Iwasawa theoretic studies
on K-groups and Selmer groups

March 2017

Takahiro Kitajima
A Thesis for the Degree of Ph.D. in Science

Iwasawa theoretic studies
on $K$-groups and Selmer groups

March 2017

Graduate School of Science and Technology
Keio University

Takahiro Kitajima
Contents

1 Introduction 2
  1.1 Background .................................................. 2
  1.2 Iwasawa theory ................................................. 3
    1.2.1 Iwasawa theory for ideal class groups ..................... 3
    1.2.2 Iwasawa theory for elliptic curves ....................... 4
  1.3 Main results .................................................. 6
    1.3.1 The plus and the minus Selmer groups for elliptic curves
          at supersingular primes in the cyclotomic $\mathbb{Z}_p$-extension 6
    1.3.2 Orders of even $K$-groups of rings of integers in the
          cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ ................ 7
  1.4 Outline ..................................................... 8

2 Iwasawa modules .................................................. 9

3 $K$-groups of rings of integers 12
  3.1 $K$-groups of rings ........................................... 12
  3.2 Lemmas ....................................................... 15
  3.3 The orders of even $K$-groups ................................ 22

4 The plus and the minus Selmer groups 26
  4.1 Definitions .................................................. 26
  4.2 The formal groups and the norm subgroups ..................... 28
    4.2.1 Honda’s theory .......................................... 29
    4.2.2 The formal groups associated to $E$ ...................... 30
    4.2.3 The norm subgroups .................................... 36
    4.2.4 The plus and the minus local conditions ................. 44
    4.2.5 More on the plus and the minus local conditions ....... 50
  4.3 Finite $\Lambda$-submodules .................................... 52
    4.3.1 Finite $\Lambda$-submodules of $\text{Sel}(F_\infty, E[p^{\infty}])^\vee$ .... 52
    4.3.2 Finite $\Lambda$-submodules of $\text{Sel}^\pm(F_\infty, E[p^{\infty}])^\vee$ .... 54
Chapter 1

Introduction

In number theory the $K$-groups of the ring of integers of a number field and the Selmer groups of an elliptic curve are important objects, and have been studied intensively. In Iwasawa theory, we study the behavior of these objects in $\mathbb{Z}_p$-extensions. The aim of this thesis is such Iwasawa theoretic study of these objects.

1.1 Background

We begin with some historical background of our research.

The $K$-groups of the ring of integers are generalizations of the ideal class groups. We briefly explain ideal class groups. The ideal class group $\text{Cl}(\mathbb{L})$ of a number field $\mathbb{L}$ is the quotient group $\text{Cl}(\mathbb{L}) = \mathbb{I}(\mathbb{L})/\mathbb{P}(\mathbb{L})$, where $\mathbb{I}(\mathbb{L})$ is the group of fractional ideals of $\mathbb{L}$ and $\mathbb{P}(\mathbb{L})$ is its subgroup of principal ideals of $\mathbb{L}$. It is known that $\text{Cl}(\mathbb{L})$ is a finite abelian group, however, it is quite hard in general to compute the exact order of $\text{Cl}(\mathbb{L})$ for each $\mathbb{L}$. Ideal class groups are widely investigated even today.

There exists a classical and remarkable formula, the analytic class number formula, which relates the ideal class groups to the Dedekind zeta function. The explicit statement is as follows. Let $\mathbb{L}$ be a number field, $\zeta_{\mathbb{L}}(s)$ the Dedekind zeta function of $\mathbb{L}$, $h(\mathbb{L})$ the order of $\text{Cl}(\mathbb{L})$, $\text{Reg}(\mathbb{L})$ the regulator of $\mathbb{L}$, and $w(\mathbb{L})$ the number of the roots of unity in $\mathbb{L}$. Then we have

$$\lim_{s \to 0} s^\frac{-r_1+r_2-1}{2}\zeta_{\mathbb{L}}(s) = -\frac{h(\mathbb{L}) \text{Reg}(\mathbb{L})}{w(\mathbb{L})},$$

where $r_1$ and $2r_2$ are the numbers of real embeddings $\mathbb{L} \hookrightarrow \mathbb{R}$ and complex embeddings $\mathbb{L} \hookrightarrow \mathbb{C}$, respectively. This formula means that the special values of the Dedekind zeta functions know the orders of the ideal class groups. As
a refinement of the analytic class number formula, there is a conjecture in
Iwasawa theory, which is called the Iwasawa Main Conjecture.

1.2 Iwasawa theory

We introduce Iwasawa theory in this section. We review some basic known
properties on ideal class groups in the first subsection, and those on Selmer
groups of an elliptic curve in the second subsection. We also mention some
problems on Selmer groups of an elliptic curve in Iwasawa theory.

1.2.1 Iwasawa theory for ideal class groups

The Iwasawa Main Conjecture for ideal class groups describes a more pre-
cise relation between the “$p$-part” of ideal class groups and the “$p$-adic”
$L$-functions for each prime number $p$, than the analytic class number for-
formula. Let $p$ be a prime number, $L$ a totally real number field, $F$ a CM
extension of $L$ such that $F/L$ is abelian, $\chi$ an odd character of $\text{Gal}(F/L)$,
$F_\infty$ the cyclotomic $\mathbb{Z}_p$-extension of $F$, and $\mathcal{X}_{F_\infty}$ the Galois group of the
maximal abelian pro-$p$ unramified extension of $F_\infty$. We define a $\text{Gal}(F/L)$-
module $O_\chi$ by $O_\chi = \mathbb{Z}_p[\text{Image}\chi]$ on which $\text{Gal}(F/L)$ acts via $\chi$; $\sigma x = \chi(\sigma)x$
for $\sigma \in \text{Gal}(F/L)$ and $x \in O_\chi$. Note that $O_\chi$ is a discrete valuation
ring and we denote by $\pi$ a prime element of $O_\chi$. Assume for simplicity
$F \cap L_\infty = L$. Then the $\chi$-part $M_\chi$ of a $\mathbb{Z}_p[\text{Gal}(F/L)]$-module $M$ is defined
by $M_\chi = M \otimes_{\mathbb{Z}_p[\text{Gal}(F/L)]} O_\chi$. Put $\Lambda_\chi = O_\chi[[\text{Gal}(F_\infty/F)]]$. Then the $\chi$-part
$\mathcal{X}_{F_\infty,\chi}$ of $\mathcal{X}_{F_\infty}$ is known to be finitely generated $\Lambda_\chi$-torsion. By the structure
theorem for $\Lambda_\chi$-modules, there exist irreducible distinguished polynomials $f_j$, nonnegative integers $s, t, m_i, n_j$ and a homomorphism

$$\mathcal{X}_{F_\infty,\chi} \to \bigoplus_{i=1}^s \Lambda_\chi/(\pi_i^{m_i}) \oplus \bigoplus_{j=1}^t \Lambda_\chi/(f_j^{n_j})$$

(1.2.1)

with finite kernel and finite cokernel. We note that the target of the homo-
morphism (1.2.1) is uniquely determined by $\mathcal{X}_{F_\infty,\chi}$. We define the character-
istic ideal of $\mathcal{X}_{F_\infty,\chi}$ by

$$\text{Char}_\Lambda(\mathcal{X}_{F_\infty,\chi}) = \left( \prod_{i=1}^s \pi_i^{m_i} \prod_{j=1}^t f_j^{n_j} \right).$$

Let $L_{p,\chi} \in \Lambda_\chi$ be the $p$-adic $L$-function of Deligne and Ribet, constructed
from the Stickelberger elements. Then the Iwasawa Main Conjecture claims
that
\[ \text{Char}_\chi(\mathcal{X}_{F_\infty,\chi}) = (\mathcal{L}_{p,\chi}) \subset \Lambda \]
for any odd character \( \chi \) such that \( \chi \neq \omega \) where \( \omega \) is the Teichmüller character.
This conjecture was proved when \( L = \mathbb{Q} \) by Mazur and Wiles (cf. [22]), and for general totally real field \( L \) and for \( p > 2 \) by Wiles (cf. [41]).

As an application of the Iwasawa Main Conjecture, we have the following formula which describes the relation between the Dedekind zeta function and the \( K \)-groups. Let \( L \) be a totally real number field, \( \mathcal{O}_L \) the ring of integers in \( L \), and \( K_m(\mathcal{O}_L) \) the \( m \)-th \( K \)-group of \( \mathcal{O}_L \) defined by Quillen. Then for each even number \( m \in \mathbb{Z}_{>0} \), we have

\[ \zeta_L(1 - m) = \pm 2^{a_m(L)} \frac{\# K_{2m-2}(\mathcal{O}_L)}{w_m(L)} \]
for some \( a_m(L) \in \mathbb{Z} \), where \( w_m(L) = \max\{ t \in \mathbb{Z}_{>0} \mid \text{Gal}(L(\mu_t)/L)^m = 1 \} \).

Next we refer a classical result on ideal class groups concerning non-existence of nontrivial finite submodules.

We denote the completed group ring \( \mathbb{Z}_p[[\text{Gal}(F_\infty/F)]] \) by \( \Lambda \). Then \( \mathcal{X}_{F_\infty} \) is known to be a finitely generated torsion module over \( \Lambda \).

If \( F \) is a CM-field, the complex conjugation \( J \) acts naturally on \( \mathcal{X}_{F_\infty} \). Further if \( p \) is odd, then \( \mathcal{X}_{F_\infty} \) is decomposed into \( \mathcal{X}_{F_\infty} = \mathcal{X}_{F_\infty}^{J=1} \oplus \mathcal{X}_{F_\infty}^{J=-1} \), where \( \mathcal{X}_{F_\infty}^{J=1} = \{ x \in \mathcal{X}_{F_\infty} \mid Jx = x \} \) and \( \mathcal{X}_{F_\infty}^{J=-1} = \{ x \in \mathcal{X}_{F_\infty} \mid Jx = -x \} \).

**Theorem 1.2.1** (Iwasawa). If \( F \) is a CM-field, then \( \mathcal{X}_{F_\infty}^{J=-1} \) has no nontrivial finite \( \Lambda \)-submodules.

If a given \( \Lambda \)-module \( M \) has no nontrivial finite \( \Lambda \)-submodules as in Theorem 1.2.1, then we can understand more precise structure of \( M \) than the general structure theorem. Actually Iwasawa studied \( \mathcal{X}_{F_\infty}^{J=-1} \) thoroughly using this non-existence of nontrivial finite \( \Lambda \)-submodules. The non-existence of nontrivial finite \( \Lambda \)-submodules is a basic and important property in Iwasawa theory.

**1.2.2 Iwasawa theory for elliptic curves**

Let \( E \) be an elliptic curve defined over \( \mathbb{Q} \) such that \( E \) has good reduction at a prime number \( p \), i.e. the reduced curve \( \overline{E} \mod p \) is nonsingular. Denote \( a_p = 1 + p - \# E(\mathbb{F}_p) \). We say that \( E \) has good ordinary reduction at \( p \) if \( a_p \equiv 0 \mod p \), and \( E \) has good supersingular reduction at \( p \) if \( a_p \equiv 0 \mod 4 \).
Note that if $E$ has good supersingular reduction at $p$ and $p \geq 5$, then $a_p = 0$ by the Hasse bound $|a_p| \leq 2\sqrt{p}$.

We put $F_0 = \mathbb{Q}(\mu_m)$ for simplicity. Let $F_\infty/F_0$ be the cyclotomic $\mathbb{Z}_p$-extension and $F_n$ the $n$-th layer. Denote $\Lambda = \mathbb{Z}_p[[\text{Gal}(F_\infty/F_0)]]$. The Selmer groups for $E$ over $F_\infty$ are subgroups of the Galois cohomology group $H^1(F_\infty, E[p^\infty])$ defined by certain “local conditions”. The Pontryagin dual of the Selmer group is a corresponding object to the ideal class group in Iwasawa theory for elliptic curves.

When $E$ has good ordinary reduction at $p$, the Pontryagin dual of the $p$-primary Selmer group $\text{Sel}(F_\infty, E[p^\infty])$ of $E$ over $F_\infty$ (see Section 4.1 for the definition) is conjectured to be $\Lambda$-torsion. This conjecture was proved in our setting by Kato. Greenberg and Hachimori-Matsuno proved that if $E$ has ordinary reduction at $p$ and $E(F_0)[p] = 0$ then the Pontryagin dual of $\text{Sel}(F_\infty, E[p^\infty])$ has no nontrivial finite $\Lambda$-submodules (cf. [7]).

On the contrary, when $E$ has good supersingular reduction at $p$, the Pontryagin dual of the $p$-primary Selmer group of $E$ over $F_\infty$ is no longer $\Lambda$-torsion. In fact, it is known that the Pontryagin dual $\text{Sel}(F_\infty, E[p^\infty])^\vee$ of the $p$-primary Selmer group has positive $\Lambda$-rank; more precisely, we have

$$\text{rank}_\Lambda \text{Sel}(F_\infty, E[p^\infty])^\vee \geq [F_0 : \mathbb{Q}]$$

(cf. [6, Theorem 1.7]). So we cannot formulate the Iwasawa Main Conjecture in the classical style in terms of the $p$-primary Selmer group. To avoid this difficulty, Shin-ichi Kobayashi [17] defined new Selmer groups $\text{Sel}^+(F_\infty, E[p^\infty])$ and $\text{Sel}^-(F_\infty, E[p^\infty])$, which we call the plus and the minus Selmer groups, when $a_p = 0$, and $F_0 = \mathbb{Q}(\mu_p)$, where $\mu_p$ denotes the group of $p$-th roots of unity. He actually proved that the Pontryagin duals $\text{Sel}^\pm(F_\infty, E[p^\infty])^\vee$ are $\Lambda$-torsion and formulated the Iwasawa Main Conjecture in the classical style. Adrian Iovita and Robert Pollack [10] generalized definitions of the plus and the minus Selmer groups to the case when $GCD(p, m) = 1$ and $a_p = 0$.

