate* $\Gamma \times \Gamma$*,* $\gamma_1 = (a, d)$ *generates* $(\Gamma \times \Gamma)/\mathrm{Ker}(\pi_{\alpha,\delta})$*, and* $\gamma_2 = (d, a)$ *generates* $(\Gamma \times \Gamma)/\mathrm{Ker}(\pi_{\delta,\alpha})$*. We identify* $\Lambda_{\alpha,\delta}$ *with* $\Lambda = W[\![T]\!]$ *by* $(a, d) \leftrightarrow 1 + T$ *and* $\Lambda_{\delta,\alpha}$ *with* Λ *by* $(d, a) \leftrightarrow 1 + T$*.*

We first state the control results of sheaves $\hat{J}^{ord}_{r/\mathbb{Q}}$ and $\hat{J}^{ord}_r[p^\infty]_{/\mathbb{Q}}$ with respect to the p-power level. For the proof, see [Hid17, Section 3].

Proposition 3.3.9. *For two positive integers $r \leq s$, we have the following isomorphisms of sheaves:*

$$\hat{J}^{ord}_{r/\mathbb{Q}} \simeq \hat{J}^{ord}_s[\gamma^{p^{r-1}} - 1]_{/\mathbb{Q}} \quad \text{and} \quad \hat{J}^{ord}_{r/\mathbb{Q}} \simeq J^{ord}_\infty[\omega_r]_{/\mathbb{Q}}$$
$$\hat{J}^{ord}_r[p^\infty]_{/\mathbb{Q}} \simeq \hat{J}^{ord}_s[p^\infty][\gamma^{p^{r-1}} - 1]_{/\mathbb{Q}} \quad \text{and} \quad \hat{J}^{ord}_r[p^\infty]_{/\mathbb{Q}} \simeq \mathfrak{g}[\omega_r]_{/\mathbb{Q}}$$

Corollary 3.3.10. *For K either a number field or a finite extension of $\mathbb{Q}_l$, $\mathfrak{g}(K)$ is a discrete cofinitely generated cotorsion Λ-module.*

In the Section 6 and 7, we will study the structure of $\mathfrak{g}(K)^\vee$ as a finitely generated Λ-module in detail. From an exact sequence of sheaves

$$0 \to J^{ord}_\infty[\omega_r] \to J^{ord}_\infty \xrightarrow{\omega_r} J^{ord}_\infty,$$

we get an isomorphism $J^{ord}_\infty[\omega_r](K) \simeq J^{ord}_\infty(K)[\omega_r]$ where K is either a number field or a finite extension of $\mathbb{Q}_l$, since the global section functor is left exact. Similarly we get

$$\mathfrak{g}[\omega_r](K) \simeq \mathfrak{g}(K)[\omega_r].$$

Proof. By Proposition 3.3.9 and the above remark, we have an isomorphism

$$\hat{J}^{ord}_r[p^\infty](K) \simeq \mathfrak{g}(K)[\omega_r].$$

Since $\hat{J}^{ord}_r[p^\infty](K)$ has finite cardinality due to Mordell-Weil theorem (global case) and Nagell-Lutz theorem (local case), so Nakayama's lemma proves the assertion. □

3.3.3 Cofreeness of Barsotti-Tate groups

We state the cofreeness result of Barsotti-Tate groups without proof. (For the proof, see [Hid86, Section 6].)

Theorem 3.3.11. *(1) $\mathfrak{g}(\overline{\mathbb{Q}})$ is a cofree Λ-module of finite rank.*

(2) For a complex conjugation c, we have $\mathrm{corank}_\Lambda(\mathfrak{g}(\overline{\mathbb{Q}})[c-1]) = \mathrm{corank}_\Lambda(\mathfrak{g}(\overline{\mathbb{Q}})[c+1])$. Hence $\mathrm{corank}_\Lambda(\mathfrak{g}(\overline{\mathbb{Q}}))$ is even.

Proposition 3.3.12. *For a prime number l, fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_l}$. Then we have an isomorphism $\mathfrak{g}(\overline{\mathbb{Q}}) \simeq \mathfrak{g}(\overline{\mathbb{Q}_l})$ of Λ-modules. Hence $\mathfrak{g}(\overline{\mathbb{Q}_l})$ is a cofree Λ-module.*

As a corollary of Theorem 3.3.11, we have following short exact sequences of Barsotti-Tate groups, which will be used frequently in later chapters.

Corollary 3.3.13. *We have the following exact sequence of sheaves:*

$$0 \to \hat{J}_n^{ord}[p^\infty]_{/\mathbb{Q}} \to \mathfrak{g}_{/\mathbb{Q}} \xrightarrow{\gamma^{p^{n-1}}-1} \mathfrak{g}_{/\mathbb{Q}} \to 0.$$

Proof. By Proposition 3.3.9, all we need to prove is the exactness at the rightmost term. By Theorem 3.3.11, $\mathfrak{g}(\overline{\mathbb{Q}})$ is a cofree Λ-module, so it is divisible by ω_n. □

CHAPTER 4

Twisted Pairings

We define various pairings between *ordinary* parts of the arithmetic cohomology groups. This section is important for our later use. We keep Notation 3.3.6 and Convention 3.3.8.

For an abelian variety A, we let $A^t := \mathrm{Pic}^0(A)$ be a dual abelian variety of A. If $f : A \to B$ is an isogeny between two abelian varities A and B, we let $f^t : B^t \to A^t$ be the dual isogeny to f.

We introduce various maps on modular Jacobians and state the relations among those maps. Recall the congruence subgroups

$$\begin{aligned}\Gamma_1^1(Np^n) &= \widehat{\Gamma}_1^1(Np^n) \cap \mathrm{SL}_2(\mathbb{Q})\\ \Gamma_{\alpha,\delta,\xi}(Np^n) &= \widehat{\Gamma}_{\alpha,\delta,\xi}(Np^n) \cap \mathrm{SL}_2(\mathbb{Q})\\ \Gamma_0(Np^n) &= \widehat{\Gamma}_0(Np^n) \cap \mathrm{SL}_2(\mathbb{Q}).\end{aligned}$$

4.1 Various actions on Jacobians

4.1.1 Polarization and the Weil involution

Definition 4.1.1. (1) We let $\lambda_n : J_n \to J_n^t$ be the map descended to $\mathbb{Q}$ from the canonical polarization of the modular Jacobian J_n.

(2) We let $w_n : J_n \to J'_n$ be an isomorphism induced by the Weil involution between $X_{\alpha,\delta,\xi}(Np^n)$ and $X_{\delta,\alpha,\xi'}(Np^n)$.

In terms of the double coset operator, we have

$$w_n = [\Gamma_{\alpha,\delta,\xi}(Np^n)\backslash\Gamma_{\alpha,\delta,\xi}(Np^n)\left(\begin{smallmatrix} 0 & -1 \\ p^n & 0 \end{smallmatrix}\right)\Gamma_{\delta,\alpha,\xi'}(Np^n)] : J_n \to J'_n$$

and the inverse of w_n is given by

$$\omega_n^{-1} = [\Gamma_{\delta,\alpha,\xi'}(Np^n)\backslash\Gamma_{\delta,\alpha,\xi'}(Np^n)\left(\begin{smallmatrix} 0 & \frac{1}{p^n} \\ -1 & 0 \end{smallmatrix}\right)\Gamma_{\alpha,\delta,\xi}(Np^n)] : J'_n \to J_n.$$

Definition 4.1.2. (1) For a prime l, we let $T(l)_n$ be a Hecke operator acting on J_n and let $T(l)'_n$ be a Hecke operator acting on J'_n. Here we regard $T(l)_n = U(l)_n$ and $T(l)'_n = U(l)'_n$ for $l \mid Np$.

(2) We let $T^*(l)_n$ be a Rosati involution image of $T(l)_n$ and $T^*(l)'_n$ be a Rosati involution image of $T(l)'_n$.

We have the following two relations:

$$\lambda_n \circ T^*(l)_n = T(l)_n^t \circ \lambda_n \tag{A}$$

$$w_n \circ T^*(l)_n = T(l)'_n \circ w_n \tag{B}$$

4.1.2 Hecke operators

Definition 4.1.3. The natural projection map $X_{\alpha,\delta,\xi}(Np^{n+1}) \twoheadrightarrow X_{\alpha,\delta,\xi}(Np^n)$ induces the following two maps:

(1) $P_{n,n+1} : J_n \to J_{n+1}$ via contravariant Picard functoriality.

(2) $A_{n+1,n} : J_{n+1} \to J_n$ via Albanese functoriality. Note that this map is well-defined since the natural projection map $X_{\alpha,\delta,\xi}(Np^{n+1}) \twoheadrightarrow X_{\alpha,\delta,\xi}(Np^n)$ has constant degree. (Remark 3.1.4-(3).)

We have the following three properties:

$$P_{n,n+1} \circ T(l)_n = T(l)_{n+1} \circ P_{n,n+1} \tag{C}$$

$$A_{n+1,n} \circ T^*(l)_{n+1} = T^*(l)_n \circ A_{n+1,n} \tag{D}$$

$$\lambda_n \circ A_{n+1,n} = P^t_{n,n+1} \circ \lambda_{n+1} \tag{E}$$

4.1.3 Twisted-Covariant map

Definition 4.1.4. We define the twisted-covariant map

$$V'_{n+1,n} := w_n \circ A_{n+1,n} \circ w_{n+1}^{-1} : J'_{n+1} \to J'_n.$$

By (B) and (D), this map satisfies :

$$V'_{n+1,n} \circ T(l)'_{n+1} = T(l)'_n \circ V'_{n+1,n} \tag{F}$$

By [Hid13b, Section 4] and [Hid13a, Section 4], we have:

$$V'_{n+1,n} = 1 + \gamma + \gamma^2 + \cdots + \gamma^{p-1} : J'_{n+1} \to J'_n \tag{G}$$

where γ is a generator of geometric Galois group $\mathrm{Gal}(X_{\delta,\alpha,\xi'}(Np^{n+1})/X_{\delta,\alpha,\xi'}(Np^n))$.

4.1.4 Diamond operators

Note that $\Gamma_0(Np^n)$ acts on $X_{\alpha,\delta,\xi}(Np^n)$ by the geometric Galois action. The action of $h \in \Gamma_0(Np^n)$ induces an automorphism of J_n over $\mathbb{Q}$ via Picard functoriality which can be written in terms of the double coset operator as

$$[\Gamma_{\alpha,\delta,\xi}(Np^n)\backslash\Gamma_{\alpha,\delta,\xi}(Np^n)h\Gamma_{\alpha,\delta,\xi}(Np^n)] : J_n \xrightarrow{\sim} J_n.$$

Similarly, the same $h \in \Gamma_0(Np^n)$ induces another isomorphism

$$[\Gamma_{\alpha,\delta,\xi}(Np^n)\backslash\Gamma_{\alpha,\delta,\xi}(Np^n)h^{-1}\Gamma_{\alpha,\delta,\xi}(Np^n)] : J_n \xrightarrow{\sim} J_n$$

defined over $\mathbb{Q}$ via Albanese functoriality.

By the same reason as with (E), we have the following identity for $g \in \Gamma_0(Np^n)$:

$$\lambda_n \circ [\Gamma_{\alpha,\delta,\xi}(Np^n)\backslash\Gamma_{\alpha,\delta,\xi}(Np^n)g^{-1}\Gamma_{\alpha,\delta,\xi}(Np^n)] = [\Gamma_{\alpha,\delta,\xi}(Np^n)\backslash\Gamma_{\alpha,\delta,\xi}(Np^n)g\Gamma_{\alpha,\delta,\xi}(Np^n)]^t \circ \lambda_n \tag{H}$$

For $g \in \Gamma_0(Np^n)$, if we let $\tilde{g} = \left(\begin{smallmatrix} 0 & -1 \\ p^n & 0 \end{smallmatrix}\right) g^{-1} \left(\begin{smallmatrix} 0 & \frac{1}{p^n} \\ -1 & 0 \end{smallmatrix}\right) \in \Gamma_0(Np^n)$ for the moment, then have the following identity

$$[\Xi \backslash \Xi g^{-1} \Xi] \circ [\Xi' \backslash \Xi' \left(\begin{smallmatrix} 0 & \frac{1}{p^n} \\ -1 & 0 \end{smallmatrix}\right) \Xi] = [\Xi' \backslash \Xi' \left(\begin{smallmatrix} 0 & \frac{1}{p^n} \\ -1 & 0 \end{smallmatrix}\right) \Xi] \circ [\Xi' \backslash \Xi' \tilde{g} \Xi'] \tag{I}$$

where $\Xi = \Gamma_{\alpha,\delta,\xi}(Np^n)$ and $\Xi' = \Gamma_{\delta,\alpha,\xi'}(Np^n)$. We can rewrite the above identity as:

$$[\Gamma_{\alpha,\delta,\xi}(Np^n) \backslash \Gamma_{\alpha,\delta,\xi}(Np^n) g^{-1} \Gamma_{\alpha,\delta,\xi}(Np^n)] \circ w_n^{-1} = w_n^{-1} \circ [\Gamma_{\delta,\alpha,\xi'}(Np^n) \backslash \Gamma_{\delta,\alpha,\xi'}(Np^n) \tilde{g} \Gamma_{\delta,\alpha,\xi'}(Np^n)] \tag{J}$$

4.2 Twisted Weil pairing

Let $W_m^n : J_n[p^m] \times J_n^t[p^m] \to \mu_{p^m}$ be the Weil pairing, which is perfect Galois-equivariant bilinear. We define a twisted Weil pairing

$$H_m^n : J_n[p^m] \times J_n'[p^m] \to \mu_{p^m}$$

by

$$H_m^n(x, y) = W_m^n(x, \lambda_n \circ w_n^{-1}(y))$$

where x, y are elements of $J_n[p^m], J_n'[p^m]$, respectively. We record the basic properties of this twisted pairing.

Proposition 4.2.1. *(1) H_m^n is a perfect, Galois-equivariant bilinear pairing.*

(2) (Hecke-equivariance) $H_m^n\,(T(l)_n(x), y) = H_m^n\,(x, T(l)_n'(y))$ where x, y are elements of $J_n[p^m], J_n'[p^m]$, respectively. Hence, H_m^n induces a perfect pairing

$$H_m^n : \hat{J}_n^{ord}[p^m] \times \hat{J'}_n^{ord}[p^m] \to \mu_{p^m}.$$

(3) For $x \in \hat{J}_n^{ord}[p^m]$ and $y \in \hat{J'}_n^{ord}[p^{m+1}]$, $H_{m+1}^n(x, y) = H_m^n(x, py)$.