Byoung Du Kim [11] generalized them to the case when $GCD(p, m) = 1$ and $a_p = 0$. Further Byoung Du Kim [12] studied in [12] the problem on the existence of nontrivial finite $\Lambda$-submodules of $\text{Sel}^\pm(F_\infty, E[p^\infty])^\vee$, however, his result was not completely general. In particular, he assumed further the congruence condition $p \equiv 1 \pmod{m}$ when he studied the plus Selmer group. We also note that he did not consider the case when $\mu_p \subset F_0$.

The aim of this thesis is to remove those conditions. In this thesis, we consider more general $F_0$. In particular, we remove the assumption on the congruence condition $p \equiv 1 \pmod{m}$. We also consider the case when $\mu_p \subset F_0$. 


1.3 Main results

We study two different objects, $K$-groups and Selmer groups, and get two different results. The main result of this thesis is the result on Selmer groups. So we explain our result on Selmer groups at first in §1.3.1, and that on $K$-groups in §1.3.2.

1.3.1 The plus and the minus Selmer groups for elliptic curves at supersingular primes in the cyclotomic $\mathbb{Z}_p$-extension

In this section, we state our main theorem on the non-existence of nontrivial finite $\Lambda$-submodules of the Pontryagin duals of the plus and the minus Selmer groups.

As in Section 1.2.2, we explain our results in the following setting. Let $E$ be an elliptic curve defined over $\mathbb{Q}$ such that $E$ has good supersingular reduction at a prime number $p$ with $a_p = 0$. Let $F = \mathbb{Q}(\mu_m)$ such that $\text{GCD}(p,m) = 1$, $F_0 = F(\mu_p)$ and $F_\infty$ the cyclotomic $\mathbb{Z}_p$-extension of $F_0$.

In this setting, our main result (Theorem 4.3.8) is the following generalization of a result of Byoung Du Kim.

**Theorem 1.3.1** (Corollary 4.3.9). Both $\text{Sel}^\pm(F_\infty, E[p^\infty])^\vee$ have no nontrivial finite $\Lambda$-submodule.

**Remark 1.3.2.** (1) Our proof works as well for more general elliptic curves and base fields than the above. The precise setting will be explained in Section 4.1, and we will get the same conclusion, i.e. non-existence of nontrivial finite $\Lambda$-submodule.

(2) We can also remove the condition $\text{GCD}(p, m) = 1$, since the Selmer groups $\text{Sel}^\pm(F_\infty, E[p^\infty])$ are objects over $F_\infty$ and the non-existence of nontrivial finite $\Lambda$-submodules is independent of the choice of a base field $F_0$.

(3) By this theorem (and the above remark), we find that the plus and the minus Selmer groups are unconditionally in “good” situation as the ideal class groups (see Theorem 1.2.1).

To prove the above theorem, we study the $\Lambda$-module structures of the plus and the minus local conditions $E^\pm(k_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p$. The key of the proof of Theorem 1.3.1 is to determine the explicit $\Lambda$-module structures of them as the following theorem.
Theorem 1.3.3 (Theorem 4.2.37). Let $E$ be an elliptic curve defined over $\mathbb{Q}_p$ with $a_p = 0$, $k = \mathbb{Q}_p(\mu_m)$ such that $\gcd(p, m) = 1$, $k_0 = k(\mu_p)$ and $k_\infty$ the cyclotomic $\mathbb{Z}_p$-extension of $k_0$. We denote the completed group ring $\mathbb{Z}_p[[\text{Gal}(k_\infty/k)]]$ by $\Lambda_k$. Then we have isomorphisms

\[
(E^-(k_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\vee} \cong \Lambda_k^{[k:Q_p]},
\]

\[
(E^+(k_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\vee} \cong \Lambda_k^{[k:Q_p]} \oplus (\Lambda_k/I) \oplus \delta,
\]

of $\Lambda_k$-modules, where $I = \ker(\Lambda_k \to \mathbb{Z}_p)$ is the augmentation ideal, and

\[
\delta = \begin{cases} 
0 & \text{if } [k : Q_p] \not\equiv 0 \text{ (mod 4)}, \\
2 & \text{otherwise.}
\end{cases}
\]

Remark 1.3.4. In the setting of [12], the Pontryagin duals of the plus and the minus local conditions $E^\pm(k_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ are $\Lambda$-free. By our theorem, we find that this $\Lambda$-freeness breaks down in general.

1.3.2 Orders of even $K$-groups of rings of integers in the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$

We formulate a problem on the orders of even $K$-groups and state our theorem on this problem.

For that purpose, we briefly review some known properties on $K$-groups. Let $A$ be a Dedekind domain and $K_m(A)$ the $m$-th Quillen $K$-group for any integer $m \geq 0$. The precise definition of the Quillen $K$-group of a ring will be introduced in Section 3.1. We know that $K_0(A)$ is isomorphic to $\mathbb{Z} \oplus \text{Cl}(A)$ (cf. [23]), Thus the ideal class group of $A$ is isomorphic to the torsion subgroup of $K_0(A)$;

\[
\text{Cl}(A) \cong K_0(A)_{\text{tors}}.
\]

When $A$ is a ring of integers, For any $m \geq 0$, $K_m(\mathcal{O}_L)$ is a finitely generated abelian group (cf. Quillen [27]). Thus the torsion part $K_m(\mathcal{O}_L)_{\text{tors}}$ is finite for any $m \geq 0$. We will study the torsion parts of the $K$-groups as an analogue of the ideal class groups. In this thesis, we study $K_m(\mathcal{A})_{\text{tors}}$ in the case when $A$ varies over the class of the rings of integers.

Let $F$ be a number field and $\hat{F}$ the composite field of all the cyclotomic $\mathbb{Z}_p$-extensions of $F$. We consider the following problem.

Problem 1.3.5. Assume that $F$ is totally real and $m \geq 0$ is an integer. Is

\[
\{ \#K_m(\mathcal{O}_L)_{\text{tors}} | L/F : \text{finite extension}, L \subset \hat{F} \}
\]

bounded?
Remark 1.3.6. When \( m \) is even, \( K_m(\mathcal{O}_L) \) is finite (cf. Borel [2]), and thus we have \( K_m(\mathcal{O}_L)_{\text{tors}} = K_m(\mathcal{O}_L) \).

Remark 1.3.7. (1) The case when \( m = 0 \) is the problem on ideal class groups, which is posed by John Coates. This case is quite hard.

(2) The case when \( m = 1 \) is true. In fact \( K_1(\mathcal{O}_L) \) is known to be isomorphic to \( \mathcal{O}_L^\times \) (cf. [1]). Hence \( K_1(\mathcal{O}_L)_{\text{tors}} = \mu_2 \) for all intermediate fields \( L \) of \( \hat{F}/F \).

In this thesis, we study the case when \( m \equiv 2 \pmod{4} \) and \( F = \mathbb{Q} \). We prove that the problem is false in this case. We now state our result more precisely.

Let \( p \) be a prime number. Let \( \mathbb{B}_\infty/\mathbb{Q} \) be the cyclotomic \( \mathbb{Z}_p \)-extension and \( \mathbb{B}_n \) the \( n \)-th layer.

**Theorem 1.3.8 (Theorem 3.3.3).** Let \( m \) be an even number \( \geq 2 \) and \( h_n = \# K_{2m-2}(\mathcal{O}_B) \). Then \( \{ h_n \mid n \geq 0 \} \) is unbounded.

Furthermore, there are infinitely many prime numbers which divide \( h_n \) for some \( n \in \mathbb{Z}_{\geq 0} \), i.e.

\[
\# \{ \ell : \text{prime number} \mid \text{there exists } n \in \mathbb{Z}_{\geq 0} \text{ such that } \ell \mid h_n \} = \infty.
\]

Remark 1.3.9. This theorem shows that the behavior of the \( K \)-groups \( K_{2m-2}(\mathcal{O}_B) \) is completely different from the conjectural behavior of the ideal class groups \( \text{Cl}(\mathbb{B}_n) \).

### 1.4 Outline

The outline of this thesis is as follows. In Chapter 2, we review some properties of Iwasawa algebras and Iwasawa modules. In Chapter 3, we prove our main theorem on the orders of even \( K \)-groups \( K_{2m-2}(\mathcal{O}_B) \). In Chapter 4, we study the \( \Lambda \)-module structures of the plus and the minus Selmer groups \( \text{Sel}^\pm(F_\infty, E[p^\infty])^\vee \) and the plus and the minus local conditions \( (E^\pm(k_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\vee \). We prove that the classical \( p \)-primary Selmer group \( \text{Sel}(F_\infty, E[p^\infty])^\vee \) has no nontrivial finite \( \Lambda \)-submodules under our setting. Finally we prove our main theorem on the non-existence of nontrivial finite \( \Lambda \)-submodules of the plus and the minus Selmer groups \( \text{Sel}^\pm(F_\infty, E[p^\infty])^\vee \).
Chapter 2

Iwasawa modules

In this chapter, we review some properties of Iwasawa algebras and Iwasawa modules. Let $p$ be a prime number, $\Gamma$ a topological group which is isomorphic to the additive group $\mathbb{Z}_p$.

**Definition 2.0.1** (Completed group ring). The completed group ring of $\Gamma$ over $\mathbb{Z}_p$ is the topological inverse limit

$$\mathbb{Z}_p[[\Gamma]] = \lim_{\leftarrow n} \mathbb{Z}_p[\Gamma/\Gamma_n],$$

where $n$ runs through positive integers, and $\Gamma_n$ the unique subgroup of $\Gamma$ of index $p^n$.

**Proposition 2.0.2** (Serre [29]). Let $\gamma$ be a topological generator of $\Gamma(\simeq \mathbb{Z}_p)$. There is a non-canonical isomorphism

$$\mathbb{Z}_p[[X]] \sim \mathbb{Z}_p[[\Gamma]],$$

$$X \mapsto \gamma - 1,$$

of topological rings.

By this proposition, we identify the completed group ring $\mathbb{Z}_p[[\Gamma]]$ with the formal power series ring $\mathbb{Z}_p[[X]]$ using any fixed generator $\gamma$, and denote the ring by $\Lambda$.

**Definition 2.0.3** (Distinguished polynomial). A polynomial $f(X) \in \mathbb{Z}_p[X]$ is said to be a distinguished polynomial if it is of the form

$$f(X) = X^s + a_{s-1}X^{s-1} + \cdots + a_1X + a_0$$

with coefficients $a_0, \ldots, a_{s-1}$ contained in the maximal ideal $(p)$ of $\mathbb{Z}_p$. 

Theorem 2.0.4 (Structure theorem for $\Lambda$-modules). Let $M$ be a finitely generated $\Lambda$-module. Then there exist irreducible distinguished polynomials $f_j \in \mathbb{Z}_p[X]$, nonnegative integers $r, s, t$, positive integers $m_i, n_j$, and a homomorphism

$$M \rightarrow \Lambda^{\oplus r} \oplus \bigoplus_{i=1}^{s} \Lambda/p^{m_i} \oplus \bigoplus_{j=1}^{t} \Lambda/f^{n_j}_j$$

with finite kernel and cokernel. The integers $r, m_i, n_j$ and the prime ideals $(f_j)$ of $\Lambda$ are uniquely determined by $M$.

This theorem guarantees the following quantities are well-defined.

Definition 2.0.5 ($\Lambda$-rank, Iwasawa invariants, characteristic ideal). With the notation of Theorem 2.0.4, we call

$$\text{rank}_\Lambda(M) = r$$

the $\Lambda$-rank of $M$,

$$\mu(M) = \sum_{i=1}^{s} m_i$$

the Iwasawa $\mu$-invariant of $M$,

$$\lambda(M) = \sum_{j=1}^{t} n_j \deg(f_j)$$

the Iwasawa $\lambda$-invariant of $M$,

$$\text{Char}_\Lambda(M) = \left( \prod_{j=1}^{t} f^{n_j}_j \right) (\subset \Lambda)$$

the characteristic ideal of $M$.

Proposition 2.0.6. Let

$$0 \rightarrow M_1 \rightarrow M_2 \rightarrow M_3 \rightarrow 0$$

be an exact sequence of $\Lambda$-modules. Then we have

$$\text{rank}_\Lambda(M_2) = \text{rank}_\Lambda(M_1) + \text{rank}_\Lambda(M_3).$$

Proof. Let $Q(\Lambda)$ be the quotient field of $\Lambda$. We have

$$\text{rank}_\Lambda(M_i) = \dim_{Q(\Lambda)} (M_i \otimes_\Lambda Q(\Lambda))$$

for $i = 1, 2, 3$, and the sequence

$$0 \rightarrow M_1 \otimes_\Lambda Q(\Lambda) \rightarrow M_2 \otimes_\Lambda Q(\Lambda) \rightarrow M_3 \otimes_\Lambda Q(\Lambda) \rightarrow 0$$

is exact. Thus we get the conclusion. \qed
We denote $M_{\Gamma_n}$ the module of $\Gamma_n$-coinvariants of $M$:

$$M_{\Gamma_n} = M/I_{\Gamma_n}M \simeq M/\omega_n(X)M,$$

where $I_{\Gamma_n}$ is the augmentation ideal

$$I_{\Gamma_n} = \langle \sigma - 1 \mid \sigma \in \Gamma_n \rangle_{\Lambda},$$

and $\omega_n(X) = (1 + X)^{p^n} - 1$.