Hence there is a perfect Galois-equivariant bilinear pairing $\hat{J}_n^{ord}[p^\infty] \times T_p J_n'^{ord} \to \mu_{p^\infty}$.

(4) For $x \in \hat{J}_n^{ord}[p^m]$ and $y \in \hat{J'}_{n+1}^{ord}[p^m]$, $H_m^{n+1}(P_{n,n+1}(x), y) = H_m^n(x, V_{n+1,n}'(y))$ holds.

(5) Take $g \in \Gamma_0(Np^n)$ and let $\tilde{g} = \left(\begin{smallmatrix} 0 & -1 \\ p^n & 0 \end{smallmatrix}\right) g^{-1} \left(\begin{smallmatrix} 0 & \frac{1}{p^n} \\ -1 & 0 \end{smallmatrix}\right)$. If x, y are elements of

$$\hat{J}_n^{ord}[p^m], \hat{J'}_n^{ord}[p^m],$$

respectively, then we have

$$H_m^n\left([\Gamma_{\alpha,\delta,\xi}(Np^n)\backslash\Gamma_{\alpha,\delta,\xi}(Np^n)g\Gamma_{\alpha,\delta,\xi}(Np^n)]x, y\right)$$

$$= H_m^n\left(x, [\Gamma_{\delta,\alpha,\xi'}(Np^n)\backslash\Gamma_{\delta,\alpha,\xi'}(Np^n)\tilde{g}\Gamma_{\delta,\alpha,\xi'}(Np^n)]y\right).$$

Proof. Since (5) directly follows from (J), we prove (2) and (4) only.

For (2),

$$\begin{aligned}
H_m^n(T(l)_n(x), y) &= W_m^n(T(l)_n(x), \lambda_n \circ w_n^{-1}(y)) && \text{(Definition)}\\
&= W_m^n(x, (T(l)_n)^t \circ \lambda_n \circ w_n^{-1}(y)) && \text{(Property of Weil pairing)}\\
&= W_m^n(x, \lambda_n \circ T^*(l)_n \circ w_n^{-1}(y)) && \text{(By (B))}\\
&= W_m^n(x, \lambda_n \circ w_n^{-1} \circ T(l)'_n(y)) && \text{(By (C))}\\
&= H_m^n(x, T(l)'_n(y)) && \text{(Definition)}
\end{aligned}$$

For (4),

$$\begin{aligned}
H_m^{n+1}(P_{n,n+1}(x), y) &= W_m^{n+1}(P_{n,n+1}(x), \lambda_{n+1} \circ w_{n+1}^{-1}(y)) && \text{(Definition)}\\
&= W_m^n(x, P_{n,n+1}^t \circ \lambda_{n+1} \circ w_{n+1}^{-1}(y)) && \text{(Property of Weil pairing)}\\
&= W_m^n(x, \lambda_n \circ A_{n+1,n} \circ w_{n+1}^{-1}(y)) && \text{(By (F))}\\
&= W_m^n(x, \lambda_n \circ w_n^{-1} \circ V'_{n+1,n}(y)) &&\\
&= H_m^n(x, V'_{n+1,n}(y)) && \text{(Definition)}
\end{aligned}$$

□

For $g = \left(\begin{smallmatrix} a & b \\ cp^n & d \end{smallmatrix}\right) \in \Gamma_0(Np^n)$, we have

$$\tilde{g} = \left(\begin{smallmatrix} 0 & -1 \\ p^n & 0 \end{smallmatrix}\right) g^{-1} \left(\begin{smallmatrix} 0 & \frac{1}{p^n} \\ -1 & 0 \end{smallmatrix}\right) = \frac{1}{ad - bcp^n}\left(\begin{smallmatrix} a & c \\ bp^n & d \end{smallmatrix}\right)$$

and this last matrix is congruent to $\left(\begin{smallmatrix} \frac{1}{d} & \frac{c}{ad} \\ 0 & \frac{1}{a} \end{smallmatrix}\right)$ modulo p^n. Hence we have the following corollary on the Λ-equivariance of our twisted pairing.

Corollary 4.2.2. *The twisted Weil pairing* $H_m^n : \hat{J}_n^{ord}[p^m] \times \hat{J'}_n^{ord}[p^m] \to \mu_{p^m}$ *satisfies*

$$H_m^n(f \cdot x, y) = H_m^n(x, \iota(f) \cdot y)$$

where x, y *are elements of* $\hat{J}_n^{ord}[p^m], \hat{J'}_n^{ord}[p^m]$, *respectively, and* $f \in W[\![T]\!]$.

In particular, we have an isomorphism $\hat{J}_n^{ord}[p^m] \simeq \hat{J'}_n^{ord}[p^m]^\vee$ *of* Λ*-modules.*

4.3 Local Tate duality

We have the following local Tate duality induced from the twisted Weil pairing.

Proposition 4.3.1 (Local Tate duality)**.** *Let* L *be a finite extension of* $\mathbb{Q}_l$.

(1) For $i = 0, 1, 2$, *the pairings* $H^i(L, \hat{J}_n^{ord}[p^m]) \times H^{2-i}(L, \hat{J'}_n^{ord}[p^m])^\iota \to Q(W)/W$ *are perfect* Λ*-equivariant bilinear pairings between finite* p*-abelian groups.*

(2) The images of the Kummer maps on $\frac{\hat{J}_n^{ord}(L)}{p^m \hat{J}_n^{ord}(K)}$ *and* $\frac{\hat{J'}_n^{ord}(L)}{p^m \hat{J'}_n^{ord}(L)}$ *into cohomology groups are orthogonal complements to each other under the pairing*

$$H^1(L, \hat{J}_n^{ord}[p^m]) \times H^1(L, \hat{J'}_n^{ord}[p^m]) \to Q(W)/W$$

of (1).

By this local Tate duality, we can construct the following perfect pairing between two Λ-modules.

Corollary 4.3.2. *Let* L *be a finite extension of* $\mathbb{Q}_l$ *for some prime* l.

(1) There is a perfect bilinear Λ*-equivariant pairing*

$$\hat{J}_n^{ord}[p^\infty](L) \times H^1(L, \hat{J'}_n^{ord}[p^\infty])^\iota_{/div} \to Q(W)/W$$

between finite p*-abelian groups.*

(2) The above pairing induces a perfect Λ*-equivariant pairing*

$$\mathfrak{g}(L) \times \varprojlim_n H^1(L, \hat{J'}_n^{ord}[p^\infty])^\iota_{/div} \to Q(W)/W$$

where the inverse limit is taken with respect to $V'_{n+1,n}$.

Note that $H^2(L, A) = 0$ for any abelian variety defined over L due to [Mil06, Theorem I.3.2]. Hence we have an isomorphism $H^1(L, A) \otimes \mathbb{Q}_p/\mathbb{Z}_p \simeq H^2(L, A[p^\infty])$ where the first group is zero since $H^1(L, A)$ is a torsion abelian group. Therefore, we have $H^2(L, A[p^\infty]) = 0$.

Proof. By the remark above, we have $H^2(L, {\hat{J}'}^{ord}_n[p^\infty]) = 0$. Hence we get

$$\frac{H^1(L, {\hat{J}'}^{ord}_n[p^\infty])}{p^t H^1(L, {\hat{J}'}^{ord}_n[p^\infty])} \simeq H^2(L, {\hat{J}'}^{ord}_n[p^t]) \simeq \hat{J}^{ord}_n[p^t](L)^\vee$$

for all t. For the last isomorphism, we used Proposition 4.3.1-(1). Passing to the projective limit with respect to t gives the desired assertion. □

4.4 Poitou-Tate duality

We have the (global) Poitou-Tate duality (See [Mil06, Theorem I.4.10] for the reference) induced from the twisted Weil pairing.

Proposition 4.4.1 (Poitou-Tate duality)**.** *There is a perfect Λ-equivariant pairing of finite p-abelian groups*

$$Ш^1_K(\hat{J}^{ord}_n[p^m]) \times Ш^2_K({\hat{J}'}^{ord}_n[p^m])^\iota \to Q(W)/W.$$

Later in the subsection 5.2.2, we will compare the Λ-coranks of $Ш^1_K(\mathfrak{g})$ and $Ш^2_K(\mathfrak{g}')$ by using this pairing. (See Proposition 5.2.8)

4.5 Twisted pairings of Flach and Cassels-Tate

4.5.1 Description of the original pairings

We briefly recall properties of pairing of Flach and Cassels-Tate.

Let K be a number field, A be an abelian variety defined over K, and let S be a finite set of places of K containing infinite places, places over p and the places of bad reduction of A. We recall the Selmer group and the Tate-Shafarevich group associated to $\widehat{A}$ (see Definition

3.3.3):

$$\mathrm{Sel}_K(\widehat{A}) := \mathrm{Ker}\left(H^1(K^S/K, \widehat{A}[p^\infty]) \to \prod_{v\in S} H^1(K_v, \widehat{A})\right)$$

$$Ш^1_K(\widehat{A}) := \mathrm{Ker}\left(H^1(K^S/K, \widehat{A}) \to \prod_{v\in S} H^1(K_v, \widehat{A})\right)$$

As we remarked before, these definitions are independent of the choice of S as long as S is finite and S contains infinite places, places over p and the places of bad reduction of A.

Remark 4.5.1. If A is a modular Jacobian J_n, then $\mathrm{Sel}_K(\widehat{J_n})$ and $Ш^1_K(\widehat{J_n})$ are $\mathbf{h}_{\alpha,\delta,\xi}$-modules and we have $\mathrm{Sel}_K(\widehat{J_n})^{ord} = \mathrm{Sel}_K(\hat{J}_n^{ord})$ and $Ш^1_K(\widehat{J_n})^{ord} = Ш^1_K(\hat{J}_n^{ord})$.

Flach [Fla90] constructed a bilinear pairing $F_A : \mathrm{Sel}_K(\widehat{A}) \times \mathrm{Sel}_K(\widehat{A^t}) \to Q(W)/W$ whose left kernel (resp. right kernel) is the maximal p-divisible subgroup of $\mathrm{Sel}_K(\widehat{A})$ (resp. $\mathrm{Sel}_K(\widehat{A^t})$). Moreover, for an isogeny $f : A \to B$ defined over K, we have

$$F_A(x, f^t(y)) = F_B(f(x), y)$$

for $x \in \mathrm{Sel}_K(\widehat{A})$ and $y \in \mathrm{Sel}_K(\widehat{B^t})$. Note that the Cassels-Tate pairing $C_A : Ш^1_K(\widehat{A}) \times Ш^1_K(\widehat{A^t}) \to Q(W)/W$ also satisfies the same functorial property (See [Mil06, Theorem I.6.26]).

4.5.2 Twisted pairing

For the modular Jacobian J_n, we define the twisted Flach's pairing and the twisted Cassels-Tate pairing by

$$S^n(x, y) = F_{J_n}(x, \lambda_n \circ w_n^{-1}(y))$$

for $x \in \mathrm{Sel}_K(\widehat{J_n})$ and $y \in \mathrm{Sel}_K(\widehat{J'_n})$ and

$$CT^n(z, v) = C_{J_n}(z, \lambda_n \circ w_n^{-1}(v))$$

for $z \in Ш^1_K(\widehat{J_n})$ and $v \in Ш^1_K(\widehat{J'_n})$. We record properties of the pairing S^n below. (Note that the twisted Cassels-Tate pairing CT^n also satisfies the same properties.)

Proposition 4.5.2. *(1) (Hecke-equivariance)* $S^n(T(l)_n(x), y) = S^n(x, T(l)'_n(y))$ *where* x, y *are elements of* $\mathrm{Sel}_K(\widehat{J_n}), \mathrm{Sel}_K(\widehat{J'_n})$*, respectively. Hence,* S^n *induces a bilinear pairing*

$$S^n : \mathrm{Sel}_K(\hat{J}_n^{ord}) \times \mathrm{Sel}_K(\hat{J'}_n^{ord}) \to Q(W)/W.$$

(2) $S^n : \mathrm{Sel}_K(\hat{J}_n^{ord})_{/div} \times \mathrm{Sel}_K(\hat{J'}_n^{ord})_{/div} \to Q(W)/W$ *is a perfect bilinear pairing.*

(3) For $x \in \mathrm{Sel}_K(\hat{J}_n^{ord})$ *and* $y \in \mathrm{Sel}_K(\hat{J'}_{n+1}^{ord})$*, we have*

$$S^{n+1}\left(P_{n,n+1}(x), y\right) = S^n\left(x, V'_{n+1,n}(y)\right).$$

(4) The twisted Flach pairing S^n *satisfies*

$$S^n(f \cdot x, y) = S^n(x, \iota(f) \cdot y)$$

where x, y *are elements of* $\mathrm{Sel}_K(\hat{J}_n^{ord}), \mathrm{Sel}_K(\hat{J'}_n^{ord})$*, respectively and* $f \in W[\![T]\!]$.

In particular, we have an isomorphism $\mathrm{Sel}_K(\hat{J}_n^{ord})_{/div} \simeq \left(\mathrm{Sel}_K(\hat{J'}_n^{ord})_{/div}\right)^{\vee}$ *of* Λ*-modules.*

Since the proof of Proposition 4.5.2 is almost identical with those of Proposition 4.2.1 and Corollary 4.2.2, we omit the proof.

CHAPTER 5

Cohomology groups arising from the Barsotti-Tate group $\mathfrak{g}$

5.1 Local cohomology groups

In this section, we let L be a finite extension of $\mathbb{Q}_l$. (Here l can be equal to p unless we mention that $l \neq p$.) We keep Notation 3.3.6 and Convention 3.3.8.

5.1.1 Basic facts

Note that $H^2(L, A) = 0$ for any abelian variety defined over L due to [Mil06, Theorem I.3.2]. Hence we have an isomorphism $H^1(L, A) \otimes \mathbb{Q}_p/\mathbb{Z}_p \simeq H^2(L, A[p^\infty])$ where the first group is zero since $H^1(L, A)$ is a torsion abelian group. Therefore, we have $H^2(L, A[p^\infty]) = 0$.

Lemma 5.1.1. *We have the following assertions:*

(1) $\mathfrak{g}(L)^\vee$ is a finitely generated torsion Λ-module whose characteristic ideal is prime to ω_n for all n. In particular, $\mathfrak{g}(L)/\omega_n\mathfrak{g}(L)$ has finite bounded order independent of n. We have $\varinjlim_n \frac{\mathfrak{g}(L)}{\omega_n\mathfrak{g}(L)} = 0$. Moreover $\varprojlim_n \frac{\mathfrak{g}(L)}{\omega_n\mathfrak{g}(L)}$ is isomorphic to Pontryagin dual of the maximal finite submodule of $\mathfrak{g}(L)^\vee$ as Λ-modules.

(2) $H^2(L, \mathfrak{g}) = 0$.

(3) $H^1(L, \mathfrak{g})^\vee[\omega_n] = 0$. Hence $H^1(L, \mathfrak{g})^\vee$ has no non-trivial finite Λ-submodules and the characteristic ideal of $(H^1(L, \mathfrak{g})^\vee)_{\Lambda-\mathrm{tor}}$ is coprime to ω_n for all n.

Proof. By the control sequence (Proposition 3.3.9), we have $\hat{J}_n^{ord}[p^\infty](L) = \mathfrak{g}(L)[\omega_n]$, and this group is finite since L is a finite extension of $\mathbb{Q}_l$ (Nagell-Lutz). So the first assertion follows from Nakayama's lemma. For (2), $H^2(L, \hat{J}_n^{ord}[p^\infty]) = 0$ as we remarked earlier, so we have $H^2(L, \mathfrak{g}) = \varinjlim_n H^2(L, \hat{J}_n^{ord}[p^\infty]) = 0$.

For (3), $\frac{H^1(L,\mathfrak{g})}{\omega_n H^1(L,\mathfrak{g})}$ injects into $H^2(L, \hat{J}_n^{ord}[p^\infty]) = 0$ so $H^1(L, \mathfrak{g})^\vee[\omega_n] = 0$, which shows (3). □

Next we calculate the Euler characteristic of the cohomology groups above.

Lemma 5.1.2 (Local Euler Characteristic Formula)**.**

$$(1) \quad \operatorname{corank}_W H^1(L, \hat{J}_n^{ord}[p^\infty]) = \begin{cases} p^{n-1} \cdot [L : \mathbb{Q}_l] \cdot \operatorname{corank}_\Lambda \mathfrak{g}(\overline{L}) & l = p \\ 0 & l \neq p \end{cases}$$

$$(2) \quad \operatorname{corank}_\Lambda H^1(L, \mathfrak{g}) = \begin{cases} [L : \mathbb{Q}_l] \cdot \operatorname{corank}_\Lambda \mathfrak{g}(\overline{L}) & l = p \\ 0 & l \neq p \end{cases}$$

Proof. By Proposition 3.3.9, we have an isomorphism $\hat{J}_n^{ord}[p^\infty](\overline{L}) \simeq \mathfrak{g}(\overline{L})[\omega_n]$. Hence $\hat{J}_n^{ord}[p^\infty](\bar{L})$ is a cofree W-module of corank $p^{n-1} \cdot \operatorname{corank}_\Lambda \mathfrak{g}(\overline{L})$ by Theorem 3.3.11-(1). Now the usual Euler characteristic formula shows (1). (Note that $\hat{J}_n^{ord}[p^\infty](L)$ is finite.)

For (2), we have the following short exact sequence by Corollary 3.3.13:

$$0 \to \frac{\mathfrak{g}(L)}{\omega_n \mathfrak{g}(L)} \to H^1(L, \hat{J}_n^{ord}[p^\infty]) \to H^1(L, \mathfrak{g})[\omega_n] \to 0.$$

Since $\frac{\mathfrak{g}(L)}{\omega_n \mathfrak{g}(L)}$ is a finite group by Lemma 5.1.1-(1), comparing W-coranks proves the second assertion. □

5.1.2 Functors $\mathfrak{F}$ and $\mathfrak{G}$

We record the definitions and properties of the functors $\mathfrak{F}$ and $\mathfrak{G}$ the proofs of which are given in the Chapter 7 of this thesis.

Definition 5.1.3. For a finitely generated Λ-module X, we define

$$\mathfrak{F}(X) := \left(\varinjlim_n \frac{X}{\omega_n X}[p^\infty] \right)^\vee$$

$$\mathfrak{G}(X) := \varprojlim_n \left(\frac{X}{\omega_n X}[p^\infty] \right).$$

Here the direct limit is taken with respect to the norm maps $\frac{X}{\omega_n X} \xrightarrow{\times \frac{\omega_{n+1}}{\omega_n}} \frac{X}{\omega_{n+1} X}$, and the inverse limit is taken with respect to the natural projections. We have the following proposition about the explicit description of two functors $\mathfrak{F}$ and $\mathfrak{G}$. For the proof, see the Chapter 7 of this thesis (Proposition 7.1.6, Proposition 7.2.5).

Proposition 5.1.4. *Let X be a finitely generated Λ-module with*

$$E(X) \simeq \Lambda^r \oplus \left(\bigoplus_{i=1}^{d} \frac{\Lambda}{g_i^{l_i}} \right) \oplus \left(\bigoplus_{\substack{m=1 \\ e_1,\dots,e_f \geq 2}}^{f} \frac{\Lambda}{\omega_{a_m+1,a_m}^{e_m}} \right) \oplus \left(\bigoplus_{n=1}^{t} \frac{\Lambda}{\omega_{b_n+1,b_n}} \right),$$

where $r \geq 0$, $g_1, \dots g_d$ are prime elements of Λ which are coprime to ω_n for all n, $d \geq 0$, $l_1, \dots, l_d \geq 1$, $f \geq 0$, $e_1, \dots, e_f \geq 2$ and $t \geq 0$.

(1) We have an injection

$$\left(\bigoplus_{i=1}^{d} \frac{\Lambda}{\iota(g_i)^{l_i}} \right) \oplus \left(\bigoplus_{\substack{m=1 \\ e_1,\dots,e_f \geq 2}}^{f} \frac{\Lambda}{\iota(\omega_{a_m+1,a_m})^{e_m-1}} \right) \hookrightarrow \mathfrak{F}(X)$$

with finite cokernel. In particular, $\mathfrak{F}(X)$ is a finitely generated Λ-torsion module.

(2) We have a pseudo-isomorphism

$$\mathfrak{G}(X) \xrightarrow{\mathfrak{G}(\phi)} \left(\bigoplus_{i=1}^{d} \frac{\Lambda}{g_i^{l_i}} \right) \oplus \left(\bigoplus_{\substack{m=1 \\ e_1,\dots,e_f \geq 2}}^{f} \frac{\Lambda}{\omega_{a_m+1,a_m}^{e_m-1}} \right).$$

In particular, $\mathfrak{G}(X)$ is a finitely generated Λ-torsion module.

(3) The two Λ-torsion modules $\mathfrak{F}(X)^\iota$ and $\mathfrak{G}(X)$ are pseudo-isomorphic.

We mention one corollary which will be used in Corollary 5.1.7.

Corollary 5.1.5. *Let X be a finitely generated Λ-module. If the characteristic ideal of $X_{\Lambda-\mathrm{tor}}$ is coprime to ω_n for all n, then there is a pseudo-isomorphism $\phi : X \to \Lambda^{\mathrm{rank}_\Lambda X} \oplus \mathfrak{F}(X)^\iota$. If we assume additionally that X does not have any non-trivial finite Λ-submodules, then ϕ is an injection.*

5.1.3 Application of the local Tate duality

By applying the functor $\mathfrak{F}$ to $H^1(L,\mathfrak{g})^\vee$, we can compare the Λ-module structure of the local cohomology groups of the Barsotti-Tate groups of two different towers. This can be regarded as an analogue of [Gre89, Proposition 1, 2].

Proposition 5.1.6. *There is a surjection $\phi : \mathfrak{g}'(L)^\vee \twoheadrightarrow \mathfrak{F}\left(H^1(L,\mathfrak{g})^\vee\right)$ with finite kernel. In particular, the two Λ-torsion modules $\mathfrak{g}'(L)^\vee$ and $\mathfrak{F}\left(H^1(L,\mathfrak{g})^\vee\right)$ are pseudo-isomorphic.*

Proof. By Corollary 3.3.13, we have a short exact sequence

$$0 \to \frac{\mathfrak{g}(L)}{\omega_n \mathfrak{g}(L)} \to H^1(L, \hat{J}_n^{ord}[p^\infty]) \to H^1(L,\mathfrak{g})[\omega_n] \to 0.$$

Since $\frac{\mathfrak{g}(L)}{\omega_n \mathfrak{g}(L)}$ is finite, we get $\frac{\mathfrak{g}(L)}{\omega_n \mathfrak{g}(L)} \to H^1(L, \hat{J}_n^{ord}[p^\infty])_{/div} \to (H^1(L,\mathfrak{g})[\omega_n])_{/div} \to 0$ by Lemma 2.1.4-(3). Note that all terms in this sequence are finite. Taking the projective limit gives the following exact sequence:

$$\varprojlim_n \frac{\mathfrak{g}(L)}{\omega_n \mathfrak{g}(L)} \to \varprojlim_n H^1(L, \hat{J}_n^{ord}[p^\infty])_{/div} \to \varprojlim_n \left(H^1(L,\mathfrak{g})[\omega_n]\right)_{/div} \to 0.$$

By Lemma 5.1.1-(1), the first term is isomorphic to the Pontryagin dual of the maximal finite submodule of $\mathfrak{g}(L)^\vee$. For the second term, we have an isomorphism

$$\varprojlim_n H^1(L, \hat{J}_n^{ord}[p^\infty])_{/div} \simeq \mathfrak{g}'(L)^\vee$$

by Corollary 4.3.2-(2). The last term is $\mathfrak{F}\left(H^1(L,\mathfrak{g})^\vee\right)$ by definition. □

Corollary 5.1.7. *(1) If $l \neq p$, then there is an injective map $H^1(L,\mathfrak{g})^\vee \hookrightarrow (\mathfrak{g}'(L)^\vee)^\iota$ with finite cokernel.*

(2) If $l = p$, then there is an injective map $H^1(L,\mathfrak{g})^\vee \hookrightarrow \Lambda^{[L:\mathbb{Q}_p]\cdot \mathrm{corank}_\Lambda \mathfrak{g}(\overline{L})} \oplus (\mathfrak{g}'(L)^\vee)^\iota$ with finite cokernel.

Proof. (1) and (2) follow from Lemma 5.1.1-(3), Proposition 5.1.6 and Corollary 5.1.5. □

Corollary 5.1.8. *(1) If $l \neq p$, then $\mathfrak{g}'(L)$ is finite if and only if $H^1(L, \mathfrak{g})^\vee = 0$.*

(2) If $l = p$, then $\mathfrak{g}'(L)$ is finite if and only if $H^1(L, \mathfrak{g})^\vee$ is a Λ-torsion-free module if and only if $H^1(L, \mathfrak{g})^\vee$ is a Λ-submodule of $\Lambda^{[L:\mathbb{Q}_p]\cdot \mathrm{corank}_\Lambda \mathfrak{g}(\overline{L})}$ of finite index. This finite index is bounded by the size of $\mathfrak{g}'(L)$.

Proof. (1) is a direct consequence of Corollary 5.1.7-(1). The equivalence of the three statements in (2) follows from Lemma 5.1.1-(3) and Corollary 5.1.7-(2).

Now we prove that if $l = p$ and $H^1(L, \mathfrak{g})^\vee$ is a Λ-submodule of $\Lambda^{[L:\mathbb{Q}_p]\cdot \mathrm{corank}_\Lambda \mathfrak{g}(\overline{L})}$ of finite index, then this index is bounded by the size of $\mathfrak{g}'(L)$.

Let C be the kernel of inclusion $H^1(L, \mathfrak{g})^\vee \hookrightarrow \Lambda^{2[L:\mathbb{Q}_p]\cdot \mathrm{corank}_\Lambda \mathfrak{g}(\overline{L})}$. For the large enough n, we have an exact sequence $0 \to C \hookrightarrow \frac{H^1(L,\mathfrak{g})^\vee}{\omega_n H^1(L,\mathfrak{g})^\vee} \to \frac{\Lambda}{\omega_n \Lambda}^{2[L:\mathbb{Q}_p]\cdot \mathrm{corank}_\Lambda \mathfrak{g}(\overline{L})}$ by the snake lemma. Hence we get an isomorphism

$$C \simeq \frac{H^1(L, \mathfrak{g})^\vee}{\omega_n H^1(L, \mathfrak{g})^\vee}[p^\infty]$$

for large enough n. The last group is the Pontryagin dual of $(H^1(L, \mathfrak{g})[\omega_n])_{/div}$.

On the other hand, from a natural exact sequence

$$0 \to \frac{\mathfrak{g}(L)}{\omega_n \mathfrak{g}(L)} \to H^1(L, \hat{J}_n^{ord}[p^\infty]) \to H^1(L, \mathfrak{g})[\omega_n] \to 0,$$

$(H^1(L, \mathfrak{g})[\omega_n])_{/div}$ is a homomorphic image of the group $H^1(L, \hat{J}_n^{ord}[p^\infty])_{/div}$, which is the Pontryagin dual of $\hat{J'}_n^{ord}[p^\infty](L)$ by Corollary 4.3.2-(1). Hence $|C|$ is bounded by $|\hat{J'}_n^{ord}[p^\infty](L)|$ for all sufficiently large n. □

Corollary 5.1.9. *If $l = p$ and $\mathfrak{g}'(L) = 0$ holds, then we have:*

- *$H^1(L, \hat{J}_n^{ord}[p^\infty])$ is a W-cofree module of corank $p^{n-1} \cdot [L : \mathbb{Q}_p] \cdot \mathrm{corank}_\Lambda \mathfrak{g}(\overline{L})$.*
- *$H^1(L, \mathfrak{g})$ is a Λ-cofree module of corank $[L : \mathbb{Q}_p] \cdot \mathrm{corank}_\Lambda \mathfrak{g}(\overline{L})$.*

Proof. Since

$$\frac{H^1(L, \hat{J}_n^{ord}[p^\infty])}{pH^1(L, \hat{J}_n^{ord}[p^\infty])} \simeq H^2(L, \hat{J}_n^{ord}[p]) \simeq \hat{J'}_n^{ord}[p](L)^\vee = 0$$

by the assumption, $H^1(L, \hat{J}_n^{ord}[p^\infty])$ is a W-cofree. The second statement follows from Corollary 5.1.8-(2). □

5.1.4 Λ-adic Mordell-Weil groups over p-adic fields

We study the Λ-module structure of the Mordell-Weil groups over p-adic fields in this subsection. Recall that $\mathfrak{G}(X) = \varprojlim_n (\frac{X}{\omega_n X}[p^\infty])$ for a finitely generated Λ-module X.