**Proposition 2.0.7** (Invariant-coinvariant exact sequences). Let

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

be an exact sequence of $\Lambda$-modules. Then there are exact sequences of $\mathbb{Z}_p$-modules

$$0 \to M_1^{\Gamma_n} \to M_2^{\Gamma_n} \to M_3^{\Gamma_n} \to (M_1)_{\Gamma_n} \to (M_2)_{\Gamma_n} \to (M_3)_{\Gamma_n} \to 0$$

for all $n \geq 0$.

**Proof.** Since all $\Gamma_n$ are pro-cyclic, we can take topological generators $\gamma_n$ of $\Gamma_n$ for all $n$, and we have exact sequences

$$0 \to M_i^{\Gamma_n} \to M_i^{\gamma_n} \to M_i \to (M_i)_{\Gamma_n} \to 0$$

for $i = 1, 2, 3$. The result follows from the snake lemma. \[\square\]

**Proposition 2.0.8** (Topological Nakayama’s lemma). Let $M$ be a $\Lambda$-module.

(1) The following three conditions are equivalent.

(i) $M$ is a finitely generated $\Lambda$-module.

(ii) $M_{\Gamma}$ is a finitely generated $\mathbb{Z}_p$-module.

(iii) $M/(p, X)M$ is a finite-dimensional $\mathbb{F}_p$-vector space.

(2) If $M$ is a finitely generated $\Lambda$-module, then

$$(p, X)M = M \iff M = 0.$$
Chapter 3

$K$-groups of rings of integers

In this chapter we study the orders $h_n$ of even $K$-groups $K_{2n-2}(O_{\mathbb{Z}_n})$. In §3.1, we review the definition of higher $K$-groups after Daniel Quillen. §3.2 is a preparation for §3.3. In particular, we estimate the absolute values of the generalized Bernoulli numbers for each valuation. In §3.3, we give an upper bound on the $p$-exponent of the quotient $h_n/h_{n-1}$. Finally we prove the main theorem (Theorem 3.3.3).

3.1 $K$-groups of rings

In this section, we review Quillen’s $Q$-construction for exact categories, and define higher $K$-groups for rings as a special case. Main references of this section are [25, 26, 33, 40].

Definition 3.1.1 (Small, essentially small categories). A category $\mathcal{A}$ is said to be small if the class of objects of $\mathcal{A}$ forms a set.

A category $\mathcal{A}$ is said to be essentially small if it is equivalent to a small category.

Example 3.1.2. Let $R$ be a ring with unit. The category $\mathcal{P}(R)$ of finitely generated projective $R$-modules is essentially small. Indeed $\mathcal{P}(R)$ has a set of isomorphism classes of objects.

For a nonnegative integer $n$, denote $\mathbf{n}$ the category with objects $\{0, 1, \ldots, n\}$, with exactly one morphism $i \rightarrow j$ for each $i \leq j$. Denote $\Delta$ the following category; the objects are $\mathbf{n}$ for all $n \in \mathbb{Z}_{\geq 0}$, and the morphisms are all functors $\mathbf{m} \rightarrow \mathbf{n}$.

A simplicial set is a contravariant functor $\Delta \rightarrow \text{Sets}$. 

12
Definition 3.1.3 (Geometric realization of a simplicial set). Let $\mathcal{F} : \Delta \to \text{Sets}$ be a simplicial set. The geometric realization $|\mathcal{F}|$ of $\mathcal{F}$ is defined to be the quotient space

$$|\mathcal{F}| = \left( \prod_{n \geq 0} (\mathcal{F}(n) \times \Delta_n) \right) / \sim,$$

where $\Delta_n = \{(t_0, \ldots, t_n) \in \mathbb{R}^{n+1} \mid t_i \geq 0, \sum t_i = 1\}$, and $\mathcal{F}(n)$ is regarded as a discrete space for each $n \geq 0$. The equivalence relation $\sim$ is defined as follows: for each $f \in \text{Hom}_{\Delta}(m, n)$, let $\tilde{f} \in \text{Cont}(\Delta_m, \Delta_n)$ be the induced continuous map. Then for any $x \in \Delta_m$ and $y \in \mathcal{F}(n)$, we set

$$(\mathcal{F}(f)(y), x) \sim (y, \tilde{f}(x)),$$

where $(\mathcal{F}(f)y, x) \in \mathcal{F}(m) \times \Delta_m$, and $(y, \tilde{f}(x)) \in \mathcal{F}(n) \times \Delta_n$. Let $\sim$ be the equivalence relation so generated, and $|\mathcal{F}|$ the quotient space, with the quotient topology.

Definition 3.1.4 (The nerve of a small category). The nerve $N\mathcal{A}$ of a small category $\mathcal{A}$ is the simplicial set $\Delta \to \text{Sets}$ defined by the following data. Its $n$-simplices are diagrams in $\mathcal{A}$ of the form

$$A_0 \to A_1 \to \cdots \to A_n.$$

Definition 3.1.5 (Classifying space of a small category). The classifying space of a small category $\mathcal{A}$ is defined to be the geometric realization of $N\mathcal{A}$ and is denoted by $B\mathcal{A}$;

$$B\mathcal{A} = |N\mathcal{A}|.$$

Definition 3.1.6 (Exact categories). An exact category $\mathcal{A}$ is an additive category $\mathcal{A}$ embedded as a full subcategory of an abelian category $\mathcal{B}$, such that $\mathcal{A}$ is closed under extension in $\mathcal{B}$ i.e. if $0 \to A' \to A \to A'' \to 0$ is an exact sequence in $\mathcal{A}$ with $A', A'' \in \mathcal{B}$, then $A$ is isomorphic to an object of $\mathcal{B}$.

An exact sequence in an exact category $\mathcal{A}$ is defined to be an exact sequence in $\mathcal{B}$ whose term lies in $\mathcal{A}$.

An epimorphism $q : A \to A''$ in $\mathcal{A}$ is said to be admissible if there is an exact sequence $0 \to A' \to A \xrightarrow{q} A'' \to 0$ in $\mathcal{A}$. A monomorphism $i : A' \to A$ in $\mathcal{A}$ is said to be admissible if there is an exact sequence $0 \to A' \xrightarrow{i} A \to A'' \to 0$ in $\mathcal{A}$.
Remark 3.1.7. The admissibility of a morphism is closed under composition in an exact category, i.e. the composition of admissible epimorphisms (resp. admissible monomorphisms) is again an admissible epimorphism (resp. admissible monomorphism).

Example 3.1.8. The category \( \mathcal{P}(R) \) is an exact category. Indeed \( \mathcal{P}(R) \) is a full subcategory of the abelian category \( \mathcal{M}(R) \) of finitely generated \( R \)-modules.

Definition 3.1.9 (\( Q \)-construction for an exact category). Let \( \mathcal{A} \) be an exact category. Define a category \( Q\mathcal{A} \) as follows: \( Q\mathcal{A} \) has the same objects as \( \mathcal{A} \). A morphism from \( A \) to \( B \) in \( Q\mathcal{A} \) is an equivalence class of diagrams

\[
A \xleftarrow{q} B' \xrightarrow{i} B,
\]

where \( i \) is an admissible monomorphism and \( q \) is an admissible epimorphism in \( \mathcal{A} \). Two such diagrams \( A \xleftarrow{q} B' \xrightarrow{i} B \) and \( A \xleftarrow{q'} B'' \xrightarrow{i'} B \) are equivalent if there is an isomorphism \( B' \rightarrow B'' \) such that the diagram

\[
\begin{array}{ccc}
A & \xleftarrow{q} & B' \\
\downarrow & & \downarrow \\
A & \xleftarrow{q'} & B''
\end{array}
\begin{array}{ccc}
\xrightarrow{i} & & \xrightarrow{i'} \\
\uparrow & & \\
B & & B
\end{array}
\]

commutes. The composition of two morphisms \( A \xleftarrow{q} B' \rightarrow B \) and \( B \xleftarrow{C'} \rightarrow C \) is the equivalence class of \( A \xleftarrow{q''} B' \times_B C' \rightarrow C \), which is defined by the diagram

\[
\begin{array}{ccc}
A & \xleftarrow{q''} & B' \times_B C' \\
\uparrow & & \downarrow \\
B' & \xrightarrow{\times_B} & B \\
\uparrow & & \uparrow \\
B' \times_B C' & \rightarrow & C
\end{array}
\]

Remark 3.1.10. The morphism \( q'' \) (resp. \( i'' \)) in the above last diagram is certainly an admissible epimorphism (resp. an admissible monomorphism). Indeed, we have \( \text{Ker}(q'') \cong \text{Ker}(C' \rightarrow B) \in \mathcal{A} \), and thus \( B' \times_B C' \in \mathcal{A} \) since \( \mathcal{A} \) is closed under extension. Therefore \( q'' \) is an admissible epimorphism. The rest of our claim follows from \( \text{Coker}(i'') \cong \text{Coker}(B' \rightarrow B) \).

We can also check that the equivalence class of the above diagram depends only on the equivalence classes of \( A \xleftarrow{B'} B \) and \( B \xleftarrow{C'} C \).
Definition 3.1.11 (Higher $K$-groups of an essentially small exact category). For a small exact category $A$, we define the $i$-th $K$-group of $A$ by the $i + 1$st homotopy group of $BQ^\ast A$:

$$K_i(A) := \pi_{i+1}(BQ^\ast A)$$

for $i \geq 0$.

For an exact category $A$ which has a set of isomorphism classes of objects, we define

$$K_i(A) := K_i(A')$$

for $i \geq 0$, where $A'$ is a small subcategory equivalent to $A$.

Remark 3.1.12. The above definition is independent of the choice of $A'$. Indeed, if two exact categories $A$ and $A'$ are equivalent then $QA$ and $QA'$ are equivalent. Therefore, if both $A$ and $A'$ are small categories, then $K_i(A) \cong K_i(A')$ for all $i$.

Definition 3.1.13 (Higher $K$-groups of rings). For a ring $R$, we denote $P(R)$ the exact category of finitely generated projective $R$-modules, and define the $i$-th $K$-group $K_i(R)$ by

$$K_i(R) := \pi_{i+1}(BQP(R))$$

for $i \geq 0$.

Example 3.1.14 (Quillen [25]). Consider a finite field $\mathbb{F}_q$ with $q$ elements. We have

$$K_i(\mathbb{F}_q) = \begin{cases} 
\mathbb{Z} & \text{if } i = 0, \\
0 & \text{if } i : \text{even} > 0, \\
\mathbb{Z}/(q^i - 1)\mathbb{Z} & \text{if } i : \text{odd}.
\end{cases}$$

3.2 Lemmas

For a totally real field $L$, $w_m(L)$ denotes the largest integer $n$ so that the Galois group of $L(\mu_n)/L$ is killed by $m$.

Lemma 3.2.1. Let $p$ be a prime number and $\mathbb{B}_n$ the $n$-th layer of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. For each even integer $m \geq 2$, we have

$$w_m(\mathbb{B}_n) = \begin{cases} 
2p^n \prod_{\ell \mid m} \ell^{1+\nu_\ell(m)} & \text{if } p - 1 \mid m, \\
2 \prod_{\ell \mid m} \ell^{1+\nu_\ell(m)} & \text{otherwise}.
\end{cases}$$
Proof. It suffices to consider the Galois groups $\text{Gal}(\mathbb{B}_n(\mu_{\ell^t})/\mathbb{B}_n)$ for each prime $\ell$.

(i) The case when $\ell \neq p$ and $\ell \neq 2$. For any integer $t \geq 1$, we have

$$\text{Gal}(\mathbb{B}_n(\mu_{\ell^t})/\mathbb{B}_n) \cong (\mathbb{Z}/\ell\mathbb{Z})^\times \times \mathbb{Z}/\ell^t - 1 \mathbb{Z}.$$ 

Thus we have

$$v_\ell(w_m(\mathbb{B}_n)) = \begin{cases} 1 + v_\ell(m) & \text{if } \ell - 1 \mid m, \\ 0 & \text{otherwise.} \end{cases}$$

(ii) The case when $\ell \neq p$ and $\ell = 2$. For any integer $t \geq 2$, we have

$$\text{Gal}(\mathbb{B}_n(\mu_{2^t})/\mathbb{B}_n) \cong (\mathbb{Z}/4\mathbb{Z})^\times \times \mathbb{Z}/2^{t-2}\mathbb{Z}.$$ 

Thus we have

$$v_2(w_m(\mathbb{B}_n)) = 2 + v_2(m).$$

(iii) The case when $\ell = p \neq 2$. For any integer $t \geq 1$, we have

$$\text{Gal}(\mathbb{B}_n(\mu_{p^{t+1}})/\mathbb{B}_n) \cong (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}/p^{t-1}\mathbb{Z}.$$ 

Thus we have

$$v_p(w_m(\mathbb{B}_n)) = \begin{cases} n + 1 + v_p(m) & \text{if } p - 1 \mid m, \\ 0 & \text{otherwise.} \end{cases}$$

(iv) The case when $\ell = p = 2$. For any integer $t \geq 2$, we have

$$\text{Gal}(\mathbb{B}_n(\mu_{2^{n+1}})/\mathbb{B}_n) \cong (\mathbb{Z}/4\mathbb{Z})^\times \times \mathbb{Z}/2^{t-2}\mathbb{Z}.$$ 

Thus we have

$$v_2(w_m(\mathbb{B}_{2,n})) = n + 2 + v_2(m).$$

Let $\psi_n$ be a generator of the group of Dirichlet characters associated to $\mathbb{B}_n$. Let $f_n$ be the conductor of $\psi_n$, i.e. $f_n = p^{n+1}$ if $p \geq 3$, and $f_n = 2^{n+2}$ if $p = 2$. For all integers $m \geq 1$ we know that

$$\zeta_{\mathbb{B}_n}(1 - m) = \prod_{\psi \in (\psi_n)} L(1 - m, \psi) = \prod_{\psi \in (\psi_n)} \left( \frac{-B_{m,\psi}}{m} \right), \quad (3.2.1)$$

16
where \( L(s, \psi) \) is the Dirichlet L-function of \( \psi \) and \( B_{m,\psi} \) is the \( m \)th generalized Bernoulli number attached to \( \psi \). These Bernoulli numbers are defined by

\[
\sum_{a=1}^{f_\psi} \psi(a)Xe^{aX}/e^{f_\psi X} - 1 = \sum_{m=0}^{\infty} B_{m,\psi} X^m/m! \in \mathbb{Q}[[X]],
\]

where \( f_\psi \) is the conductor of \( \psi \). We have the functional equation on Dirichlet L-functions

\[
\Gamma(s) \cos \left( \frac{\pi(s - \delta_\psi)}{2} \right) L(s, \psi) = \frac{\tau(\psi)}{2\sqrt{-1}} \frac{(2\pi)^s}{f_\psi} L(1 - s, \overline{\psi}),
\]

where \( \Gamma(s) \) is the Gamma function, \( \psi \) is a nontrivial Dirichlet character of conductor \( f_\psi \), \( \tau(\psi) = \sum_{a=1}^{f_\psi} \psi(a) e^{2\pi \sqrt{-1}/a f_\psi} \) is the Gauss sum,

\[
\delta_\psi = \begin{cases} 
0 & \text{if } \psi \text{ is an even character,} \\
1 & \text{if } \psi \text{ is an odd character.}
\end{cases}
\]

Now we give an evaluation on the complex absolute value of \( B_{m,\psi_n}/m \).