Proposition 5.1.10. *Let L be a finite extension of $\mathbb{Q}_p$.*

(1) The natural map $\hat{J}^{ord}_n(L) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p \to J^{ord}_\infty(L) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p[\omega_n]$ has finite kernel for all n whose orders are bounded as n varies.

(2) $(J^{ord}_\infty(L) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)^\vee$ is $\mathbb{Z}_p$-torsion-free. In particular, $(J^{ord}_\infty(L) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)^\vee$ has no non-trivial finite Λ-submodules.

(3) $\mathfrak{G}\left((J^{ord}_\infty(L) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)^\vee\right) = 0$.

(4) We have a Λ-linear injection

$$(J^{ord}_\infty(L) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)^\vee \hookrightarrow \Lambda^r \oplus \left(\bigoplus_{n=1}^{t} \frac{\Lambda}{\omega_{b_n, b_n - 1}} \right)$$

with finite cokernel for some integers $r, b_1, \ldots, b_n$.

Proof. The proof is essentially same as that of [Lee18, Theorem 2.1.2] □

Lemma 5.1.11. *Let $0 \to X \to Y \to Z \to 0$ be an exact sequence of finitely generated Λ-modules. If $char_\Lambda(Z_{\Lambda-\mathrm{tor}})$ is coprime to $char_\Lambda(Y_{\Lambda-\mathrm{tor}})$, then we have the following statements:*

(1) The natural injection $X_{\Lambda-\mathrm{tor}} \hookrightarrow Y_{\Lambda-\mathrm{tor}}$ has finite cokernel.

(2) If we assume furthermore that Z does not have any non-trivial finite Λ-submodule, then we have an isomorphism $X_{\Lambda-\mathrm{tor}} \simeq Y_{\Lambda-\mathrm{tor}}$. Hence X is Λ-torsion-free if and only if Y is Λ-torsion-free.

(3) Under the same assumption of (2), if X is a torsion Λ-module, then Z is a torsion-free Λ-module with $\mathrm{rank}_\Lambda Y = \mathrm{rank}_\Lambda Z$.

(4) Under the same assumption of (2), if Y is a Λ-free module, then X is also a Λ-free module.

Proof. From an exact sequence $0 \to X_{\Lambda-\mathrm{tor}} \to Y_{\Lambda-\mathrm{tor}} \to Z_{\Lambda-\mathrm{tor}}$ and the assumption about characteristic ideals, the image of $Y_{\Lambda-\mathrm{tor}} \to Z_{\Lambda-\mathrm{tor}}$ should be finite, which shows (1). Note that (2) is a direct consequence of (1).

For (3), if X is a torsion Λ-module, then we have the following exact sequence

$$0 \to X_{\Lambda-\mathrm{tor}} \to Y_{\Lambda-\mathrm{tor}} \to Z_{\Lambda-\mathrm{tor}} \to 0$$

by Lemma 2.1.4-(1). Since $char_{\Lambda}(Z_{\Lambda-\mathrm{tor}})$ is coprime to $char_{\Lambda}(Y_{\Lambda-\mathrm{tor}})$, $char_{\Lambda}(Z_{\Lambda-\mathrm{tor}})$ is whole Λ due to the multiplicative property of characteristic ideals. Since Z does not contain any non-trivial finite Λ-submodule, we have $Z_{\Lambda-\mathrm{tor}} = 0$.

Now we prove (4). By the assumptions on Y and Z, we have $X[\omega_n] = Y[\omega_n] = 0$ and an exact sequence $Z[\omega_n] \hookrightarrow \frac{X}{\omega_n X} \to \frac{Y}{\omega_n Y}$. Here $Z[\omega_n]$ is a free $\mathbb{Z}_p$-module since Z does not have any non-trivial finite Λ-submodule, and $\frac{Y}{\omega_n Y}$ is a $\mathbb{Z}_p$-free module since Y is a Λ-free. Therefore $\frac{X}{\omega_n X}$ is also a free $\mathbb{Z}_p$-module and this shows that X is a Λ-free by [NSW00, Proposition 5.3.19]. □

By applying the above lemma to the exact sequence

$$0 \to \left(\frac{H^1(L, \mathfrak{g})}{J^{ord}_{\infty}(L) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p} \right)^{\vee} \to (H^1(L, \mathfrak{g}))^{\vee} \to (J^{ord}_{\infty}(L) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)^{\vee} \to 0,$$

we obtain the following proposition.

Proposition 5.1.12. *Let L be a finite extension of $\mathbb{Q}_p$.*

(1) $\mathrm{corank}_{\Lambda} \left(J^{ord}_{\infty}(L) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p\right) \geq \frac{1}{2}[L : \mathbb{Q}_p] \cdot \mathrm{corank}_{\Lambda}\, \mathfrak{g}(\overline{L}) \geq \mathrm{corank}_{\Lambda} \left(\frac{H^1(L,\mathfrak{g})}{J^{ord}_{\infty}(L) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p} \right)$.

(2) We have an isomorphism $\left(\frac{H^1(L,\mathfrak{g})}{J^{ord}_{\infty}(L) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p} \right)^{\vee}_{\Lambda-\mathrm{tor}} \simeq H^1(L, \mathfrak{g})^{\vee}_{\Lambda-\mathrm{tor}}$.

(3) We have a Λ-linear injection $\left(\frac{H^1(L,\mathfrak{g})}{J^{ord}_{\infty}(L) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p} \right)^{\vee} \hookrightarrow \Lambda^r \oplus (\mathfrak{g}'(L)^{\vee})^{\iota}$ *with finite cokernel where* $r \leq \frac{1}{2}[L : \mathbb{Q}_p] \cdot \mathrm{corank}_{\Lambda}\, \mathfrak{g}(\overline{L})$.

(4) $\left(\frac{H^1(L,\mathfrak{g})}{J^{ord}_{\infty}(L) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p} \right)^{\vee}$ *is Λ-torsion-free if and only if $H^1(L, \mathfrak{g})$ is Λ-torsion-free if and only if $\mathfrak{g}'(L)$ is finite.*

(5) Assume that $H^1(L, \mathfrak{g})$ is Λ-cofree (for instance, under the assumption of Corollary *5.1.9). Then $\frac{H^1(L,\mathfrak{g})}{J_\infty^{ord}(L)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p}$ is a cofree Λ-module with*

$$\mathrm{corank}_\Lambda \left(\frac{H^1(L, \mathfrak{g})}{J_\infty^{ord}(L) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p} \right) \leq \frac{1}{2}[L : \mathbb{Q}_p] \cdot \mathrm{corank}_\Lambda\, \mathfrak{g}(\overline{L}).$$

Proof. For (1), by Lemma 5.1.2-(2), it is sufficient to prove the first inequality only. Since $\hat{J}_n^{ord}(L)$ is a p-adic Lie group of dimension $\frac{p^{n-1}}{2} \cdot [L : \mathbb{Q}_p] \cdot \mathrm{corank}_\Lambda\, \mathfrak{g}(\overline{L})$ by [Hid17, Lemma 5.5], we get (1) from Proposition 5.1.10-(1).

By Proposition 5.1.10-(2), $(J_\infty^{ord}(L) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)^\vee$ has no non-trivial finite Λ-submodule. This shows (2) by Lemma 5.1.11-(2). (3) follows from (1) and Corollary 5.1.7-(2). (4) follows from Lemma 5.1.11-(2) and Corollary 5.1.8-(2). (5) is a direct consequence of Lemma 5.1.11-(4). □

5.2 Global cohomology groups

In this section, in addition to Notation 3.3.6 and Convention 3.3.8, we also assume the following.

Convention 5.2.1 (Global). *We let K be a number field and S be a finite set of places of K containing the infinite places and places dividing Np.*

We first mention one basic lemma on Λ-cotorsionness of H^0 for our later use. It is an analogue of Lemma 5.1.1-(1) and hence we omit the proof. (The proof of Lemma 5.1.1-(1) still works if we use Mordell-Weil theorem instead of Nagell-Lutz.)

Lemma 5.2.2. *$\mathfrak{g}(K)^\vee$ is a finitely generated torsion Λ-module whose characteristic ideal is prime to ω_n for all n. In particular, $\frac{\mathfrak{g}(K)}{\omega_n\mathfrak{g}(K)}$ has finite bounded order independent of n. We have $\varinjlim_n \dfrac{\mathfrak{g}(K)}{\omega_n\mathfrak{g}(K)} = 0$. Moreover $\varprojlim_n \dfrac{\mathfrak{g}(K)}{\omega_n\mathfrak{g}(K)}$ is isomorphic to the Pontryagin dual of the maximal finite submodule of $\mathfrak{g}(K)^\vee$ as a Λ-module.*

5.2.1 Cofreeness of H^2

Lemma 5.2.3. *Let A be an abelian variety over a number field K, and let S be a finite set of places of K containing infinite places, places over p, and places of bad reduction of A. Then we have:*

(1) $H^i(K^S/K, A[p^\infty]) = 0$ for all $i \geq 3$.

(2) $H^2(K^S/K, A[p^\infty])$ is a W-cofree module. In particular, $H^2(K^S/K, A[p^\infty]) = 0$ if and only if $H^2(K^S/K, A[p^\infty])$ has trivial W-corank.

Proof. Since $\mathrm{Gal}(K^S/K)$ has p-cohomological dimension 2 (p is odd), we get the vanishing of $H^i(K^S/K, A[p^m])$ for all m and for all $i \geq 3$. Passing to the direct limit gives (1). For (2), note that we have an injection

$$\frac{H^2(K^S/K, A[p^\infty])}{pH^2(K^S/K, A[p^\infty])} \hookrightarrow H^3(K^S/K, A[p]) = 0.$$

Hence $H^2(K^S/K, A[p^\infty])$ is a p-divisible cofinitely generated W-module, so W-cofree. □

Corollary 5.2.4. *(1) $H^i(K^S/K, \hat{J}_n^{ord}[p^\infty]) = H^i(K^S/K, \mathfrak{g}) = 0$ for all $i \geq 3$.*

(2) $H^2(K^S/K, \mathfrak{g})$ is a Λ-cofree module.

Proof. The first assertion of (1) follows from Lemma 5.2.3-(1). Taking the direct limit with respect to n proves the assertion for $\mathfrak{g}$.

For (2), we have an injection $\frac{H^2(K^S/K,\mathfrak{g})}{\omega_n H^2(K^S/K,\mathfrak{g})} \hookrightarrow H^3(K^S/K, \hat{J}_n^{ord}[p^\infty])$ which implies that $\frac{H^2(K^S/K,\mathfrak{g})}{\omega_n H^2(K^S/K,\mathfrak{g})} = 0$ by the previous Lemma 5.2.3-(1). On the other hand, $H^2(K^S/K, \mathfrak{g})[\omega_n]$ is W-cofree since it is a homomorphic image of a W-cofree module $H^2(K^S/K, \hat{J}_n^{ord}[p^\infty])$. By [NSW00, Proposition 5.3.19], $H^2(K^S/K, \mathfrak{g})$ is Λ-cofree. □

Corollary 5.2.5. *If $H^2(K^S/K, \mathfrak{g}) = 0$, then $H^1(K^S/K, \mathfrak{g})^\vee$ has no non-trivial finite Λ-submodules.*

Proof. We have an isomorphism $H^1(K^S/K, \mathfrak{g})^\vee[\omega_n] \simeq H^2(K^S/K, \hat{J}_n^{ord}[p^\infty])^\vee$ where the last group is W-free by Lemma 5.2.3-(2). For the large enough n, the maximal finite submodule of $H^1(K^S/K,\mathfrak{g})^\vee$ is contained in $H^1(K^S/K,\mathfrak{g})^\vee[\omega_n]$. Hence it has to vanish since any W-free module does not have non-trivial finite submodules. $\square$

We have the following global Euler characteristic formula of cohomology of Barsotti-Tate groups.

Proposition 5.2.6 (Global Euler Characteristic Formula)**.** *We have the following two identities:*

$$\mathrm{corank}_W\, H^1(K^S/K,\hat{J}_n^{ord}[p^\infty]) - \mathrm{corank}_W\, H^2(K^S/K,\hat{J}_n^{ord}[p^\infty]) = \frac{1}{2}[K:\mathbb{Q}]\cdot p^{n-1}\cdot \mathrm{corank}_\Lambda\, \mathfrak{g}(\overline{\mathbb{Q}}).$$

$$\mathrm{corank}_\Lambda\, H^1(K^S/K,\mathfrak{g}) - \mathrm{corank}_\Lambda\, H^2(K^S/K,\mathfrak{g}) = \tfrac{1}{2}[K:\mathbb{Q}]\cdot \mathrm{corank}_\Lambda\, \mathfrak{g}(\overline{\mathbb{Q}}).$$

In particular,

$$\mathrm{corank}_\Lambda\, H^1(K^S/K,\mathfrak{g}) = \frac{1}{2}[K:\mathbb{Q}]\cdot \mathrm{corank}_\Lambda\, \mathfrak{g}(\overline{\mathbb{Q}})$$

if and only if

$$H^2(K^S/K,\mathfrak{g}) = 0.$$

The assertion about the W-corank follows from the usual global Euler characteristic formula combined with Theorem 3.3.11-(2). The last equivalence follows from Corollary 5.2.4-(2).

Proof. If we compute the W-corank of the exact sequence

$$0 \to \frac{H^1(K^S/K,\mathfrak{g})^\vee}{\omega_n H^1(K^S/K,\mathfrak{g})^\vee} \to H^1(K^S/K,\hat{J}_n^{ord}[p^\infty])^\vee \to \mathfrak{g}(K)^\vee[\omega_n] \to 0,$$

the quantity

$$\mathrm{corank}_W\, H^1(K^S/K,\hat{J}_n^{ord}[p^\infty]) - p^{n-1}\cdot \mathrm{corank}_\Lambda\, H^1(K^S/K,\mathfrak{g})$$

is bounded independent of n. Since the same assertion holds for H^2, we get the assertion about the Λ-corank. $\square$

5.2.2 Application of the Poitou-Tate duality

In this section, we prove a theorem relating Λ-coranks of $Ш^1_K(\mathfrak{g})$ and $Ш^2_K(\mathfrak{g}')$. Main tool is the Poitou-Tate duality between $Ш^1$ and $Ш^2$. We state a technical lemma without proof.