**Lemma 3.2.2.** Let \( m \) be an even integer \( \geq 2 \). For all \( n \geq 1 \) we have

\[
\frac{2}{3} \frac{(m - 1)!}{(2\pi)^m} \sqrt{f_n} m^{-1} \sqrt{f_n} < \left| B_{m,\psi_n}/m \right| < \frac{10}{3} \frac{(m - 1)!}{(2\pi)^m} m^{-1} \sqrt{f_n}.
\]

**Proof.** By the functional equation on Dirichlet L-functions, we have

\[
\left| B_{m,\psi_n}/m \right| = \left| L(1 - m, \psi_n) \right|
\]

\[
= 2 \frac{(m - 1)!}{(2\pi)^m} \sqrt{f_n} \left| L(m, \overline{\psi_n}) \right|.
\]

Thus it is enough to prove that \( \frac{1}{3} \) \( < \left| L(m, \overline{\psi_n}) \right| \) \( < \frac{5}{3} \). This follows from the following evaluation;

\[
\left| L(m, \overline{\psi_n}) - 1 \right| = \left| \sum_{a=2}^{\infty} \frac{\overline{\psi_n}(a)}{a^m} \right|
\]

\[
\leq \sum_{a=2}^{\infty} \frac{1}{a^2} = \frac{\pi^2}{6} - 1 < \frac{2}{3}.
\]

\[ \square \]
Next we give an evaluation on the $\ell$-adic valuation of $\frac{1}{2} B_{m, \psi_n}/m$. We use a congruence on $\ell$-adic $L$-functions, which follows from the Taylor expansion of $L_\ell(s, \chi)$; for a nontrivial Dirichlet character $\chi$ whose conductor $f_\chi$ is not divisible by $\ell^2$ if $\ell \geq 3$, by $2^3$ if $\ell = 2$, we have

$$\frac{1}{2} L_\ell(1 - m, \chi) \equiv \frac{1}{2} L_\ell(1 - m', \chi) \pmod{\ell}$$

for all integers $m, m' \geq 1$ and both sides are $\ell$-integral ([37, Corollary 5.13]).

**Lemma 3.2.3.** Let $m$ be an even integer $\geq 2$. For each prime number $\ell \neq p$,

$$v_\ell \left( \frac{1}{2} B_{m, \psi_n} \right) = 0 \quad \text{for large enough } n > 0.$$

**Proof.** We know that

$$L_\ell(1 - m, \psi_n \omega_\ell^m) = -(1 - \psi_n(\ell)^{m-1}) \frac{B_{m, \psi_n}}{m},$$

$$L_\ell(0, \psi_n \omega_\ell^m) = -(1 - \psi_n \omega_\ell^{m-1}(\ell)) B_{1, \psi_n \omega_\ell^{m-1}}.$$

(i) the case when $p = 2$.

Since $\ell \neq 2$, $\ell^2$ does not divide $f_{\psi_n \omega_\ell^m} = 2^{n+2} \ell$ which is the conductor of $\psi_n \omega_\ell^m$. Hence we have a congruence on $\ell$-adic $L$-functions

$$\frac{1}{2} L_\ell(1 - m, \psi_n \omega_\ell^m) \equiv \frac{1}{2} L_\ell(0, \psi_n \omega_\ell^m) \pmod{\ell}.$$ 

Here we note that $\ell - 1$ does not divide $m - 1$. In fact, $\ell - 1$ is an even integer, on the other hand, $m - 1$ is an odd integer. This means that $\psi_n \omega_\ell^{m-1}(\ell) = 0$. Thus we have

$$\frac{1}{2} B_{m, \psi_n} \equiv \frac{1}{2} B_{1, \psi_n \omega_\ell^{m-1}} \pmod{\ell}.$$ 

Therefore

$$v_\ell \left( \frac{1}{2} B_{m, \psi_n} \right) = 0 \iff v_\ell \left( \frac{1}{2} B_{1, \psi_n \omega_\ell^{m-1}} \right) = 0.$$ 

By Washington’s result [39], we have $v_\ell \left( \frac{1}{2} B_{1, \psi_n \omega_\ell^{m-1}} \right) = 0$ for $n$ large enough, and hence we get the conclusion.

(ii) the case when $p \geq 3$. 

18
For an odd prime $\ell$, $\ell^2$ does not divide $f_{\psi_n\omega_\ell^m} = \ell p^{n+1}$, and for the prime $2 (\equiv \ell)$, $2^i$ does not divide $f_{\psi_n\omega_2^m} = f_{\psi_n} = p^{n+1}$ since $m$ is an even integer. Hence we have a congruence on $\ell$-adic $L$-functions

$$\frac{1}{2}L_\ell(1-m, \psi_n\omega_\ell^m) \equiv \frac{1}{2}L_\ell(0, \psi_n\omega_\ell^m) \pmod{\ell}.$$ 

Here we note that $\ell - 1$ does not divide $m - 1$ as in the case (i) if $\ell$ is an odd prime. If $\ell = 2$, then $\omega_2^{m-1} = \omega_2$. In any case, we have $\psi_n\omega_\ell^m(\ell) = 0$. Thus we have

$$\frac{1}{2}B_{m,\psi_n} \equiv \frac{1}{2}B_{1,\psi_n\omega_\ell^{m-1}} \pmod{\ell}.$$ 

Therefore

$$v_\ell\left(\frac{1}{2}B_{m,\psi_n}\right) = 0 \iff v_\ell\left(\frac{1}{2}B_{1,\psi_n\omega_\ell^{m-1}}\right) = 0.$$ 

By Washington’s result [39], we have $v_\ell(\frac{1}{2}B_{1,\psi_n\omega_\ell^{m-1}}) = 0$ for $n$ large enough, and we get the conclusion. \qed

**Remark 3.2.4.** The above result on $v_\ell(\frac{1}{2}B_{m,\psi_n}/m)$ can also be proved by using gamma transforms of appropriate rational function measures in [30]. Indeed, let $m$ be an even integer $\geq 2$, $g$ any integer and put

$$R_m(X) = \left(X \frac{d}{dX}\right)^{m-1} \left(\sum_{a=1}^{g}X^a\right) \pmod{\ell} \in \mathbb{Q}_\ell(X),$$

where the right-hand side is independent of the choice of $g$. The integer $g$ will be taken sufficiently large in the proof for technical reason.

Let $\alpha_m$ be a $\mathbb{Q}_\ell$-valued rational function measure on $\mathbb{Z}_p$ whose associated rational function is $R_m$. The $\Gamma$-transform of $\alpha_m$ is the function of characters $\psi$ on $\mathbb{Z}_p^\times$ of the second kind for $p$ defined by

$$\Gamma_{\alpha_m}(\psi) = \int_{\mathbb{Z}_p^\times} \psi(x)d\alpha_m(x).$$

By the same method as in the proof of [30, Proposition 4.1], we have

$$\Gamma_{\alpha_m}(\psi) = L(p)(1 - m, \psi)$$

for all but finitely many Dirichlet characters $\psi$ of the second kind for $p$. Then [30, Remark after Theorem 3.1] implies that

$$v_\ell\left(\frac{1}{2}L(1-m, \psi)\right) = v_\ell\left(\frac{1}{2}L(p)(1 - m, \psi)\right) = 0.$$
for all but finitely many $\psi$ of the second kind for $p$. Here the first equality holds since $\psi(p) = 0$ for all but finitely many $\psi$ and thus the Euler factor $1 - \psi(p)p^{-1+m} = 1$.

**Lemma 3.2.5.** For $n > 0$ large enough, we have $v_2(B_m,\psi_n/m) < 1$.

*Proof.* At first, we show that for any odd integers $a, b \in \mathbb{Z}$, 

$$\psi_n(b) = \psi_n(a) \iff b \equiv a, 2^{n+2} - a \pmod{2^{n+2}}.$$ 

Assume that $\psi_n(b) = \psi_n(a)$ and $b \not\equiv a \pmod{2^{n+2}}$. As $a, b \in (\mathbb{Z}/2^{n+2}\mathbb{Z})^\times = (-1, 5)$, we can write them uniquely as $a \equiv (-1)^{x_a}5^{y_a}, b \equiv (-1)^{x_b}5^{y_b} \pmod{2^{n+2}}$ for some integers $x_a, x_b, y_a, y_b$ satisfying $0 \leq x_a, x_b \leq 1, 0 \leq y_a, y_b \leq 2^n - 1$. Then we have $\zeta_{2n}^{y_b} = \psi_n(b) = \psi_n(a) = \zeta_{2n}^{y_a}$ and thus we get $y_b = y_a$.

By our assumption, we may assume $x_a = 0$ and $x_b = 1$. Therefore we get $b \equiv -5^{y_b} \equiv -a \pmod{2^{n+2}}$.

Next, we show that for any odd integers $a, b \in \mathbb{Z}$,

$$\psi_n(b) = -\psi_n(a) \iff b \equiv 2^{n+1} + a, 2^{n+1} - a \pmod{2^{n+2}}.$$ 

Assume that $\psi_n(b) = -\psi_n(a)$. Let $x_a, x_b, y_a, y_b$ be integers as above. Then we see $y_b \equiv 2^{n-1} + y_a \pmod{2^n}$. Thus we have $b \equiv (-1)^{x_a}5^{2^{n-1}}a \pmod{2^{n+2}}$. Note that we have $5^{2^{n-1}} \equiv 2^{n+1} + 1 \pmod{2^{n+2}}$. Since $a$ is an odd integer, we get $b \equiv 2^{n+1}a + a \equiv 2^{n+1} + a \pmod{2^{n+2}}$ if $x_a = x_b$, and $b \equiv -2^{n+1}a - a \equiv 2^{n+1} - a \pmod{2^{n+2}}$ if $x_a \not= x_b$.

Put $x = 2^n$. Then we have

$$\sum_{a=1}^{2^n} a^i\psi_n(a) = \sum_{a=1}^{2^n} (a^i - (x - a)^i - (x + a)^i + (2x - a)^i) \psi_n(a).$$ 

Note that $\{\psi_n(a) \mid 1 \leq a \leq 2^n, a: \text{odd}\}$ is a basis of the ring of integers
\[ Z[\zeta_{2^n}] \text{. For each even integer } i > 0, \text{ we have} \]
\[ a^i - (x - a)^i - (x + a)^i + (2x - a)^i \]
\[ = a^i - \sum_{j=0}^{i} \binom{i}{i-j} x^j (-a)^{i-j} - \sum_{j=0}^{i} \binom{i}{i-j} x^j a^{i-j} \]
\[ + \sum_{j=0}^{i} \binom{i}{i-j} (2x)^j (-a)^{i-j} \]
\[ = \left( -\sum_{j=1}^{i} \binom{i}{i-j} x^j (-a)^{i-j} - \sum_{j=1}^{i} \binom{i}{i-j} x^j a^{i-j} \right) \]
\[ + \sum_{j=1}^{i} \binom{i}{i-j} (2x)^j (-a)^{i-j} \]
\[ = -2 \sum_{j=1}^{i} \binom{i}{i-j} x^j a^{i-j} \]
\[ + \sum_{j=1}^{i} \binom{i}{i-j} (2x)^j a^{i-j} - \sum_{j=2}^{i} \binom{i}{i-j} (2x)^j a^{i-j} \]
\[ = \sum_{j=2}^{i} \binom{i}{i-j} (-2 + 2^j) x^j a^{i-j} - \sum_{j=2}^{i} \binom{i}{i-j} (2x)^j a^{i-j} - i \cdot 2x \cdot a^{i-1} \]
\[ = 2x^2 \left( \sum_{j=2}^{i} \binom{i}{i-j} (-1 + 2^{j-1}) x^j a^{i-j} - \sum_{j=2}^{i} 2(2x)^{j-2} \binom{i}{i-j} a^{i-j} \right) \]
\[ - 2xia^{i-1}. \]

Thus we have
\[ \sum_{a=1}^{2^n} (a^i - (x - a)^i - (x + a)^i + (2x - a)^i) \psi_n(a) \]
\[ \equiv \sum_{a=1}^{2^n} (-2xia^{i-1}) \psi_n(a) \not\equiv 0 \pmod{2^{n+3+\nu_2(i)}} \]

21
for every $n$ such that $n + 1 = v_2(x) ≥ 1 + v_2(i)$.

Finally, we claim that for $n$ large enough we have

$$v_2(B_{m, \psi_n}) = v_2 \left( \frac{1}{f_n} \sum_{a=1}^{f_n} a^m \psi_n(a) \right) < 1 + v_2(m) \quad (3.2.2)$$

and thus $v_2(B_{m, \psi_n}/m) < 1$. In fact, for $i = 2, 4, \ldots, m - 2$ we have

$$v_2 \left( \binom{m}{i} B_{m-i} \sum_{a=1}^{f_n} a^i \psi_n(a) \right) \geq 2(n + 2) + 0 - 1 + (n + 2 + v_2(i)) = 3n + 5 + v_2(i).$$

For $i = m - 1$, we note that

$$0 = f_n B_{m-1, \psi_n} = \sum_{j=1}^{m-1} \binom{m-1}{j} B_{m-1-j} \sum_{a=1}^{f_n} a^j \psi_n(a)$$

since $\psi_n$ is an even character. Thus we have

$$v_2 \left( \binom{m}{m-1} B_1 \sum_{a=1}^{f_n} a^{m-1} \psi_n(a) \right) = v_2 \left( \binom{m}{m-1} B_1 \left( - \sum_{j=1}^{m-2} \binom{m-1-j}{j} B_{m-1-j} \sum_{a=1}^{f_n} a^j \psi_n(a) \right) \right) \geq (n + 2) + 1 - 1 + ((n + 2) + 0 - 1 + 0) = 2n + 3.$$

For $i = m$, we have

$$v_2 \left( \sum_{a=1}^{f_n} a^m \psi_n(a) \right) < n + 3 + v_2(m).$$

Therefore we get the conclusion (3.2.2).

\[ \square \]

3.3 The orders of even $K$-groups

Let $\psi_n$ be as in the previous section. Let $h_n = \#K_{2m-2}(O_{B_n})$. The work of Voevodsky and Rost on the Bloch–Kato Conjecture in [36] implies that there are isomorphisms up to finite 2-torsion:

$$K_{2m-2}(O_{B_n}) \cong H^2_{m, 2}(O_{B_n}, \mathbb{Z}(m)),$$
where the right hand side denotes the motivic cohomology of $\text{Spec}(\mathcal{O}_{\mathbb{B}_n})$. The deviation between $K$-theory and motivic cohomology depends on $m \mod 8$ and is known by work of Rognes–Weibel (cf. [28]). Since $\mathbb{B}_n$ is totally real, the Iwasawa Main Conjecture, which was proved by Wiles [41] for odd $p$ and for $p = 2$ in case of an abelian field, implies that for any even number $m \geq 2$

$$\zeta_{\mathbb{B}_n}(1 - m) = \pm \frac{\# H^2_{\text{mot}}(\mathcal{O}_{\mathbb{B}_n}, \mathbb{Z}(m))}{w_m(\mathbb{B}_n)}.$$ 

Thus we have $h_n = \pm 2^{b_n} w_m(\mathbb{B}_n) \zeta_{\mathbb{B}_n}(1 - m)$ for some integer $b_n$. By Lemma 3.2.1 and (3.2.1), we have

$$\frac{h_n}{h_{n-1}} = 2^{b_n} \times p^{\delta_p} \times \prod_{\sigma \in \text{Gal}(\mathbb{Q}(\zeta_{n^p})/\mathbb{Q})} \left| - \frac{B_m \phi_{\sigma}}{m} \right|,$$

where $b_n = b_n - b_{n-1}$,

$$\delta_p = \begin{cases} 1 & \text{if } p - 1 | m, \\ 0 & \text{otherwise}. \end{cases}$$

We define $c_n = v_p \left( \frac{h_n}{h_{n-1}} \right)$.

Now we give an asymptotic formula for $c_n$ by Iwasawa theory when $p$ is odd. Let $A_{\mathbb{Q}(\mu_{p^{n+1}})}$ be the $p$-Sylow subgroup of the ideal class group of the CM field $\mathbb{Q}(\mu_{p^{n+1}})$ and $\mathcal{X} = \lim \sup_{n \to \infty} A_{\mathbb{Q}(\mu_{p^{n+1}})}$. Let $\omega$ be the Teichmüller character for $\Delta = \text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$, i.e. for $a \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$, $\omega(a)$ is defined to be a $(p - 1)$th root of unity such that $a \equiv \omega(a) \pmod{p}$. Let $\mathcal{X}^\omega$ be the submodule of $\mathcal{X}$ on which each $\sigma \in \Delta$ acts by $\omega^i(\sigma)$.

**Proposition 3.3.1.** If $p$ is odd, then we have $c_n = \lambda$ for $n$ large enough, where $\lambda$ is the Iwasawa $\lambda$-invariant $\lambda(\mathcal{X}^\omega |_{\mathcal{X}})$.

**Proof.** We show that there exist constants $\lambda$ and $\nu$ so that $v_p(h_n) = \lambda n + \nu$ for $n$ large enough.

Let $\mathcal{X}^-$ be the submodule of $\mathcal{X}$ on which complex conjugation acts by $-1$. The Quillen–Lichtenbaum Conjecture, which now is a theorem due to Voevodsky and Rost [36], implies that $K_{2m-2}(\mathcal{O}_{\mathbb{B}_n}) \otimes \mathbb{Z}_p$ is isomorphic to $H^2_b(\text{Spec}(\mathcal{O}_{\mathbb{B}_n}[1/p]), \mathbb{Z}_p(m))$ for each $n$ (cf. [31]), and the étale cohomology is isomorphic to the Pontryagin dual of the Galois coinvariant of $\mathcal{X}^- \otimes \mathbb{Z}_p(m-1)$ (cf. [3], [20]). Therefore we have isomorphisms of groups

$$K_{2m-2}(\mathcal{O}_{\mathbb{B}_n}) \otimes \mathbb{Z}_p \cong (\mathcal{X}^- \otimes \mathbb{Z}_p(m-1))^{\text{Gal}(\mathbb{B}_{\infty}/\mathbb{B}_n)}$$

and we know that $(\mathcal{X}^- \otimes \mathbb{Z}_p(m-1))^{\text{Gal}(\mathbb{B}_{\infty}(\mu_p)/\mathbb{B}_n)} = (\mathcal{X}^\omega |_{\mathcal{X}})^{\text{Gal}(\mathbb{B}_{\infty}/\mathbb{B}_n)}$. Note that the Iwasawa $\mu$-invariant $\mu(\mathbb{Q}(\mu_p))$ is 0. Thus we get the conclusion from the Iwasawa theory on ideal class groups. \qed

23
Next we will give an upper bound on $c_n$ when $p = 2$. By definition, we have

$$B_{m, \psi_n} = \frac{1}{f_n} \sum_{i=1}^{m} \left( f_n^{m-i} \cdot \binom{m}{i} \cdot B_{m-i} \sum_{a=1}^{f_n} a^i \psi_n(a) \right),$$

where $B_{m-i}$ are the Bernoulli numbers.

**Proposition 3.3.2.** $c_n < b'_n + 1 + \phi(2^n)$ where $\phi$ is the Euler function.

**Proof.** This follows from Lemma 3.2.5. \qed

Finally we prove the main theorem.

**Theorem 3.3.3.** Let $m$ be an even number $\geq 2$. Let $p$ be a prime number. Let $B_{\infty}/\mathbb{Q}$ be the cyclotomic $\mathbb{Z}_p$-extension and $B_n$ the $n$-th layer. Let $h_n = \#K_{2m-2}(\mathcal{O}_{B_n})$. Then for each $m \geq 2$ and all $p$

$$\{h_n \mid n \in \mathbb{Z}_{\geq 0}\} \text{ is unbounded.}$$

Furthermore, for any even number $m \geq 2$ and each prime $p$, there are infinitely many prime numbers which divide $h_n$ for some $n \in \mathbb{Z}_{\geq 0}$, i.e.

$$\#\{\ell : \text{prime number} \mid \text{there exists } n \in \mathbb{Z}_{\geq 0} \text{ such that } \ell|h_n\} = \infty.$$

**Proof.** To prove the former statement, we show that the quotient $h_n/h_{n-1}$ tends to infinity as $n \to \infty$.

By (3.3.1) and Lemma 3.2.2, we have

$$\frac{h_n}{h_{n-1}} = 2^{b'_n} \times p^{\delta_p} \times \prod_{\sigma \in \text{Gal}(\mathbb{Q}(\zeta_p^n)/\mathbb{Q})} \left| -\frac{B_{m, \psi_n^\sigma}}{m} \right| \geq 2^{b'_n} p^{\delta_p} \left( \frac{2}{3} \frac{(m-1)!}{(2\pi)^m} f_n^{m-1} \sqrt{f_n} \right)^{\phi(p^n)} \to \infty \ (n \to \infty),$$

where $\delta_p = 1$ if $p - 1|m$ and otherwise $\delta_p = 0$.

We show the latter statement, namely the existence of infinitely many prime numbers which divide $h_n$ for some $n$.

We first consider the case when $p > 2$. Assume that there are only finitely many prime numbers which divide $h_n$ for some $n$, i.e.

$$\{\ell : \text{prime number} \mid \text{there exists } n \in \mathbb{Z}_{\geq 0} \text{ such that } \ell|h_n\} = \{\ell_1, \ldots, \ell_r\}$$

for some integer $r$. For each $\ell_i \neq 2, p$, there exists an integer $N(\ell_i)$ such that $\ell_i$ does not divide $h_n/h_{n-1}$ for every $n > N(\ell_i)$ by Lemma 3.2.3. Hence by
the finiteness of \( \ell_i' \)'s, there exists an integer \( N_0 \) such that \( \ell_i \) except for 2 and \( p \) does not divide \( h_n / h_{n-1} \) for every \( n > N_0 \) and for every \( i \). For the prime 2, there exists an integer \( N_1 \) such that \( v_2(h_n / h_{n-1}) = b'_n + \phi(p^n)v_2(B_{m,\psi_n} / m) = b'_n + \phi(p^n) \) for every \( n > N_1 \) by Lemma 3.2.3. Furthermore, we know that there exist a constant \( \lambda \) and an integer \( N_2 \) such that \( c_n = v_p(h_n / h_{n-1}) = \lambda \) for every \( n > N_2 \) by Proposition 3.3.1. Thus we have

\[
\frac{h_n}{h_{n-1}} = 2^{b'_n} 2^{\phi(p^n)} p^{\alpha_n} = 2^{b'_n} 2^{\phi(p^n)} p^\lambda
\]

for every \( n > \max(N_0, N_1, N_2) \). On the other hand we have

\[
\frac{h_n}{h_{n-1}} \geq 2^{b'_n} p^{\delta_p} \left( \frac{2(m-1)!}{3(2\pi)^m} f_{n-1}^{m-1} \sqrt{f_n} \right)^{\phi(p^n)}
\]

\[
> 2^{b'_n} f_{n}^{(m-1)\phi(p^n)}
\]

for \( n \) large enough as in the proof of the former statement. Since \( f_n = p^{n+1} \), we have

\[
2^{\phi(p^n)} > p^{(m-1)(n+1)\phi(p^n) - \lambda}
\]

for \( n \) large enough. This is a contradiction.

Next we study the case when \( p = 2 \). By the same method as above, we see that \( h_n / h_{n-1} \) is a power of 2 for \( n \) large enough. Thus, we have

\[
\frac{h_n}{h_{n-1}} = 2^{c_n} < 2^{b'_n} \cdot 2^{1+\phi(2^n)}
\]

for \( n \) large enough by Proposition 3.3.2. On the other hand we have

\[
\frac{h_n}{h_{n-1}} \geq 2^{b'_n} \cdot 2 \left( \frac{2(m-1)!}{3(2\pi)^m} f_{n-1}^{m-1} \sqrt{f_n} \right)^{\phi(2^n)}
\]

\[
> 2^{b'_n} \cdot 2 \cdot f_{n}^{(m-1)\phi(2^n)}
\]

for \( n \) large enough as in the proof of the former statement. Since \( f_n = 2^{n+2} \), we have

\[
2^{1+\phi(2^n)} > 2^{1+(m-1)(n+2)\phi(2^n)}
\]

for \( n \) large enough. This is a contradiction.
Chapter 4

The plus and the minus Selmer groups

In this chapter, we study the $\Lambda$-module structure of the plus and the minus Selmer groups $\text{Sel}^\pm(F_\infty, E[p^\infty])^\vee$. In §4.1, we define the plus and the minus Selmer groups following Shin-ichi Kobayashi, and fix a global setting. In §4.2, we study the $\Lambda$-module structure of the plus and the minus local conditions $(E^\pm(k_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\vee$ in a local setting. In §4.3, we first prove that the classical $p$-primary Selmer group $\text{Sel}(F_\infty, E[p^\infty])^\vee$ has no nontrivial finite $\Lambda$-submodules (Theorem 4.3.5) under our setting. Finally, we prove that the plus and the minus Selmer groups $\text{Sel}^\pm(F_\infty, E[p^\infty])^\vee$ also have no nontrivial finite $\Lambda$-submodules (Theorem 4.3.8).