Lemma 5.2.7. *(1) Let A be a cofinitely generated W-module. Then $A[p^m]$ and $\frac{A}{p^m A}$ are finite modules. For all sufficiently large m, $|A[p^m]| = p^{m\cdot \mathrm{rank}_{\mathbb{Z}_p} W \cdot \mathrm{corank}_W A + c}$ for some constant c independent of m and $|\frac{A}{p^m A}|$ is a constant independent of m.*

(2) Let X be a cofinitely generated Λ-module. Then $X[\omega_n]$ and $\frac{X}{\omega_n X}$ are cofinitely generated W-modules. For all sufficiently large n, $\mathrm{corank}_W X[\omega_n] = p^{n\cdot \mathrm{rank}_\Lambda X} + c$ for some constant c independent of n, and $\mathrm{corank}_W \frac{X}{\omega_n X}$ is a constant independent of n.

Note first that by the local vanishing of H^2 of the Barsotti-Tate groups (Lemma 5.1.1-(2)), we have

$$Ш^2_K(\hat{J}^{ord}_n[p^\infty]) = H^2(K^S/K, \hat{J}^{ord}_n[p^\infty]) \quad \text{and} \quad Ш^2_K(\mathfrak{g}) = H^2(K^S/K, \mathfrak{g}).$$

Proposition 5.2.8. *(1)* $\mathrm{rank}_W(Ш^1_K(\hat{J}^{ord}_n[p^\infty])^\vee) = \mathrm{rank}_W(Ш^2_K(\hat{J'}^{ord}_n[p^\infty])^\vee)$*. In particular,* $Ш^1_K(\hat{J}^{ord}_n[p^\infty])$ *is finite if and only if* $Ш^2_K(\hat{J'}^{ord}_n[p^\infty]) = 0$*.*

(2) $\mathrm{rank}_\Lambda(Ш^1(\mathfrak{g})^\vee) = \mathrm{rank}_\Lambda(Ш^2(\mathfrak{g}')^\vee)$*. In particular,* $Ш^1(\mathfrak{g})^\vee$ *is Λ-torsion if and only if* $Ш^2(\mathfrak{g}') = 0$*.*

The second parts of the assertions (1) and (2) follow from the cofreeness of H^2 (Lemma 5.2.3-(2) and Corollary 5.2.4-(2)).

Proof. (1) We let

$$A_{m,n} := \mathrm{Ker}\left(\frac{\hat{J}^{ord}_n[p^\infty](K)}{p^m \hat{J}^{ord}_n[p^\infty](K)} \to \prod_{v\in S} \frac{\hat{J}^{ord}_n[p^\infty](K_v)}{p^m \hat{J}^{ord}_n[p^\infty](K_v)}\right)$$
$$B_{m,n} := \mathrm{Coker}\left(\frac{\hat{J}^{ord}_n[p^\infty](K)}{p^m \hat{J}^{ord}_n[p^\infty](K)} \to \prod_{v\in S} \frac{\hat{J}^{ord}_n[p^\infty](K_v)}{p^m \hat{J}^{ord}_n[p^\infty](K_v)}\right)$$

and

$$C_{m,n} := \mathrm{Ker}\left(\frac{H^1(K^S/K, \hat{J'}^{ord}_n[p^\infty])}{p^m H^1(K^S/K, \hat{J'}^{ord}_n[p^\infty])} \to \prod_{v\in S} \frac{H^1(K_v, \hat{J'}^{ord}_n[p^\infty])}{p^m H^1(K_v, \hat{J'}^{ord}_n[p^\infty])}\right)$$
$$D_{m,n} := \mathrm{Coker}\left(\frac{H^1(K^S/K, \hat{J'}^{ord}_n[p^\infty])}{p^m H^1(K^S/K, \hat{J'}^{ord}_n[p^\infty])} \to \prod_{v\in S} \frac{H^1(K_v, \hat{J'}^{ord}_n[p^\infty])}{p^m H^1(K_v, \hat{J'}^{ord}_n[p^\infty])}\right).$$

For fixed n and sufficiently large m, the sizes of $A_{m,n}, B_{m,n}, C_{m,n}, D_{m,n}$ are constants by Lemma 5.2.7-(1).

For $i = 0, 1$, we have the following commutative diagram:

$$\begin{array}{ccccc}
\frac{H^i(K^S/K, \hat{J}^{ord}_n[p^\infty])}{p^m H^i(K^S/K, \hat{J}^{ord}_n[p^\infty])} & \hookrightarrow & H^{i+1}(K^S/K, \hat{J}^{ord}_n[p^m]) & \twoheadrightarrow & H^{i+1}(K^S/K, \hat{J}^{ord}_n[p^\infty])[p^m] \\
\downarrow Res & & \downarrow Res & & \downarrow Res \\
\prod_{v\in S} \frac{H^i(K_v, \hat{J}^{ord}_n[p^\infty])}{p^m H^i(K_v, \hat{J}^{ord}_n[p^\infty])} & \hookrightarrow & \prod_{v\in S} H^{i+1}(K_v, \hat{J}^{ord}_n[p^m]) & \twoheadrightarrow & \prod_{v\in S} H^{i+1}(K_v, \hat{J}^{ord}_n[p^\infty])[p^m]
\end{array}$$

By the snake lemma, we have the following two exact sequences:

$$0 \to A_{m,n} \to \text{Ш}^1_K(\hat{J}^{ord}_n[p^m]) \to \text{Ш}^1_K(\hat{J}^{ord}_n[p^\infty])[p^m] \to B_{m,n}$$
$$0 \to C_{m,n} \to \text{Ш}^2_K(\hat{J'}^{ord}_n[p^m]) \to \text{Ш}^2_K(\hat{J'}^{ord}_n[p^\infty])[p^m] \to D_{m,n}$$

By Poitou-Tate duality (Proposition 4.4.1), we know that $\text{Ш}^1_K(\hat{J}^{ord}_n[p^m])$ and $\text{Ш}^2_K(\hat{J'}^{ord}_n[p^m])$ have same size. Since sizes of the $A_{m,n}, B_{m,n}, C_{m,n}, D_{m,n}$ are independent of m for sufficiently large m, Lemma 5.2.7-(1) shows $\mathrm{rank}_W(\text{Ш}^1_K(\hat{J}^{ord}_n[p^\infty])^\vee) = \mathrm{rank}_W(\text{Ш}^2_K(\hat{J'}^{ord}_n[p^\infty])^\vee)$.

(2) We let

$$E_n := \mathrm{Ker}\left(\frac{\mathfrak{g}(K)}{\omega_n \mathfrak{g}(K)} \to \prod_{v\in S} \frac{\mathfrak{g}(K_v)}{\omega_n \mathfrak{g}(K_v)}\right)$$
$$F_n := \mathrm{Coker}\left(\frac{\mathfrak{g}(K)}{\omega_n \mathfrak{g}(K)} \to \prod_{v\in S} \frac{\mathfrak{g}(K_v)}{\omega_n \mathfrak{g}(K_v)}\right)$$

and

$$G_n := \mathrm{Ker}\left(\frac{H^1(K^S/K,\mathfrak{g}')}{\omega_n H^1(K^S/K,\mathfrak{g}')} \to \prod_{v\in S}\frac{H^1(K_v,\mathfrak{g}')}{\omega_n H^1(K_v,\mathfrak{g}')}\right)$$
$$H_n := \mathrm{Coker}\left(\frac{H^1(K^S/K,\mathfrak{g}')}{\omega_n H^1(K^S/K,\mathfrak{g}')} \to \prod_{v\in S}\frac{H^1(K_v,\mathfrak{g}')}{\omega_n H^1(K_v,\mathfrak{g}')}\right).$$

For sufficiently large n, W-coranks of the E_n, F_n, G_n, H_n are constants by Lemma 5.2.7-(2).

By the same token as the proof of (1), we have the following two exact sequences:

$$0 \to E_n \to Ш^1_K(\hat{J}^{ord}_n[p^\infty]) \to Ш^1_K(\mathfrak{g})[\omega_n] \to F_n$$
$$0 \to G_n \to Ш^2_K(\hat{J'}^{ord}_n[p^\infty]) \to Ш^2_K(\mathfrak{g}')[\omega_n] \to H_n$$

By (1), we know that $Ш^1_K(\hat{J}^{ord}_n[p^\infty])$ and $Ш^2_K(\hat{J'}^{ord}_n[p^\infty])$ have same W-corank. Since W-coranks of E_n, F_n, G_n, H_n are independent of n for sufficiently large n, Lemma 5.2.7-(2) shows that

$$\mathrm{rank}_\Lambda(Ш^1(\mathfrak{g})^\vee) = \mathrm{rank}_\Lambda(Ш^2(\mathfrak{g}')^\vee).$$

□

CHAPTER 6

Structure of global Λ-adic cohomology groups

We keep Notation 3.3.6, Convention 3.3.8 and Convention 5.2.1 in this chapter.

6.1 Λ-adic Selmer groups

In this section, we study the Λ-adic Selmer groups which are defined as the kernels of certain global-to-local restriction maps. Following [GV00], we show that under mild assumptions, the "Selmer-defining map" is surjective (Corollary 6.1.8). In Subsection 6.1.3, using the twisted Flach pairing, we study the algebraic functional equation of Selmer groups between (α, δ, ξ)-tower and (δ, α, ξ')-tower which is one of the main results of this thesis (Theorem 6.1.9).

6.1.1 Basic properties

Definition 6.1.1. We define the following Selmer groups:

(1) $\mathrm{Sel}_{K,p^m}(\hat{J}_n^{ord}) := \mathrm{Ker}\left(H^1(K^S/K, \hat{J}_n^{ord}[p^m]) \to \prod_{v \in S} \frac{H^1(K_v, \hat{J}_n^{ord}[p^m])}{\hat{J}_n^{ord}(K_v)/p^m \hat{J}_n^{ord}(K_v)} \right).$

(2) $\mathrm{Sel}_{K}(\hat{J}_n^{ord}) := \mathrm{Ker}\left(H^1(K^S/K, \hat{J}_n^{ord}[p^\infty]) \to \prod_{v \in S} \frac{H^1(K_v, \hat{J}_n^{ord}[p^\infty])}{\hat{J}_n^{ord}(K_v) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p} \right).$

(3) $\mathrm{Sel}_{K}(J_\infty^{ord}) := \mathrm{Ker}\left(H^1(K^S/K, \mathfrak{g}) \to \prod_{v \in S} \frac{H^1(K_v, \mathfrak{g})}{J_\infty^{ord}(K_v) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p} \right) = \varinjlim_n \mathrm{Sel}_K(\hat{J}_n^{ord}).$

Notation 6.1.2. *We let*

$$s_n : \mathrm{Sel}_K(\hat{J}_n^{ord}) \to \mathrm{Sel}_K(J_\infty^{ord})[\omega_n]$$

be the natural restriction map. We also define

$$s'_n : \mathrm{Sel}_K(\hat{J'}^{ord}_n) \to \mathrm{Sel}_K(J'^{ord}_\infty)[\omega_n].$$

By Hida's control theorem (Theorem 1.2.1), $\mathrm{Coker}(s_n)$ *and* $\mathrm{Coker}(s'_n)$ *are finite for all* $n \geq 2$*.*

Remark 6.1.3. (1) $\mathrm{Sel}_{K,p^m}(\hat{J}^{ord}_n)$ is finite for all m, n.

(2) We have an exact sequence

$$0 \to \frac{\hat{J}^{ord}_n[p^\infty](K)}{p^m \hat{J}^{ord}_n[p^\infty](K)} \to \mathrm{Sel}_{K,p^m}(\hat{J}^{ord}_n) \to \mathrm{Sel}_K(\hat{J}^{ord}_n)[p^m] \to 0$$

for all m, n. In particular, $\frac{|\mathrm{Sel}_{K,p^m}(\hat{J}^{ord}_n)|}{p^{m\cdot \mathrm{corank}_W \mathrm{Sel}_K(\hat{J}^{ord}_n)}}$ becomes stable as m goes to infinity.

(3) By definition of the Selmer groups, we have an injection

$$\mathrm{Ker}(s_n) \hookrightarrow \mathrm{Ker}\left(H^1(K^S/K, \hat{J}^{ord}_n[p^\infty]) \to H^1(K^S/K, \mathfrak{g})[\omega_n]\right) \simeq \frac{\mathfrak{g}(K)}{\omega_n \mathfrak{g}(K)}.$$

Hence $\mathrm{Ker}(s_n)$ is finite and bounded independent of n by Lemma 5.2.2. Moreover, we have

$$\varinjlim_n \mathrm{Ker}(s_n) = \varinjlim_n \mathrm{Coker}(s_n) = 0.$$

We also have an injection

$$\varprojlim_n \mathrm{Ker}(s_n) \hookrightarrow N^\vee$$

by Lemma 5.2.2, where N is the maximal finite Λ-submodule of $\mathfrak{g}(K)^\vee$.

As a consequence of the last remark, we have the following formula relating the corank of p-adic Selmer groups of (α, δ, ξ)-tower and (δ, α, ξ')-tower.

Proposition 6.1.4. *(1) (Greenberg-Wiles formula) The value* $\frac{|\mathrm{Sel}_{K,p^m}(\hat{J}^{ord}_n)|}{|\mathrm{Sel}_{K,p^m}(\hat{J'}^{ord}_n)|}$ *becomes stationary as* m *goes to infinity.*

(2) $\mathrm{corank}_W \mathrm{Sel}_K(\hat{J}^{ord}_n) = \mathrm{corank}_W \mathrm{Sel}_K(\hat{J'}^{ord}_n)$ *for all* (α, δ, ξ) *and* n*. Hence we have*

$$\mathrm{corank}_W \left(\mathrm{Sel}_K(J^{ord}_\infty)[\omega_n]\right) = \mathrm{corank}_W \left(\mathrm{Sel}_K(J'^{ord}_\infty)[\omega_n]\right).$$

Proof. (1) follows from the Greenberg-Wiles formula [DDT95, Theorem 2.19] combined with Proposition 4.3.1-(2). The first statement of (2) is a direct consequence of (1) and Remark 6.1.3-(2). The second statement of (2) follows from Hida's control theorem (Theorem 1.2.1). □

6.1.2 Surjectivity of global-to-local restriction map

Recall that $\mathrm{Sel}_K(J_\infty^{ord})$ is defined as a kernel of global-to-local restriction map $H^1(K^S/K,\mathfrak{g}) \to \prod_{v\in S} \dfrac{H^1(K_v,\mathfrak{g})}{J_\infty^{ord}(K_v)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p}$. We let $C_\infty(K)$ be the **cokernel of this restriction map.** In this subsection, we show that this group is "small" under mild assumptions. (Corollary 6.1.8).

We first construct various exact sequences induced from the Poitou-Tate sequence. For a finitely or a cofinitely generated $\mathbb{Z}_p$-module M, we let $T_pM := \varprojlim_n M[p^n] \simeq \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p, M)$. Note that for M with finite cardinality, we have $T_pM = 0$ and $\mathrm{Ext}^1_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p, M) \simeq M$ where the isomorphism is functorial in M. Hence the exact sequence $0 \to Q \to R \to U \to V \to 0$ of cofinitely generated $\mathbb{Z}_p$-modules with finite Q induces another exact sequence $0 \to T_pR \to T_pU \to T_pV$.

Proposition 6.1.5. *(1) We have the following four exact sequences:*

$$0 \to \mathrm{Sel}_K(J_\infty^{ord}) \to H^1(K^S/K,\mathfrak{g}) \to \prod_{v\in S}\frac{H^1(K_v,\mathfrak{g})}{J_\infty^{ord}(K_v)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p} \to C_\infty(K) \to 0 \tag{W}$$

$$0 \to C_\infty(K) \to \left(\varprojlim_n \varprojlim_m \mathrm{Sel}_{K,p^m}(\hat{J'}^{ord}_n)\right)^\vee \to H^2(K^S/K,\mathfrak{g}) \to 0 \tag{X}$$

$$0 \to \mathfrak{F}\left(\mathfrak{g}'(K)^\vee\right) \to \varprojlim_n \varprojlim_m \mathrm{Sel}_{K,p^m}(\hat{J'}^{ord}_n) \to \varprojlim_n T_p\mathrm{Sel}_K(\hat{J'}^{ord}_n) \to 0 \tag{Y}$$

$$0 \to \varprojlim_n T_p\mathrm{Sel}_K(\hat{J'}^{ord}_n) \to \mathrm{Hom}_\Lambda(\mathrm{Sel}_K(J'^{ord}_\infty)^\vee,\Lambda) \to \varprojlim_n T_p\mathrm{Coker}(s'_n) \tag{Z}$$

(2) For all places v of K dividing p, let

$$\epsilon_v := \mathrm{corank}_\Lambda(J_\infty^{ord}(K_v)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p) - \frac{1}{2}[K_v:\mathbb{Q}_p]\cdot \mathrm{corank}_\Lambda\,\mathfrak{g}(\overline{K_v}).$$

Note that ϵ_v is non-negative by Proposition 5.1.12-(1). We have the following identity:

$$\mathrm{corank}_\Lambda\left(\mathrm{Sel}_K(J_\infty^{ord})\right) = \mathrm{corank}_\Lambda\left(H^2(K^S/K,\mathfrak{g})\right) + \mathrm{corank}_\Lambda\left(C_\infty(K)\right) + \sum_{v\mid p}\epsilon_v.$$

Proof. By [CS00, page 11], we have an exact sequence

$$0 \to \mathrm{Sel}_K(\hat{J}_n^{ord}) \to H^1(K^S/K,\hat{J}_n^{ord}[p^\infty]) \to \prod_{v\in S}\frac{H^1(K_v,\hat{J}_n^{ord}[p^\infty])}{\hat{J}_n^{ord}(K_v)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p}$$
$$\to \left(\varprojlim_m \mathrm{Sel}_{K,p^m}(\hat{J'}^{ord}_n)\right)^\vee \to H^2(K^S/K,\hat{J}_n^{ord}[p^\infty]) \to 0.$$

Taking the direct limit with respect to n proves W and X.

On the other hand, by [CS00, Lemma 1.8], we have an exact sequence

$$0 \to \hat{J'}^{ord}_n[p^\infty](K) \to \varprojlim_m \mathrm{Sel}_{K,p^m}(\hat{J'}^{ord}_n) \to T_p\mathrm{Sel}_K(\hat{J'}^{ord}_n) \to 0.$$

Taking direct limit with respect to n proves Y.

Since $\mathrm{Ker}(s'_n)$ is finite, the exact sequence

$$0 \to \mathrm{Ker}(s'_n) \to \mathrm{Sel}_K(\hat{J'}^{ord}_n) \to \mathrm{Sel}_K(J'^{ord}_\infty)[\omega_n] \to \mathrm{Coker}(s'_n) \to 0$$

induces another exact sequence

$$0 \to T_p\mathrm{Sel}_K(\hat{J'}^{ord}_n) \to T_p(\mathrm{Sel}_K(J'^{ord}_\infty)[\omega_n]) \to T_p\mathrm{Coker}(s'_n)$$

by the remark mentioned before this proposition. Taking projective limit with respect to n combined with Lemma 7.1.2-(2) in the appendix proves Z.

Lastly, by Proposition 7.1.6-(2) and Lemma 5.1.2-(2) we have:

$$\mathrm{corank}_\Lambda\left(H^1(K^S/K,\mathfrak{g})\right) = \frac{1}{2}[K:\mathbb{Q}]\cdot \mathrm{corank}_\Lambda\,\mathfrak{g}(\overline{K}) + \mathrm{corank}_\Lambda\left(H^2(K^S/K,\mathfrak{g})\right)$$
$$\mathrm{corank}_\Lambda\left(H^1(K_v,\mathfrak{g})\right) = 0 \quad (v \nmid p).$$

Hence (2) follows from the calculation of Λ-coranks of the four terms in the sequence W. $\square$

Corollary 6.1.6. *(1) $\varprojlim_n T_p\mathrm{Sel}_K(\hat{J'}^{ord}_n)$ is a torsion-free Λ-module. Hence we have a natural isomorphism*

$$\mathfrak{F}\left(\mathfrak{g}'(K)^\vee\right) \simeq \left(\varprojlim_n \varprojlim_m \mathrm{Sel}_{K,p^m}(\hat{J'}^{ord}_n)\right)_{\Lambda-\mathrm{tor}}$$

and these groups vanish if $\mathfrak{g}'(K)$ is finite.

(2) $\varprojlim_n T_p\mathrm{Sel}_K(\hat{J'}^{ord}_n) = 0$ if and only if $\varprojlim_n \varprojlim_m \mathrm{Sel}_{K,p^m}(\hat{J'}^{ord}_n)$ is a torsion Λ-module. If this is the case, $H^2(K^S/K,\mathfrak{g}) = 0$ and we have isomorphisms

$$C_\infty(K)^\vee \simeq \varprojlim_n \varprojlim_m \mathrm{Sel}_{K,p^m}(\hat{J'}^{ord}_n) \simeq \mathfrak{F}\left(\mathfrak{g}'(K)^\vee\right)$$

Proof. We prove (1) first. Since $\mathrm{Hom}_\Lambda(\mathrm{Sel}_K(J'^{ord}_\infty)^\vee, \Lambda)$ is a free Λ-module, $\varprojlim_n T_p\mathrm{Sel}_K(\hat{J}'^{ord}_n)$ is a torsion-free Λ-module by the sequence Z. The second and the third assertion of (1) follows from the sequence Y and Lemma 5.2.3-(1).

The first statement of (2) follows directly from (1) and the fact that $\mathfrak{F}(\mathfrak{g}'(K)^\vee)$ is a torsion Λ-module. By the sequence X, we have an injection

$$H^2(K^S/K, \mathfrak{g})^\vee \hookrightarrow \varprojlim_n \varprojlim_m \mathrm{Sel}_{K,p^m}(\hat{J}'^{ord}_n)$$

where $H^2(K^S/K, \mathfrak{g})^\vee$ is a Λ-free by the Corollary 5.2.4-(2).

Hence if $\varprojlim_n \varprojlim_m \mathrm{Sel}_{K,p^m}(\hat{J}'^{ord}_n)$ is a torsion Λ-module, then $H^2(K^S/K, \mathfrak{g}) = 0$. Hence from the sequence X, we get an isomorphism

$$C_\infty(K)^\vee \simeq \varprojlim_n \varprojlim_m \mathrm{Sel}_{K,p^m}(\hat{J}'^{ord}_n).$$

□

Proposition 6.1.7. *If $\mathrm{Sel}_K(J^{ord}_\infty)$ is a Λ-cotorsion module, then we have:*

(1) $Ш^1_K(\mathfrak{g})$ is a cotorsion Λ-module.

(2) $H^2(K^S/K, \mathfrak{g}) = 0$. Hence $H^1(K^S/K, \mathfrak{g})^\vee$ has no non-trivial finite Λ-submodules by Corollary 5.2.5.

(3) $C_\infty(K)^\vee$ is a Λ-torsion module isomorphic to $\mathfrak{F}(\mathfrak{g}'(K)^\vee)$.

(4) For all places v dividing p, we have

$$\mathrm{corank}_\Lambda\left(J^{ord}_\infty(K_v) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p\right) = \frac{1}{2}[K_v : \mathbb{Q}_p] \cdot \mathrm{corank}_\Lambda\, \mathfrak{g}(\overline{K})$$

Proof. The assertion (1) is obvious since $Ш^1_K(\mathfrak{g})$ is a Λ-submodule of $\mathrm{Sel}_K(J^{ord}_\infty)$. By the corank computation in Proposition 6.1.5-(2), we have

$$\mathrm{corank}_\Lambda\left(H^2(K^S/K, \mathfrak{g})\right) = \mathrm{corank}_\Lambda\left(C_\infty(K)\right) = \epsilon_v = 0$$

for all v dividing p. Hence we have (2) since $H^2(K^S/K, \mathfrak{g})$ is a cofree Λ-module.

From the sequence X in Proposition 6.1.5-(1) and the above corank identity, we know that $\varprojlim_n \varprojlim_m \mathrm{Sel}_{K,p^m}(\hat{J}'^{ord}_n)$ is a torsion Λ-module. Now (3) follows from an exact sequence X combined with Corollary 6.1.6-(2). □

We have the following corollary about the surjectivity of the "Selmer-defining map", which is an analogue of [GV00, Proposition 2.1] and [GV00, Proposition 2.5].

Corollary 6.1.8. *Suppose that* $\mathrm{Sel}_K(J_\infty^{ord})$ *is a* Λ*-cotorsion.*

(1) If $\mathfrak{g}'(K)$ *is finite, then we have* $C_\infty(K) = 0$.

(2) If we furthermore assume that $\mathfrak{g}'(K_v)$ *is finite for all* $v \in S$ *and* $\mathfrak{g}'(K_v) = 0$ *for all places* $v|p$*, then* $\mathrm{Sel}_K(J_\infty^{ord})^\vee$ *has no non-trivial pseudo-null* Λ*-submodules.*

Proof. By the Proposition 6.1.7-(3), we have $C_\infty(K) \simeq \mathfrak{F}\left(\mathfrak{g}'(K)^\vee\right) \simeq 0$ since $\mathfrak{g}'(K)$ is finite.

For the second part, by Corollary 5.1.8-(1), Proposition 5.1.12-(5) and Proposition 6.1.7-(2), we have :

- $H^1(K_v, \mathfrak{g}) = 0$ for all v in S not dividing p.
- $\frac{H^1(K_v,\mathfrak{g})}{J_\infty^{ord}(K_v)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p}$ is a cofree Λ-module for all v dividing p.
- $H^1(K^S/K, \mathfrak{g})^\vee$ has no non-trivial finite Λ-submodules.

Since $C_\infty(K) = 0$ by the first part, we have an exact sequence

$$0 \to \left(\prod_{v|p} \frac{H^1(K_v, \mathfrak{g})}{J_\infty^{ord}(K_v) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p}\right)^\vee \to H^1(K^S/K, \mathfrak{g})^\vee \to \mathrm{Sel}_K(J_\infty^{ord})^\vee \to 0,$$

where the first term is a Λ-free as we mentioned above. Now [GV00, Lemma 2.6] shows the desired assertion. ☐

6.1.3 Algebraic functional equation of Λ-adic Selmer groups

Now we compare $E\left(\mathrm{Sel}_K(J_\infty^{ord})^\vee\right)$ and $E\left(\mathrm{Sel}_K(J_\infty'^{ord})^\vee\right)$.

Theorem 6.1.9. *We have an isomorphism*

$$E\left(\mathrm{Sel}_K(J_\infty^{ord})^\vee\right) \simeq E\left(\mathrm{Sel}_K(J_\infty'^{ord})^\vee\right)^\iota$$

of Λ*-modules.*

Proof. By Lemma 2.4.2, it is sufficient to show the following two statements:

- $\mathrm{corank}_W\left(\mathrm{Sel}_K(J_\infty^{ord})[\omega_n]\right) = \mathrm{corank}_W\left(\mathrm{Sel}_K(J_\infty'^{ord})[\omega_n]\right)$ for all n.
- There is a Λ-linear map $\mathfrak{G}\left(\mathrm{Sel}_K(J_\infty'^{ord})^\vee\right) \to \mathfrak{F}\left(\mathrm{Sel}_K(J_\infty^{ord})^\vee\right)$ with finite kernel.

The first statement is Proposition 6.1.4-(2). For the second statement, consider an exact sequence

$$0 \to \mathrm{Ker}(s_n) \to \mathrm{Sel}_K(\hat{J}_n^{ord}) \to \mathrm{Sel}_K(J_\infty^{ord})[\omega_n] \to \mathrm{Coker}(s_n) \to 0.$$

We have

$$\mathrm{Ker}(s_n) \to \mathrm{Sel}_K(\hat{J}_n^{ord})_{/div} \to \left(\mathrm{Sel}_K(J_\infty^{ord})[\omega_n]\right)_{/div} \to \mathrm{Coker}(s_n) \to 0.$$

By taking the direct limit and the Pontryagin dual, we get

$$\varprojlim_n \left(\mathrm{Sel}_K(\hat{J}_n^{ord})_{/div}\right)^\vee \simeq \mathfrak{G}\left(\mathrm{Sel}_K(J_\infty^{ord})^\vee\right). \tag{6.1}$$

Now we look at (δ, α, ξ')-tower. By the same token, we get

$$\mathrm{Ker}(s'_n) \to \mathrm{Sel}_K(\hat{J'}_n^{ord})_{/div} \to \left(\mathrm{Sel}_K(J_\infty'^{ord})[\omega_n]\right)_{/div} \to \mathrm{Coker}(s'_n) \to 0.$$

Note that all the terms in this sequence are finite. By taking projective limit, we get the following exact sequence:

$$\varprojlim_n \mathrm{Ker}(s'_n) \to \varprojlim_n \mathrm{Sel}_K(\hat{J'}_n^{ord})_{/div} \to \varprojlim_n \left(\mathrm{Sel}_K(J_\infty'^{ord})[\omega_n]\right)_{/div}. \tag{6.2}$$

We now analyze the three terms in the above sequence (6.2).