4.1 Definitions

Let $p$ be a prime number, $F$ a finite extension of $\mathbb{Q}$, and $E$ an elliptic curve defined over $F$. For a finite extension $L/F$, the $p$-primary Selmer group for $E$ over $L$ is defined by

$$\text{Sel}(L, E[p^\infty]) := \text{Ker}\left( H^1(L, E[p^\infty]) \rightarrow \prod_v \frac{H^1(L_v, E[p^\infty])}{E(L_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right),$$

where $v$ runs through all the places of $L$, $L_v$ is the completion of $L$ at the place $v$, and $E(L_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ is regarded as a subgroup of $H^1(L_v, E[p^\infty])$ by the Kummer map. For a number field $L$ which is an infinite extension of $F$, we define the $p$-primary Selmer group for $E$ over $L$ by

$$\text{Sel}(L, E[p^\infty]) := \varprojlim_{L'} \text{Sel}(L', E[p^\infty]),$$
where \( L' \) runs through all the subfields of \( L \) that are finite extensions of \( F \), and the transition maps are restriction maps between the cohomology groups.

We denote \( F_n = F(\mu_{p^n}) \), \( F_{-1} = F \) and \( F_\infty = \bigcup_n F_n \), where \( \mu_{p^n} \) denotes the group of \( p^n \)-th roots of unity. We fix a generator \((\zeta_{p^n})\) of \( \mathbb{Z}_p(1) \), namely, for each \( n \geq 0 \), \( \zeta_{p^n} \) is a primitive \( p^n \)-th root of unity such that \( \zeta_{p^n+1}^{p^n} = \zeta_{p^n} \).

Then by definition, we have

\[
\text{Sel}(F_\infty, E[p^\infty]) = \lim_{\to n} \text{Sel}(F_n, E[p^\infty]).
\]

Throughout this thesis, we fix the following notations:

- \( p \) is an odd prime number,
- \( F \) is a finite extension of \( \mathbb{Q} \),
- \( E \) is an elliptic curve defined over a subfield \( F' \) of \( F \).

Denote \( S_{p}^{ss} \) the set of all primes of \( F' \) lying above \( p \) where \( E \) has supersingular reduction.

Throughout this thesis, we assume the following:

- any prime \( w \in S_{p}^{ss} \) is unramified in \( F \),
- \( F'_w = \mathbb{Q}_p \) for any prime \( w \in S_{p}^{ss} \), where \( F'_w \) is the completion of \( F' \) at the prime \( w \),
- \( E \) has good reduction at any prime \( w|p \) of \( F' \),
- \( S_{p}^{ss} \) is nonempty, and
- \( a_w = 1 + N_{F'/\mathbb{Q}}(w) - \#\tilde{E}_w(F_w) = 0 \) for any prime \( w \in S_{p}^{ss} \), where \( N_{F'/\mathbb{Q}} \) is the norm for \( F'/\mathbb{Q} \), \( \tilde{E}_w \) is the reduction of \( E \) at \( w \), and \( F_w \) is the residue field of \( F' \) at \( w \).

When \( p \geq 5 \), the condition \( a_w = 0 \) is automatically satisfied since we have \( p|a_w \) and \( |a_w| \leq 2\sqrt{p} \).

Denote \( S_{p,F}^{ss} \) the set of all primes of \( F \) lying above \( S_{p}^{ss} \).

Following Shin-ichi Kobayashi [17] we define subgroups \( E^+(F_{n,v}) \) and \( E^-(F_{n,v}) \) of \( E(F_{n,v}) \) for each prime \( v \in S_{p,F}^{ss} \), and define plus and minus Selmer groups \( \text{Sel}^+(F_n, E[p^\infty]) \), \( \text{Sel}^-(F_\infty, E[p^\infty]) \) as the following (see also [11] and [14]).
**Definition 4.1.1.** (1) For a prime \( v \in S_{p,E} \) and \( n \geq -1 \), let \( F_{n,v} \) be the completion of \( F_n \) at the unique prime of \( F_n \) lying above \( v \). We define

\[
E^+(F_{n,v}) = \left\{ P \in E(F_{n,v}) \mid \text{Tr}_{n/m+1} P \in E(F_{m,v}) \right\},
\]

\[
E^-(F_{n,v}) = \left\{ P \in E(F_{n,v}) \mid \text{Tr}_{n/m+1} P \in E(F_{m,v}) \right\},
\]

where \( \text{Tr}_{n/m+1} : E(F_{n,v}) \to E(F_{m+1,v}) \) is the trace map.

(2) The plus and the minus Selmer groups are defined by

\[
\text{Sel}^+(F_n, E[p^\infty]) := \text{Ker} \left( \text{Sel}(F_n, E[p^\infty]) \to \bigoplus_{v \in S_{p,E}} H^1(F_{n,v}, E[p^\infty]) \right),
\]

\[
\text{Sel}^-(F_n, E[p^\infty]) := \lim_{\to n}\text{Sel}^+(F_n, E[p^\infty]).
\]

We denote the Pontryagin dual of a module \( M \) by \( M^\vee \). Let \( \mathcal{G}_n = \text{Gal}(F_n/F) \) and \( \mathcal{G}_\infty = \text{Gal}(F_\infty/F) \). Then the group ring \( \mathbb{Z}_p[\mathcal{G}_n] \) acts naturally on \( \text{Sel}^+(F_n, E[p^\infty])^\vee \) and the completed group ring \( \Lambda(\mathcal{G}_\infty) := \Lambda[\mathcal{G}_\infty] \) on \( \text{Sel}^+(F_\infty, E[p^\infty])^\vee \).

The Pontryagin dual of the usual \( p \)-primary Selmer group \( \text{Sel}(F_\infty, E[p^\infty])^\vee \) is not a torsion \( \Lambda(\mathcal{G}_\infty) \)-module, however, \( \text{Sel}^+(F_\infty, E[p^\infty])^\vee \) are known to be \( \Lambda(\mathcal{G}_\infty) \)-torsion in the case when \( F = \mathbb{Q} \) (cf. [17] Theorem 2.2).

In this thesis, we study the \( \Lambda \)-module \( \text{Sel}^+(F_\infty, E[p^\infty])^\vee \) in our setting, where \( \Lambda = \mathbb{Z}_p[[\text{Gal}(F_\infty/F_0)]] \). In the following we also assume that

- both \( \text{Sel}^+(F_\infty, E[p^\infty])^\vee \) are \( \Lambda \)-torsion.

### 4.2 The formal groups and the norm subgroups

In this section we study the local conditions of the plus and the minus Selmer groups defined in the previous section. The problem is completely in local setting, and thus we use the following local setting unless otherwise specified.

Let \( E/\mathbb{Q}_p \) be an elliptic curve with \( a_p = 0 \), and \( \hat{E} \) the formal group defined over \( \mathbb{Z}_p \) associated with the minimal model of \( E \) over \( \mathbb{Q}_p \). Let \( k \) be a finite unramified extension of \( \mathbb{Q}_p \) of degree \( d = [k : \mathbb{Q}_p] \), and \( \mathcal{O}_k \) the ring of integers of \( k \). For each \( n \geq -1 \), let \( k_n = k(\mu_{p^{n+1}}) \), and \( \mathfrak{m}_n \) be the maximal ideal of \( k_n \). Let \( k_\infty = \bigcup_{n \geq -1} k_n \), and \( \mathfrak{m}_\infty = \bigcup_{n \geq -1} \mathfrak{m}_n \). Let \( G_n = \text{Gal}(k_n/\mathbb{Q}_p) \), \( G_\infty = \text{Gal}(k_\infty/\mathbb{Q}_p) \), \( \Gamma_n = \text{Gal}(k_\infty/k_n) \), \( \Gamma = \Gamma_0 (= \text{Gal}(k_\infty/k_0)) \), and \( \Delta = \)
Gal(\(k(\mu_p)/k\)) = Gal(\(k_0/k_{-1}\)). Let \(\phi\) be the Frobenius map of Gal(\(k/Q_p\)) = \(G_{-1}\) characterized by \(x^p \equiv x^p \mod pO_k\). We denote \(\Lambda = \mathbb{Z}_p[[\Gamma]]\). We fix a topological generator \(\gamma \in \Gamma\). Then we identify \(\mathbb{Z}_p[[\Gamma]]\) with \(\mathbb{Z}_p[[X]]\), and \(\mathbb{Z}_p[[G_\infty]]\) with \(\mathbb{Z}_p[G_0][[X]]\) by identifying \(\gamma \) with \(1 + X\).

### 4.2.1 Honda’s theory

In this subsection we recall Honda’s theory of formal groups. We restrict ourselves to one-dimensional commutative formal groups defined over \(O_k\).

Let \(k_\phi[[T]]\) (resp. \(O_{k,\phi}[[T]]\)) be the non-commutative power series ring on \(T\) with the multiplication rule: \(T\alpha = \alpha \phi T\) for \(\alpha \in k\) (resp. \(\alpha \in O_k\)). We define an \(O_k\)-submodule \(P\) of the (commutative) power series ring \(k[[X]]\) by:

\[
P = \left\{ f(X) = \sum_{i=0}^{\infty} a_i X^i \in k[[X]] \left| \begin{array}{c} ia_i \in O_k \text{ for } i \geq 0, f(0) \in pO_k \end{array} \right. \right\}.
\]

For \(u = \sum_{i=0}^{\infty} b_i T^i \in O_{k,\phi}[[T]]\) and \(f \in P\), we define an element \(u * f \in P\) by:

\[
(u * f)(X) = \sum_{i=0}^{\infty} b_i f^{\phi^i}(X^p),
\]

where the superscript \(\phi^i\) of \(f\) means that we apply \(\phi^i\) to the coefficients of the power series \(f\). We can check that \(P\) is a left \(O_{k,\phi}[[T]]\)-module by the action \(*\).

**Definition 4.2.1.** An element \(u = u(T) \in O_{k,\phi}[[T]]\) is said to be special if \(u \equiv p \mod \deg 1\). Let \(u\) be a special element of \(O_{k,\phi}[[T]]\). An element \(f \in P\) is said to be of Honda type \(u\), if \(f\) satisfies the following two conditions:

\[
\begin{align*}
(i) & \quad f(X) \equiv \alpha X \mod \deg 2 \text{ for some } \alpha \in O_k^\times, \\
(ii) & \quad (u * f)(X) \equiv 0 \mod pO_k[[X]].
\end{align*}
\]

For a one-dimensional formal group \(\mathcal{F}\) defined over \(\mathbb{Z}_p\), we denote the formal logarithm by \(\log_{\mathcal{F}}\) and the formal exponential by \(\exp_{\mathcal{F}}\). We remark that \(\log_{\mathcal{F}}(X) \in P\).

**Theorem 4.2.2** (Honda).

\[
\begin{align*}
(i) & \quad \text{Let } \mathcal{F} \text{ be a formal group of dimension 1 defined over } O_k. \text{ Then there exists a unique Eisenstein polynomial } u = u(T) \in O_k[T] \text{ such that } \\
& \quad \log_{\mathcal{F}}(X) \in P \text{ is of the Honda type } u.
\end{align*}
\]
(ii) Let $F$ and $G$ be formal groups defined over $\mathcal{O}_k$ of dimension 1 whose logarithms are of the same Honda type $u$. Then $\exp_F \circ \log_G(X)$ is an element of $\mathcal{O}_k[[X]]$ and gives an isomorphism $F \simeq G$.

(iii) Let $u$ be an Eisenstein polynomial. Then there exist an element of $\mathcal{P}$ of the Honda type $u$. If $f \in \mathcal{P}$ is of the Honda type $u$, there exists a formal group defined over $\mathcal{O}_k$ with the logarithm $f$.

Proof. See [9] Theorem 2, 4, and Proposition 2.6 and 3.5.

4.2.2 The formal groups associated to $E$

In this subsection we introduce a system of local points $(d_n)_n$ which is intrinsically same with Byoung Du Kim’s one, and study $\hat{E}(m_n)$ for all $n$. The goal of this subsection is to describe the $\mathbb{Z}_p[G_n]$-modules $\hat{E}(m_n)$ in terms of the system of local points $(d_n)_n$.

**Proposition 4.2.3.** For any $n$, $\hat{E}(m_n)$ is $\mathbb{Z}_p$-torsion-free.

**Proof.** We can prove this by the same method as the proof of [17] Proposition 8.7.

The above proposition implies that the formal logarithm $\log_{\hat{E}}(X)$ induces an injective homomorphism $\log_{\hat{E}} : \hat{E}(m_n) \to k_n$ for all $n$, since the kernel of the logarithm of a formal group precisely consists of the elements of finite order.

For such a one-dimensional formal group $\mathcal{F}$ defined over $\mathbb{Z}_p$ with height 2, the formal logarithm $\log_{\mathcal{F}}$ induces isomorphisms as in the following proposition (cf. The proof of Proposition 2.1 in [19], and Lemma 2.4 in [8]).

**Proposition 4.2.4.** Let $\mathcal{F}$ be a one-dimensional formal group defined over $\mathbb{Z}_p$ with height 2. For a finite extension $L/\mathbb{Q}_p$, denote by $m_L$ its maximal ideal. Then the logarithm $\log_{\mathcal{F}} : \mathcal{F}(m_L) \to L$ induces isomorphisms

$$\log_{\mathcal{F}} : \mathcal{F}(m^j_L) \xrightarrow{\sim} m^j_L$$

for all $j > v_L(p)/(p^2 - 1)$, where $v_L$ is the normalized valuation of $L$ so that $v_L(\pi_L) = 1$ for a uniformizer $\pi_L$ of $L$.

Following [11] and [14] we construct a system of local points $(d_n)_n$.

Fix a generator $\zeta$ of the group of roots of unity in $k$. Then $\zeta$ is a primitive $(p^d - 1)$th root of unity, and we have $k = \mathbb{Q}_p(\zeta)$.
Let \( g(X) = (X + \zeta)^p - \zeta^p \in \mathcal{O}_k[X] \), \( g^{(m)}(X) = g^{m-1} \circ g^{m-2} \circ \cdots \circ g(X) = (X + \zeta)^{p^m} - \zeta^{p^m} \) for \( m \geq 1 \) and \( g^{(0)}(X) = X \). We define a formal power series \( \log g(X) \) by

\[
\log g(X) = \sum_{m=0}^{\infty} (-1)^m \frac{g^{(2m)}(X)}{p^{mn}}.
\]

We can check that

\[
(\log g)^{(n+1)}(X) = \sum_{i=1}^{\infty} (-1)^{i-1} \zeta^{p^{-i-1}p^n} p^i \in \mathfrak{m}_k
\]

and \( (\log g)^{(n+1)}(X) \in \mathcal{O}_k[[X]] \) for each \( n \). This means that \( \log g^{-(n+1)}(X) \) is of the Honda type \( T_2 + p \) for each \( n \).

**Theorem 4.2.5** (Honda [9] Theorem 5). Let \( E \) be an elliptic curve defined over \( \mathbb{Q}_p \) with good reduction at \( p \). Then \( \log \hat{E}(X) \) is of the Honda type \( T_2 - ap + T + p \).

**Proposition 4.2.6.** Over the ring of the unramified quadratic extension of \( \mathbb{Q}_p \), the formal group \( \hat{E} \) is isomorphic to the Lubin-Tate formal group of height 2 with the parameter \(-p\).

Hence by Theorem 4.2.2 we see that

(i) there is a formal group \( \mathcal{G}_n \) defined over \( \mathcal{O}_k \) whose formal logarithm \( \log \mathcal{G}_n \) is given by \( \log g^{-(n+1)} \) for each \( n \), and

(ii) the power series \( \exp \hat{E} \circ \log \mathcal{G}_n \) is contained in \( \mathcal{O}_k[[X]] \) and gives an isomorphism \( \mathcal{G}_n \to \hat{E} \) over \( \mathcal{O}_k \) for each \( n \).

We fix a generator \( (\zeta_n) \) of \( \mathbb{Z}_p(1) \), namely, for each \( n \geq 0 \), \( \zeta_n \) is a primitive \( p^n \)th root of unity such that \( \zeta_{p^{n+1}} = \zeta_n \). Let \( \pi_n = \zeta^{p^{n+1}} - (\zeta_{p^{n+1}} - 1) \in \mathfrak{m}_n \) for \( n \geq -1 \) and \( \pi_n = 0 \) for \( n < -1 \). For each \( n \), we can easily show that

\[
g^{(m),p^{-(n+1)}}(\pi_n) = \pi_{n-m}
\]

for any \( m \geq 0 \) by direct calculation.

Put

\[
\varepsilon_n = \zeta^{p^{n+1}} - \zeta^{p^n} - \zeta^{p^{n+2}} + \cdots = \sum_{i=1}^{\infty} (-1)^{i-1} \zeta^{p^{n+i+1}} p^i \in \mathfrak{m}_k
\]

for \( n \geq -1 \). Since \( \log \mathcal{G}_n : \mathcal{G}_n(\mathfrak{m}_k) \to \mathfrak{m}_k \) is an isomorphism for all \( n \) (cf. Proposition 4.2.4), there is \( \varepsilon_n \in \mathcal{G}_n(\mathfrak{m}_k) \) such that \( \log \mathcal{G}_n(\varepsilon_n) = \varepsilon_n \) for \( n \geq -1 \).
Definition 4.2.7. We define
\[ d_n = \exp_E \circ \log_{\mathcal{G}_n}(e_n[+]_{\mathcal{G}_n}\pi_n) \]
for \( n \geq -1 \), where \([+]_{\mathcal{G}_n}\) is the addition of \( \mathcal{G}_n \).

For \( n \geq m \), we denote by \( \text{Tr}_{n/m} : \hat{E}(m_n) \to \hat{E}(m_m) \) the trace (norm) with respect to the group-law \( \hat{E}(X, Y) \).

Proposition 4.2.8. The system of local points \((d_n)_n \in \prod_{n \geq -1} \hat{E}(m_n)\) satisfies

1. \( \text{Tr}_{n/n-1}(d_n) = -d_{n-2} \) for each \( n \geq 1 \),
2. \( \text{Tr}_{0/-1}(d_0) = -(\varphi + \varphi^{-1})d_{-1} \).

Proof. We prove this by the same method as the proof of Lemma 8.9 in [17].

Since \( \log_{\hat{E}} \) is injective (cf. Proposition 4.2.3) and commute with the action of \( G_n \) on \( \hat{E}(m_n) \), it is enough to show that the relation holds after applying \( \log_{\hat{E}} \) to both sides of the equality.

We have
\[
\log_{\hat{E}}(d_n) = \log_{\mathcal{G}_n}(e_n[+]_{\mathcal{G}_n}\pi_n) = \log_{\mathcal{G}_n}(e_n) + \log_{\mathcal{G}_n}(\pi_n)
= \varepsilon_n + \sum_{m=0}^{\left\lceil \frac{n+1}{2} \right\rceil} (-1)^m \frac{\pi_{n-2m}}{p^m}.
\]

Here the last equality follows from (4.2.1) and \( \pi_n = 0 \) for \( n \leq -1 \).

For \( n \geq 1 \), we have
\[
\text{Tr}_{n/n-1} \log_{\hat{E}}(d_n) = p\varepsilon_n - \zeta^{-n+1}p + \sum_{m=1}^{\left\lceil \frac{n+1}{2} \right\rceil} (-1)^m \frac{\pi_{n-2m}}{p^{m-1}}
= -\varepsilon_{n-2} - \sum_{m=0}^{\left\lceil \frac{n-1}{2} \right\rceil} (-1)^m \frac{\pi_{n-2-2m}}{p^{m-1}}
= -\log_{\hat{E}}(d_{n-2}).
\]

For \( n = 0 \), we have
\[
\text{Tr}_{0/-1} \log_{\hat{E}}(d_0) = (p - 1)\varepsilon_0 - \zeta^{-1}p
= -(\varphi + \varphi^{-1})\varepsilon_{-1}
= -(\varphi + \varphi^{-1}) \log_{\hat{E}}(d_{-1}).
\]
\( \square \)
Remark 4.2.9. As long as we define local points as values of certain power series at certain points, the factor \( \varphi + \varphi^{-1} \) in the condition (2) always appears (cf. [18] Proposition 3.10, (3.3)). Although Byoung Du Kim did not mention explicitly in [11], [12], this factor \( \varphi + \varphi^{-1} \) was an obstruction. He assumed in [11] and [12] that \( k = \mathbb{Q}_p \) when he considered the plus Selmer groups in order to make the situation simpler, i.e. \( \varphi + \varphi^{-1} = 2 \) in \( \mathbb{Z}_p[G_{-1}] = \mathbb{Z}_p \). In this thesis, we consider general unramified extension \( k/\mathbb{Q}_p \), carefully taking into account this factor \( \varphi + \varphi^{-1} \) in \( \mathbb{Z}_p[G_{-1}] \).

Lemma 4.2.10. \( \varphi + \varphi^{-1} \) is a unit in \( \mathbb{Z}_p[G_{-1}] \) if and only if \( d \equiv /0 \pmod{4} \).

Proof. First we note that \( \varphi + \varphi^{-1} \in \mathbb{Z}_p[G_{-1}]^\times \) if and only if \( 1 + \varphi^2 \in \mathbb{Z}_p[G_{-1}]^\times \).

If \( d \) is odd, we have
\[
(1 + \varphi^2)(1 - \varphi^2 + \varphi^4 - \cdots + (-1)^{(3d-2)/2} \varphi^{d-2}) = 1 + (-1)^{d-1} = 2.
\]

If \( d \) is even, we have
\[
(1 + \varphi^2)(1 - \varphi^2 + \varphi^4 - \cdots + (-1)^{d-2}(1 - \varphi^d) = 1 + (-1)^{(d-2)/2} = \begin{cases} 2 & \text{if } d \not\equiv 0 \pmod{4}, \\ 0 & \text{if } d \equiv 0 \pmod{4}, \end{cases}
\]
and \( 1 - \varphi^2 + \varphi^4 - \cdots + (-1)^{(d-2)/2} \varphi^{d-2} \not= 0 \) in \( \mathbb{Z}_p[G_{-1}] \). Since 2 is invertible in \( \mathbb{Z}_p[G_{-1}] \), we get the conclusion of Lemma 4.2.10. \( \square \)

Remark 4.2.11. What we really proved is the following; (1) \( \varphi + \varphi^{-1} \) is a unit if \( d \not\equiv 0 \pmod{4} \), (2) \( \varphi + \varphi^{-1} \) is a zero-divisor if \( d \equiv 0 \pmod{4} \).

Moreover, we can easily check the following lemma.

Lemma 4.2.12. We have
\[
\text{Ann}_{\mathbb{Z}_p[G_{-1}]}(\varphi + \varphi^{-1}) = \begin{cases} 0 & \text{if } d \not\equiv 0 \pmod{4}, \\ \langle 1 - \varphi^2 + \varphi^4 - \cdots - \varphi^{d-2} \rangle_{\mathbb{Z}_p[G_{-1}]} & \text{if } d \equiv 0 \pmod{4}, \end{cases}
\]
and \( \text{rank}_{\mathbb{Z}_p} \text{Ann}_{\mathbb{Z}_p[G_{-1}]}(\varphi + \varphi^{-1}) = 2 \) if \( d \equiv 0 \pmod{4} \).

To describe the quotient modules \( \hat{E}(\mathfrak{m}_n)/\hat{E}(\mathfrak{m}_{n-1}) \) using the local points \((d_n)_n\), we prepare the following lemma.
Lemma 4.2.13. We have \( m_n/m_{n-1} = \langle \pi_n \rangle_{Z_p[G_n]} \) for \( n \geq 0 \).

Proof. It is enough to show that \( \zeta(\zeta_{p^n+1} - 1) \) generates \( m_n/m_{n-1} \) as a \( Z_p[G_n] \)-module.

We first observe the ring of integers \( \mathcal{O}_{k_n} \) of \( k_n \). Let \( P_m = \{(\zeta_{p^m} - 1)^\tau \mid \tau \in \text{Gal}(k/m)\} \) for \( m \geq 1 \) and \( P_0 = \{1\} \). Since \( \mathcal{O}_{k_n} = \mathcal{O}_k[\zeta_{p^n+1}] \), we have

\[
\mathcal{O}_{k_n} = \langle P_0 \cup P_1 \cup \cdots \cup P_{n+1} \rangle_{\mathcal{O}_k}.
\]

Thus, for \( x \in \mathcal{O}_{k_n} \), we can write \( x = a_0 + \sum_{m=1}^{n+1} \sum_{\tau \in \text{Gal}(k/m)k} a_{m,\tau}(\zeta_{p^m} - 1)^\tau \) with \( a_0, a_{m,\tau} \in \mathcal{O}_k \). With this notation, since each \( (\zeta_{p^m} - 1)^\tau \) already has positive valuation, we see that \( x \in m_n \) if and only if \( a_0 \in m_k \).

Take any class in \( m_n/m_{n-1} \) with a representative \( x \in m_n \). Write \( x = a_0 + \sum_{m=1}^{n+1} \sum_{\tau \in \text{Gal}(k/m)k} a_{m,\tau}(\zeta_{p^m} - 1)^\tau \). In this summation, the summands \( a_0 \) and \( a_{m,\tau}(\zeta_{p^m} - 1)^\tau \) with \( 1 \leq m \leq n \) are contained in \( m_{n-1} \). Since \( \mathcal{O}_k = Z_p\zeta = \langle \zeta \rangle_{Z_p[G_{n-1}]} \), each \( a_{n+1,\tau} \in \mathcal{O}_k \) can be written as \( a_{n+1,\tau} = \sum_{i=0}^{d-1} b_{\tau,i}\zeta^{d^i} \) with \( b_{\tau,i} \in \mathcal{O}_p \). Therefore we have

\[
x \equiv \sum_{\tau \in \text{Gal}(k_{n+1}/k)} a_{n+1,\tau}(\zeta_{p^{n+1}} - 1)^\tau \equiv \sum_{\tau \in \text{Gal}(k_{n+1}/k)} \sum_{i=0}^{d-1} b_{\tau,i}\zeta^{d^i}(\zeta_{p^{n+1}} - 1)^\tau \pmod{m_{n-1}}.
\]

Here, \( \zeta^{d^i}(\zeta_{p^{n+1}} - 1)^\tau \) with \( 0 \leq i \leq d-1 \), \( \tau \in \text{Gal}(k_{n+1}/k) \) are exactly the Galois conjugates of \( \zeta(\zeta_{p^{n+1}} - 1) \) by \( G_n = G_{n-1} \times \text{Gal}(k_{n+1}/k) \). This completes the proof. \( \square \)

Proposition 4.2.14. For \( n \geq 0 \), we have \( \log E(\mathcal{E}(m_n)) \subseteq m_n + k_{n-1} \) and the formal logarithm \( \log E \) induces canonical isomorphisms of \( Z_p[G_n] \)-modules,

\[
\mathcal{E}(m_n)/\mathcal{E}(m_{n-1}) \xrightarrow{\sim} m_n/m_{n-1}.
\]

By these isomorphisms, \( d_n \) is sent to \( \pi_n \). In particular, we have

\[
\mathcal{E}(m_n)/\mathcal{E}(m_{n-1}) = \langle d_n \rangle_{Z_p[G_n]}.
\]

Proof. We prove this by the same method as the proof of Proposition 8.11 in [17] or Proposition 4.9 in [10].