- $\varprojlim_n \mathrm{Ker}(s'_n)$ is finite by Remark 6.1.3-(3).
- By the perfectness of twisted Flach pairing (Proposition 4.5.2-(4)), the middle term in (6.2) is isomorphic to $\varprojlim_n \left(\mathrm{Sel}_K(\hat{J}_n^{ord})_{/div}\right)^\vee$, and this group is, by the (6.1) above, isomorphic to $\mathfrak{G}\left(\mathrm{Sel}_K(J_\infty^{ord})^\vee\right)$ as Λ-modules.

- The last term in (6.2) is $\mathfrak{F}\left(\mathrm{Sel}_K(J'^{ord}_\infty)^\vee\right)$ by the definition of the functor $\mathfrak{F}$.

Therefore, there is a Λ-linear map $\mathfrak{G}\left(\mathrm{Sel}_K(J^{ord}_\infty)^\vee\right) \to \mathfrak{F}\left(\mathrm{Sel}_K(J'^{ord}_\infty)^\vee\right)$ with the finite kernel, which shows the desired assertion. □

Remark 6.1.10. If we consider the Tate-Shafarevich groups instead of the Selmer groups, under the analogous assumptions (control of the Tate-Shafarevich groups), we get a pseudo-isomorphism between

$$\mathfrak{G}\left(\text{Ш}^1_K(J^{ord}_\infty)^\vee\right) \quad \text{and} \quad \mathfrak{G}\left(\text{Ш}^1_K(J'^{ord}_\infty)^\vee\right)^\iota .$$

The proof uses the (twisted) Cassels-Tate paiting, instead of Flach's one. The reason why we can only compare the values of $\mathfrak{G}$ for Ш^1 is that we do not have an analogue of the Greenberg-Wiles formula for the Ш^1.

6.2 Λ-adic Tate-Shafarevich groups

Define a Λ-adic Tate-Shafarevich group by $\text{Ш}^1_K(J^{ord}_\infty) := \varinjlim_n \text{Ш}^1_K(\hat{J}^{ord}_n)$ which fits into a natural exact sequence

$$0 \to J^{ord}_\infty(K) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}_K(J^{ord}_\infty) \to \text{Ш}^1_K(J^{ord}_\infty) \to 0.$$

We also have a natural map $\text{Ш}^1_K(\hat{J}^{ord}_n) \to \text{Ш}^1_K(J^{ord}_\infty)[\omega_n]$. Note that $\text{Ш}^1_K(J^{ord}_\infty)$ is a cofinitely generated Λ-module.

6.2.1 Cotorsionness of Λ-adic Ш^1

Next we show that under the Hida's control theorem of the Selmer groups (Theorem 1.2.1) and the finiteness of $\text{Ш}^1_K(\hat{J}^{ord}_n)$, $\text{Ш}^1_K(J^{ord}_\infty)^\vee$ is a finitely generated torsion Λ-module. This can be regarded as a Λ-adic analogue of the Tate-Shafarevich conjecture.

Theorem 6.2.1. *Suppose that $\text{Ш}^1_K(\hat{J}^{ord}_n)$ is finite for all n. Then the functor $\mathfrak{G}$ induces an isomorphism*

$$\text{Ш}^1_K(J^{ord}_\infty)^\vee \simeq \mathfrak{G}\left(\mathrm{Sel}_K(J^{ord}_\infty)^\vee\right)$$

of Λ*-modules. In particular,* $Ш^1_K(J^{ord}_\infty)^\vee$ *is a finitely generated torsion* Λ*-module.*

Proof. Proof is similar with that of Theorem 2.2.4. $\square$

Corollary 6.2.2. *Suppose that* $Ш^1_K(\hat{J}^{ord}_n)$ *and* $Ш^1_K(\hat{J'}^{ord}_n)$ *are finite for all* n*. Then we have* Λ*-linear isomorphisms*

$$E\left(Ш^1_K(J^{ord}_\infty)^\vee\right) \simeq E\left(Ш^1_K(J'^{ord}_\infty)^\vee\right)^\iota$$

$$E\left((J^{ord}_\infty(K) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)^\vee\right) \simeq E\left((J'^{ord}_\infty(K) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)^\vee\right)^\iota$$

Proof. This follows from Theorem 6.1.9 and Theorem 6.2.1. $\square$

6.2.2 Estimates on the size of $Ш^1$

Under the boundedness of $\mathrm{Coker}(s_n)$, we can compute an estimate of the size of $Ш^1_K(\hat{J}^{ord}_n)$.

Theorem 6.2.3. *Suppose that* $\mathrm{Coker}(s_n)$ *is (finite and) bounded independent of* n*, and also suppose that* $Ш^1_K(\hat{J}^{ord}_n)$ *is finite for all* n*. Then there exists an integer* ν *such that*

$$\left|Ш^1_K(\hat{J}^{ord}_n)\right| = p^{e_n} \quad (n >> 0)$$

where

$$e_n = p^n \mu\left(Ш^1_K(\hat{J}^{ord}_\infty)^\vee\right) + n\lambda\left(Ш^1_K(\hat{J}^{ord}_\infty)^\vee\right) + \nu.$$

Proof. Proof is similar with that of Theorem 2.3.1. $\square$

Corollary 6.2.4. *Suppose that* $\mathrm{Coker}(s_n), \mathrm{Coker}(s'_n)$ *are (finite and) bounded independent of* n*,. If the groups* $Ш^1_K(\hat{J}^{ord}_n), Ш^1_K(\hat{J'}^{ord}_n)$ *are finite for all* n*, then the ratios*

$$\frac{\left|Ш^1_K(\hat{J}^{ord}_n)\right|}{\left|Ш^1_K(\hat{J'}^{ord}_n)\right|} \quad \text{and} \quad \frac{\left|Ш^1_K(\hat{J'}^{ord}_n)\right|}{\left|Ш^1_K(\hat{J}^{ord}_n)\right|}$$

are bounded independent of n*.*

Proof. This follows from Theorem 6.1.9, Theorem 6.2.1, and Theorem 6.2.3. $\square$

CHAPTER 7

Functors $\mathfrak{F}$ and $\mathfrak{G}$

7.1 The functor $\mathfrak{F}$

We first recall our convention on Pontryagin dual. For a locally compact Hausdorff continuous Λ-module M, we define $M^\vee := \mathrm{Hom}_{cts}(M, \mathbb{Q}_p/\mathbb{Z}_p)$ which is also a locally compact Hausdorff. $M^\vee$ becomes a continuous Λ-module via action defined by $(f\cdot\phi)(m) := \phi(\iota(f)\cdot m)$ where $f \in \Lambda$, $m \in M$, $\phi \in M^\vee$.

If M, N are two locally compact Hausdorff continuous Λ-modules with a perfect pairing $P : M \times N \to \mathbb{Q}_p/\mathbb{Z}_p$ satisfying $P(f \cdot x, y) = P(x, \iota(f) \cdot y)$, then P induces Λ-module isomorphisms $M \simeq N^\vee$ and $N \simeq M^\vee$.

Definition 7.1.1. For any finitely generated Λ-module X, define $\mathfrak{F}(X) = \left(\varinjlim_n \frac{X}{\omega_n X}[p^\infty]\right)^\vee$. Here direct limit is taken with respect to norm maps $\frac{X}{\omega_n X} \xrightarrow{\times \frac{\omega_{n+1}}{\omega_n}} \frac{X}{\omega_{n+1}X}$. $\mathfrak{F}$ is contravariant and preserves finite direct sums.

Our goal is examining Λ-module structure of $\mathfrak{F}(X)$ for a finitely generated Λ-module X (Proposition 7.1.6). We will use the following proposition crucially.

Lemma 7.1.2. *(1) Let M be a finitely generated Λ-module, and let $\{\pi_n\}$ be a sequence of non-zero elements of Λ such that $\pi_0 \in m, \pi_{n+1} \in \pi_n m$, $\frac{M}{\pi_n M}$ is finite for all n where m is the maximal ideal of Λ. Then we have an isomorphism*

$$\left(\varinjlim_n \frac{M}{\pi_n M}\right)^\vee \simeq \mathrm{Ext}^1_\Lambda(M, \Lambda)^\iota$$

as Λ-modules.

(2) For a finitely generated Λ-module X, we have an isomorphism

$$\varprojlim_n T_p(X^\vee[\omega_n]) \simeq \mathrm{Hom}_\Lambda(X,\Lambda)^\iota$$

.

Proof. We only need to prove (2) since (1) is [NSW00, Proposition 5.5.6]. By (1), we have an isomorphism $T_p(X^\vee[\omega_n]) \simeq \mathrm{Ext}^1_\Lambda(\frac{X}{\omega_n X},\Lambda)^\iota$ and this last group is isomorphic to

$$\mathrm{Hom}_\Lambda(\frac{X}{\omega_n X},\frac{\Lambda}{\omega_n\Lambda})^\iota \simeq \mathrm{Hom}_\Lambda(X,\frac{\Lambda}{\omega_n\Lambda})^\iota.$$

Hence $\varprojlim_n T_p(X^\vee[\omega_n]) \simeq \varprojlim_n \mathrm{Hom}_\Lambda(X,\frac{\Lambda}{\omega_n\Lambda})^\iota \simeq \mathrm{Hom}_\Lambda(X,\Lambda)^\iota$. □

Lemma 7.1.3. *(1) If K is finite, then $\mathfrak{F}(K)=0$.*

(2) $\mathfrak{F}(\Lambda)=0$.

(3) If g is a prime element of Λ coprime to ω_n for all $n\geq 0$, then for all $e\geq 1$, we have

$$\mathfrak{F}(\frac{\Lambda}{g^e}) = \frac{\Lambda}{\iota(g)^e}.$$

(4)

$$\mathfrak{F}(\frac{\Lambda}{\omega^e_{m+1,m}}) = \begin{cases} \frac{\Lambda}{\iota(\omega_{m+1,m})^{e-1}} & e\geq 2, \\ 0 & e=1. \end{cases}$$

Proof. For (2), $\frac{\Lambda}{\omega_n\Lambda}$ is $\mathbb{Z}_p$-torsion-free so $\mathfrak{F}(\Lambda)=0$. For (3), note that $\frac{\Lambda}{(g^e,\omega_n)}$ is finite if g is a prime element of Λ coprime to ω_n for all $n\geq 0$. So by Lemma 7.1.2-(1), we get

$$\mathfrak{F}\left(\frac{\Lambda}{g^e}\right) \simeq \mathrm{Ext}^1_\Lambda(\frac{\Lambda}{g^e},\Lambda)^\iota \simeq \frac{\Lambda}{\iota(g)^e}.$$

For (4), we only prove for $e\geq 2$. Let $h=\omega_{m+1,m}$ and consider the following exact sequence for $n\geq m+1$:

$$0\to \frac{\Lambda}{(h^{e-1},\frac{\omega_n}{h})} \xrightarrow{\times h} \frac{\Lambda}{(h^e,\omega_n)} \to \frac{\Lambda}{h} \to 0.$$

Since $\frac{\Lambda}{h}$ is $\mathbb{Z}_p$ torsion-free, we get $\frac{\Lambda}{(h^{e-1}, \frac{\omega_n}{h})}[p^\infty] \simeq \frac{\Lambda}{(h^e, \omega_n)}[p^\infty]$. So we get

$$\begin{aligned}
\mathfrak{F}(\frac{\Lambda}{h^e}) &= \left(\varinjlim_n \frac{\Lambda}{(h^e, \omega_n)}[p^\infty]\right)^\vee = \left(\varinjlim_n \frac{\Lambda}{(h^{e-1}, \frac{\omega_n}{h})}[p^\infty]\right)^\vee \\
&= \left(\varinjlim_n \frac{\Lambda}{(h^{e-1}, \frac{\omega_n}{h})}\right)^\vee \qquad \text{(Since } h \text{ is coprime to } \frac{\omega_n}{h} \text{ for all } n \geq m+1 \text{)} \\
&\simeq \mathrm{Ext}^1_\Lambda(\frac{\Lambda}{h^{e-1}}, \Lambda)^\iota \qquad \text{(By Lemma 7.1.2-(1))} \\
&\simeq \frac{\Lambda}{\iota(h)^{e-1}}
\end{aligned}$$

which shows the assertion. □

Lemma 7.1.4. *Let $0 \to K \to X \xrightarrow{\phi} Z \to 0$ be a short exact sequence of finitely generated Λ modules where K is finite. Then the natural map $\mathfrak{F}(\phi) : \mathfrak{F}(Z) \to \mathfrak{F}(X)$ is an isomorphism.*

Proof. Since the tensor functor is right exact, we have $\frac{K}{\omega_n K} \to \frac{X}{\omega_n X} \to \frac{Z}{\omega_n Z} \to 0$.

Let A_n, B_n be the kernel and image of $\frac{K}{\omega_n K} \to \frac{X}{\omega_n X}$, recpectively. Note that both are finite modules since K is finite. We have the following two short exact sequences

$$0 \to A_n \to \frac{K}{\omega_n K} \to B_n \to 0 \tag{7.1}$$

$$0 \to B_n \to \frac{X}{\omega_n X} \to \frac{Z}{\omega_n Z} \to 0 \tag{7.2}$$

By Lemma 2.1.4-(2), two sequences remain exact after taking p^∞-torsion parts. Since $\mathfrak{F}(K) = 0$ by Lemma 7.1.3, we get $(\varinjlim_n B_n[p^\infty])^\vee = 0$ from (7.1). Applying this to (7.2) gives an isomorphism

$$\mathfrak{F}(\phi) : \mathfrak{F}(Z) \xrightarrow{\mathfrak{F}(\phi)} \mathfrak{F}(X).$$

□

Lemma 7.1.5. *Let $0 \to Z \xrightarrow{\psi} S \to C \to 0$ be a short exact sequence of finitely generated Λ modules where C is finite. Then the natural map $\mathfrak{F}(\psi) : \mathfrak{F}(S) \to \mathfrak{F}(Z)$ is an injection with finite cokernel.*

Proof. By the snake lemma, we have $C[\omega_n] \to \frac{Z}{\omega_n Z} \to \frac{S}{\omega_n S} \to \frac{C}{\omega_n C} \to 0$.

If we let $X_n = \mathrm{Ker}(C[\omega_n] \to \frac{Z}{\omega_n Z}), E_n = \mathrm{Im}(C[\omega_n] \to \frac{Z}{\omega_n Z}), D_n = \mathrm{Ker}(\frac{S}{\omega_n S} \to \frac{C}{\omega_n C})$, then we get the following three short exact sequences:

$$0 \to X_n \to C[\omega_n] \to E_n \to 0 \tag{7.3}$$

$$0 \to E_n \to \frac{Z}{\omega_n Z} \to D_n \to 0 \tag{7.4}$$

$$0 \to D_n \to \frac{S}{\omega_n S} \to \frac{C}{\omega_n C} \to 0 \tag{7.5}$$

Since C is finite, X_n and E_n are finite for all n. So the sequences $(7.3), (7.4)$ remain exact after taking p^∞-torsion parts due to Lemma 2.1.4-(2). On the other hand, we have $\varinjlim_n \frac{C}{\omega_n C} = 0$ and $\varinjlim_n C[\omega_n] = C$. So by taking direct limit and Pontryagin dual for the sequences $(7.3), (7.4), (7.5)$, we get

$$0 \to \mathfrak{F}(S) \to \mathfrak{F}(Z) \to C^\vee.$$

□

Now we can prove our main goal.

Proposition 7.1.6. *Let X be a finitely generated Λ-module. If we let*

$$E(X) \simeq \Lambda^r \oplus \left(\bigoplus_{i=1}^{d} \frac{\Lambda}{g_i^{l_i}} \right) \oplus \left(\bigoplus_{\substack{m=1 \\ e_1 \cdots e_f \geq 2}}^{f} \frac{\Lambda}{\omega_{a_m+1, a_m}^{e_m}} \right) \oplus \left(\bigoplus_{n=1}^{t} \frac{\Lambda}{\omega_{b_n+1, b_n}} \right)$$

where $r \geq 0$, $g_1, \cdots g_d$ are prime elements of Λ which are coprime to ω_n for all n, $d \geq 0$, $l_1, \cdots, l_d \geq 1$, $f \geq 0$, $e_1, \cdots, e_f \geq 2$ and $t \geq 0$, then we have an injection

$$\left(\bigoplus_{i=1}^{d} \frac{\Lambda}{\iota(g_i)^{l_i}} \right) \oplus \left(\bigoplus_{\substack{m=1 \\ e_1 \cdots e_f \geq 2}}^{f} \frac{\Lambda}{\iota(\omega_{a_m+1, a_m})^{e_m - 1}} \right) \hookrightarrow \mathfrak{F}(X)$$

with finite cokernel. In particular, $F(X)$ is a finitely generated Λ-torsion module.

Proof. By the structure theorem of the finitely generated Λ-modules, we have an exact sequence

$$0 \to K \to X \to E(X) \to C \to 0$$

where K, C are finite modules. Let Z be the image of $X \longrightarrow E(X)$. Now Lemma 7.1.3, Lemma 7.1.4, Lemma 7.1.5 applied to two short exact sequences $0 \to K \to X \to Z \to 0$ and $0 \to Z \to E(X) \to C \to 0$ give the desired assertion. □

Corollary 7.1.7. *Let X be a finitely generated Λ-module and let $X_{\Lambda-\mathrm{tor}}$ be the maximal Λ-torsion submodule of X. If characteristic ideal of $X_{\Lambda-\mathrm{tor}}$ is coprime to ω_n for all n, then there is a pseudo-isomorphism $\phi : X \to \Lambda^{\mathrm{rank}_\Lambda X} \oplus \mathfrak{F}(X)^\iota$. If we assume additionally that X does not have any non-trivial finite submodules, then ϕ is an injection.*

7.2 The functor $\mathfrak{G}$

Now we consider another functor $\mathfrak{G}$.

Definition 7.2.1. For a finitely generated Λ-module X, define $\mathfrak{G}(X) = \varprojlim_n \left(\frac{X}{\omega_n X}[p^\infty]\right)$. Note that $\mathfrak{G}$ is covariant and preserves finite direct sums.

Lemma 7.2.2. *(1) If $\frac{X}{\omega_n X}$ is finite for all n, then $\mathfrak{G}(X) \simeq X$. In particular, $\mathfrak{G}(\frac{\Lambda}{g^e}) \simeq \frac{\Lambda}{g^e}$ if g is coprime to ω_n for all n.*

(2) $\mathfrak{G}(\Lambda) = 0$.

(3)

$$\mathfrak{G}(\frac{\Lambda}{\omega_{m+1,m}^e}) = \begin{cases} \frac{\Lambda}{\omega_{m+1,m}^{e-1}} & e \geq 2, \\ 0 & e = 1. \end{cases}$$

Proof. For (1), since $\frac{X}{\omega_n X}$ is finite for all n, we get $\mathfrak{G}(X) = \varprojlim_n \frac{X}{\omega_n X}$ which is isomorphic to X. Since $\frac{\Lambda}{\omega_n \Lambda}$ is $\mathbb{Z}_p$-torsion-free, $\mathfrak{G}(\Lambda) = 0$. Proof of (3) is almost same as that of Lemma 7.1.3-(4). □

Lemma 7.2.3. *Let $0 \to K \to X \to Z \to 0$ be a short exact sequence of finitely generated Λ-modules where K is finite. Then we have a short exact sequence $0 \to K \simeq \mathfrak{G}(K) \to \mathfrak{G}(X) \to \mathfrak{G}(Z) \to 0$.*

Proof. By the snake lemma, we get $Z[\omega_n] \to \frac{K}{\omega_n K} \to \frac{X}{\omega_n X} \to \frac{Z}{\omega_n Z} \to 0$. Define E_n, A_n, B_n as

$$E_n = \mathrm{Ker}(Z[\omega_n] \to \frac{K}{\omega_n K}), A_n = \mathrm{Im}(Z[\omega_n] \to \frac{K}{\omega_n K}), B_n = \mathrm{Ker}(\frac{X}{\omega_n X} \to \frac{Z}{\omega_n Z}).$$

Then we get the following three exact sequences:

$$0 \to E_n \to Z[\omega_n] \to A_n \to 0 \tag{7.6}$$

$$0 \to A_n \to \frac{K}{\omega_n K} \to B_n \to 0 \tag{7.7}$$

$$0 \to B_n \to \frac{X}{\omega_n X} \to \frac{Z}{\omega_n Z} \to 0 \tag{7.8}$$

Since all the terms in sequence (7.6), (7.7), (7.8) are compact, the sequences (7.6), (7.7), (7.8) remain exact after taking projective limit.

We can easily show that $\varprojlim_n A_n = 0$ and $\varprojlim_n \frac{K}{\omega_n K} \simeq \varprojlim_n B_n$. Since B_n is finite, ($\because K$ is finite), the sequence (7.8) remains exact after taking p^∞-torsion parts. By taking projective limit, we get

$$0 \to \varprojlim_n \frac{K}{\omega_n K} \simeq \varprojlim_n B_n \to \varprojlim_n \frac{X}{\omega_n X}[p^\infty] \to \varprojlim_n \frac{Z}{\omega_n Z}[p^\infty] \to 0$$

which gives the assertion. □

Lemma 7.2.4. *Let $0 \to Z \to S \to C \to 0$ be a short exact sequence of finitely generated Λ modules where C is finite. Then we have an exact sequence $0 \to \mathfrak{G}(Z) \to \mathfrak{G}(S) \to \mathfrak{G}(C) \simeq C$.*

Proof. By the snake lemma, we get $C[\omega_n] \to \frac{M}{\omega_n M} \to \frac{S}{\omega_n S} \to \frac{C}{\omega_n C} \to 0$. Let

$$A_n = \mathrm{Ker}(C[\omega_n] \to \frac{M}{\omega_n M}), B_n = \mathrm{Im}(C[\omega_n] \to \frac{M}{\omega_n M}), E_n = \mathrm{Ker}(\frac{S}{\omega_n S} \to \frac{C}{\omega_n C}).$$

Then we get the following three short exact sequences:

$$0 \to A_n \to C[\omega_n] \to B_n \to 0 \tag{7.9}$$

$$0 \to B_n \to \frac{M}{\omega_n M} \to E_n \to 0 \tag{7.10}$$

$$0 \to E_n \to \frac{S}{\omega_n S} \to \frac{C}{\omega_n C} \to 0 \tag{7.11}$$

We can easily show that $\varprojlim_n B_n = 0$. Taking p^∞-torsion parts from (7.10), (7.11) gives the following two short exact sequences:

$$0 \to B_n \to \frac{M}{\omega_n M}[p^\infty] \to E_n[p^\infty] \to 0 \tag{7.12}$$

$$0 \to E_n[p^\infty] \to \frac{S}{\omega_n S}[p^\infty] \to \frac{C}{\omega_n C}[p^\infty] \tag{7.13}$$

Here, (7.12) is exact due to Lemma 2.1.4.

Since all the terms in (7.12), (7.13) are finite, taking projective limit preserves those two short exact sequences. Combining with $\varprojlim_n B_n = 0$ gives the assertion. $\square$

Now we can prove our main goal for $\mathfrak{G}$, which is an analogue of Proposition 7.1.6.

Proposition 7.2.5. *Let X be a finitely generated Λ-module. If we let*

$$E(X) \simeq \Lambda^r \oplus \left(\bigoplus_{i=1}^{d} \frac{\Lambda}{g_i^{l_i}} \right) \oplus \left(\bigoplus_{\substack{m=1 \\ e_1 \cdots e_f \geq 2}}^{f} \frac{\Lambda}{\omega_{a_m+1,a_m}^{e_m}} \right) \oplus \left(\bigoplus_{n=1}^{t} \frac{\Lambda}{\omega_{b_n+1,b_n}} \right)$$

where $r \geq 0$, $g_1, \cdots g_d$ are prime elements of Λ which are coprime to ω_n for all n, $d \geq 0$, $l_1, \cdots, l_d \geq 1$, $f \geq 0$, $e_1, \cdots, e_f \geq 2$ and $t \geq 0$, then we have a pseudo-isomorphism

$$\mathfrak{G}(X) \xrightarrow{\mathfrak{G}(\phi)} \left(\bigoplus_{i=1}^{d} \frac{\Lambda}{g_i^{l_i}} \right) \oplus \left(\bigoplus_{\substack{m=1 \\ e_1 \cdots e_f \geq 2}}^{f} \frac{\Lambda}{\omega_{a_m+1,a_m}^{e_m-1}} \right).$$

In particular, $\mathfrak{G}(X)$ is a finitely generated Λ-torsion module.

Proof. By the structure theorem of the finitely generated Λ-modules, we have an exact sequence

$$0 \to K \to X \to E(X) \to C \to 0$$

where K, C are finite modules. Let Z be the image of $X \longrightarrow E(X)$. Now Lemma 7.2.2, Lemma 7.2.3, Lemma 7.2.4 applied to two short exact sequences $0 \to K \to X \to Z \to 0$ and $0 \to Z \to E(X) \to C \to 0$ give the desired assertion. $\square$

Combining Proposition 7.1.6 and Proposition 7.2.5, we get the following corollary.

Corollary 7.2.6. *For any finitely generated Λ-module X, two Λ-torsion modules $\mathfrak{F}(X)^\iota$ and $\mathfrak{G}(X)$ are pseudo-isomorphic.*

[CG96] John Coates and Ralph Greenberg. "Kummer theory for abelian varieties over local fields." *Inventiones Mathematicae*, **124**(1-3):129–174, 1996.

[CS00] John Coates and Ramdorai Sujatha. *Galois cohomology of elliptic curves*. Narosa, 2000.

[DDT95] Henri Darmon, Fred Diamond, and Richard Taylor. "Fermat's last theorem." *Current Developments in Mathematics*, **1**(1):157, 1995.

[Fla90] Matthias Flach. "A generalisation of the Cassels-Tate pairing." *J. reine angew. Math*, **412**:113–127, 1990.

[Gre89] Ralph Greenberg. "Iwasawa theory of p-adic representations." *Algebraic number theory*, pp. 97–137, 1989.

[Gre99] Ralph Greenberg. "Iwasawa theory for elliptic curves." In *Arithmetic theory of elliptic curves*, pp. 51–144. Springer, 1999.

[GV00] Ralph Greenberg and Vinayak Vatsal. "On the Iwasawa invariants of elliptic curves." *Inventiones mathematicae*, **142**(1):17–63, 2000.

[Hid86] Haruzo Hida. "Galois representations into $\mathrm{GL}_2(\mathbb{Z}_p[\![X]\!])$ attached to ordinary cusp forms." *Inventiones mathematicae*, **85**(3):545–613, 1986.

[Hid12] Haruzo Hida. *p-adic automorphic forms on Shimura varieties*. Springer Science & Business Media, 2012.

[Hid13a] Haruzo Hida. "Λ-adic Barsotti–Tate groups." 2013.

[Hid13b] Haruzo Hida. "Limit Mordell–Weil groups and their p-adic closure." 2013.

[Hid17] Haruzo Hida. "Analytic variation of Tate-Shafarevich groups." preprint, 2017.

[Ima75] Hideo Imai. "A remark on the rational points of abelian varieties with values in cyclotomic $\mathbb{Z}_p$-extensions." *Proceedings of the Japan Academy*, **51**(1):12–16, 1975.

[Lee18] Jaehoon Lee. "Structure of Mordell-Weil groups over $\mathbb{Z}_p$-extensions." *arXiv:1809.10351*, 2018.

[Maz72] Barry Mazur. "Rational points of abelian varieties with values in towers of number fields." *Inventiones mathematicae*, **18**(3-4):183–266, 1972.

[Mil06] James S Milne. *Arithmetic duality theorems*. Citeseer, 2006.

[NSW00] Jürgen Neukirch, Alexander Schmidt, Kay Wingberg, and Alexander Schmidt. *Cohomology of number fields*, volume 323. Wiley Online Library, 2000.