For the first statement, we only note that by the commutative diagram

\[
\begin{array}{ccc}
\mathcal{E}(m_n) & \xrightarrow{\log E} & k_n \\
\exp_{G_{n-1}} \circ \log E & \cong & \log_{G_{n-1}} \\
G_{n-1}(m_n) & &
\end{array}
\]

34
it is enough to consider \( \log_{G-1} (= \log_{G}) \) on \( G-1(\mathfrak{m}_n) \) instead of \( \log_{\hat{E}} \) on \( \hat{E}(\mathfrak{m}_n) \).

Then we can show that \( \log_{G-1}(G-1(\mathfrak{m}_n)) \subseteq \mathfrak{m}_n + k_{n-1} \) as in [17], [10].

Since we have \( \log_{\hat{E}}(\mathfrak{m}_n) \cap k_{n-1} = \log_{\hat{E}}(\mathfrak{m}_{n-1}) \), the natural map

\[
\hat{E}(\mathfrak{m}_n)/\hat{E}(\mathfrak{m}_{n-1}) \rightarrow (\mathfrak{m}_n + k_{n-1})/k_{n-1} \cong \mathfrak{m}_n/\mathfrak{m}_{n-1}
\]

is injective. Since \( \varepsilon_n \in \mathfrak{m}_1 \) and \( \pi_{n-2m} \in \mathfrak{k}_{n-2} \) for \( m \geq 1 \), we have

\[
\log_{\hat{E}}(d_n) = \varepsilon_n + \pi_n + \sum_{m=1}^{\lfloor \frac{n}{2} \rfloor} (-1)^m \pi_{n-2m} / \mathfrak{p}_n
\equiv \pi_n \pmod{k_{n-1}}.
\]

Since \( \pi_n \) generates \( \mathfrak{m}_n/\mathfrak{m}_{n-1} \) as a \( \mathbb{Z}_p[G_n] \)-module (cf. Lemma 4.2.13), the above injection is in fact a bijection and \( d_n \) generates \( \hat{E}(\mathfrak{m}_n)/\hat{E}(\mathfrak{m}_{n-1}) \) as a \( \mathbb{Z}_p[G_n] \)-module.

**Corollary 4.2.15.** We have

\[
\hat{E}(\mathfrak{m}_n) = \begin{cases} 
(d_{-1})_{\mathbb{Z}_p[G_{-1}]} & \text{if } n = -1, \\
(d_n, d_{n-1})_{\mathbb{Z}_p[G_n]} & \text{if } n \geq 0.
\end{cases}
\]

**Proof.** The case when \( n = -1 \) follows from \( \hat{E}(\mathfrak{m}_{-1}) \cong \mathfrak{m}_{-1} \) (see Proposition 4.2.4) and Nakayama’s lemma. The case when \( n \geq 0 \) follows easily from Proposition 4.2.14 and the trace relations satisfied by the \( d_n \) (see Proposition 4.2.8).

**Remark 4.2.16.** We defined the system of local points \( (d_n)_n \) following Byoung Du Kim [11] and M. Kim [14] in the above. We can take another system of local points instead of \( (d_n)_n \). Indeed, what we need for the following discussion is a system of local points \( (d_n)_n \) which satisfies the following three conditions

1. \( \text{Tr}_{n/\mathfrak{m}_{n-1}}(d_n) = -d_{n-2} \) for each \( n \geq 1 \) (Proposition 4.2.8 (1)),
2. \( \text{Tr}_{0/\mathfrak{m}_{-1}}(d_0) = - (\varphi + \varphi^{-1})d_{-1} \) (Proposition 4.2.8 (2)),
3. \( \hat{E}(\mathfrak{m}_n)/\hat{E}(\mathfrak{m}_{n-1}) = (d_n)_{\mathbb{Z}_p[G_n]} \) (Proposition 4.2.14).

Such a system \( (d_n)_n \) obviously admits at least a difference of multiplication by a unit in \( \mathbb{Z}_p[G_{-1}]^\times \). Shin-ichi Kobayashi constructed such a system of local points also in [18] Proof of Proposition 3.12 by using another formal power series \( \ell_t(X) \) and a system \( (\zeta_{p^n+1} - 1)_n \) instead of \( \log_{\hat{E}}(X) \) and a system
Lemma 4.2.18. In our setting, the formal power series \( \ell_\epsilon(X) \) is defined for each \( \epsilon \in \hat{E}(m_k) \) by
\[
\ell_\epsilon(X) = \epsilon + \sum_{m=0}^{\infty} (-1)^m \frac{f^{(2m)}(\epsilon' X)}{p^m} \in k[[X]],
\]
where \( \epsilon = \log_\tilde{E}(\epsilon) \in m_k, \epsilon' = (\varphi^2 + p)\epsilon^{-1} \in \mathcal{O}_k, f(X) = (X + 1)^p - 1 \) and \( f^{(m)}(X) \) is the \( m \)-iterated composition of \( f \). By using this formal power series, Kobayashi defined \( d_{\epsilon,n} \) for each \( n \geq -1 \) by
\[
d_{\epsilon,n} = \exp_\tilde{E} \circ \ell_\epsilon^{-(n+1)}(\zeta_{p^{n+1}} - 1) \in \hat{E}(m_n).
\]
Then the first and the second conditions, which are listed above, are satisfied. If we take \( \epsilon \in m_k \) such that \( m_k = \langle \epsilon \rangle \mathbb{Z}_p[\mathbb{G}_n] \), then the third condition is also satisfied. We also note that we can take such a \( \epsilon \in m_k \), since \( m_k \) is known to be a cyclic \( \mathbb{Z}_p[\mathbb{G}_n] \)-module.

### 4.2.3 The norm subgroups

Following Shin-ichi Kobayashi [17] (and M. Kim [14]), we define the \( n \)-th plus subgroup \( \hat{E}^+(m_n) \), the \( n \)-th minus subgroup \( \hat{E}^-(m_n) \) and the \( n \)-th norm subgroup \( \mathcal{C}(m_n) \) of \( \hat{E}(m_n) \):

**Definition 4.2.17.** We define
\[
\hat{E}^+(m_n) = \left\{ P \in \hat{E}(m_n) \mid \begin{array}{l}
\text{Tr}_{n/m+1} P \in \hat{E}(m_{n}) \\
\text{for all even } m, -1 \leq m \leq n - 1
\end{array} \right\},
\]
\[
\hat{E}^-(m_n) = \left\{ P \in \hat{E}(m_n) \mid \begin{array}{l}
\text{Tr}_{n/m+1} P \in \hat{E}(m_{n}) \\
\text{for all odd } m, -1 \leq m \leq n - 1
\end{array} \right\}
\]
for \( n \geq 0 \). We denote \( \hat{E}^\pm(m_\infty) = \bigcup_n \hat{E}^\pm(m_n) \). We also define
\[
\mathcal{C}(m_n) = \left\{ P \in \hat{E}(m_n) \mid \begin{array}{l}
\text{Tr}_{n/m+1} P \in \hat{E}(m_{n}) \\
\text{for all } m \equiv n \pmod{2}, -1 \leq m \leq n - 1
\end{array} \right\}
\]
for \( n \geq 0 \) and \( \mathcal{C}(m_{-1}) = \hat{E}(m_{-1}) \).

By the following lemma, it is enough to study \( \hat{E}^\pm(m_n) \) instead of \( E^\pm(k_n) \) in our purpose.

**Lemma 4.2.18.** The natural maps \( \hat{E}^\pm(m_n) \rightarrow E^\pm(k_n) \) induce isomorphisms \( \hat{E}^\pm(m_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \cong E^\pm(k_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \) for all \( n \), and thus we have
\[
\hat{E}^\pm(m_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \cong E^\pm(k_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p.
\]
Proof. We consider the following commutative diagrams

\[
\begin{array}{ccccccccc}
0 & \longrightarrow & \hat{E}(m_n) & \longrightarrow & E(k_n) & \longrightarrow & \hat{E}(\mathbb{F}_k) & \longrightarrow & 0 \\
& & \downarrow & & \downarrow & & \downarrow_{\iota_n^\pm} & & \\
0 & \longrightarrow & \hat{E}^\pm(m_n) & \longrightarrow & E^\pm(k_n) & \longrightarrow & A_n^\pm & \longrightarrow & 0,
\end{array}
\]

where \(\hat{E}\) is the reduction of \(E\) modulo \(p\), \(\mathbb{F}_k\) is the residue field of \(k\) and \(A_n^\pm\) is the cokernel of \(\hat{E}^\pm(m_n) \rightarrow E^\pm(k_n)\). Since \(\hat{E}^\pm(m_n) = \hat{E}(m_n) \cap E^\pm(k_n)\), we see that the right vertical arrows \(\iota_n^\pm\) are injective. Thus \(A_n^\pm\) are finite as \(\hat{E}(\mathbb{F}_k)\) is finite. We also note that \(A_n^\pm[p^\infty] = 0\), since \(E/\mathbb{Q}_p\) has supersingular reduction. From the above, our claim will follow immediately. \(\square\)

By comparing two definitions, we get the following relations between the plus subgroups (the minus subgroups) and the norm subgroups.

**Lemma 4.2.19.** We have

\[
\hat{E}^+(m_n) = \begin{cases} 
\mathcal{C}(m_n) & \text{if } n \text{ is even}, \\
\mathcal{C}(m_{n-1}) & \text{if } n \text{ is odd},
\end{cases}
\]

\[
\hat{E}^-(m_n) = \begin{cases} 
\mathcal{C}(m_n) & \text{if } n \text{ is odd}, \\
\mathcal{C}(m_{n-1}) & \text{if } n \text{ is even}.
\end{cases}
\]

We now describe \(\mathcal{C}(m_n)\) in terms of the system of local points \((d_n)_n\), and thus we get a description of plus and minus subgroups \(\hat{E}^\pm(m_n)\).

**Proposition 4.2.20.** (1) For each \(n \geq -1\), the \(n\)-th norm subgroup is generated by \(d_n\) and \(d_{-1}\) as a \(\mathbb{Z}_p[G_n]\)-module;

\[
\mathcal{C}(m_n) = \langle d_n, d_{-1} \rangle_{\mathbb{Z}_p[G_n]}.
\]

(2) For each \(n \geq 0\), we have an exact sequence

\[
0 \longrightarrow \hat{E}(m_{-1}) \longrightarrow \mathcal{C}(m_n) \oplus \mathcal{C}(m_{n-1}) \longrightarrow \hat{E}(m_n) \longrightarrow 0, \quad (4.2.2)
\]

where the first map is diagonal embedding by inclusions, and the second map is \((a, b) \mapsto a - b\).
Proof. We will prove this by the same method as the proof of Proposition 8.12 in [17]. The main difference is the element \( d_{-1} \) in the first statement.

We first show that \( \mathcal{C}(m_n) \cap \mathcal{C}(m_{n-1}) = \hat{E}(m_n) \) for \( n \geq 0 \). It is clear that \( \mathcal{C}(m_n) \cap \mathcal{C}(m_{n-1}) \supseteq \hat{E}(m_n) \) by definition. Let \( P \in \mathcal{C}(m_n) \cap \mathcal{C}(m_{n-1}) \). We show that, if \( P \in \hat{E}(m_n) \) for some \( m \geq 0 \), then \( P \in \hat{E}(m_{n-1}) \). In the case when \( m \equiv n \pmod{2} \), we have \( p^{n-m}P = \text{Tr}_{n/m}P \in \hat{E}(m_{n-1}) \) by the definition of \( \mathcal{C}(m_{n-1}) \). Therefore for \( \sigma \in \text{Gal}(k_m/k_{m-1}) \), we have \( p^{n-m}(P^\sigma - P) = 0 \). Hence, by Proposition 4.2.3, \( P \in \hat{E}(m_{n-1}) \). In the case when \( m \equiv n - 1 \pmod{2} \), our claim is shown similarly by considering \( \mathcal{C}(m_n) \) instead of \( \mathcal{C}(m_{n-1}) \) in the above argument. The other inclusion is clearly true.

For the moment, let \( \mathcal{C}'(m_n) \) be the \( \mathbb{Z}_p[G_n] \)-submodule of \( \hat{E}(m_n) \) generated by \( d_n \) and \( d_{-1} \). By the trace relations on \( d_n \), clearly we have \( \mathcal{C}(m_n) \supseteq \mathcal{C}'(m_n) \).

We now prove

\[
\mathcal{C}(m_n) = \mathcal{C}'(m_n), \quad \mathcal{C}(m_n) + \mathcal{C}(m_{n-1}) = \hat{E}(m_n)
\]

for \( n \geq 0 \), simultaneously by induction.

In the case when \( n = 0 \), we have

\[
\mathcal{C}(m_0) = \hat{E}(m_0) = \langle d_0, d_{-1} \rangle_{\mathbb{Z}_p[G_0]} = \mathcal{C}'(m_0),
\]

\[
\mathcal{C}(m_0) + \mathcal{C}(m_1) = \hat{E}(m_0) + \hat{E}(m_1) = \hat{E}(m_0)
\]

by Corollary 4.2.15.

In the case when \( n \geq 1 \), by the induction hypothesis we have

\[
\hat{E}(m_{n-1}) = \mathcal{C}(m_{n-1}) + \mathcal{C}(m_{n-2}), \quad \mathcal{C}(m_{n-2}) = \mathcal{C}'(m_{n-2}) \tag{4.2.3}
\]

and by the trace relation we have \( \mathcal{C}'(m_{n-2}) \subseteq \mathcal{C}'(m_n) \). Therefore, by Proposition 4.2.14 and (4.2.3), we have

\[
\hat{E}(m_n) = \langle d_n \rangle_{\mathbb{Z}_p[G_n]} + \hat{E}(m_{n-1})
\]

\[
= (\langle d_n \rangle_{\mathbb{Z}_p[G_n]} + \mathcal{C}'(m_{n-2})) + \mathcal{C}(m_{n-1})
\]

\[
\subseteq \mathcal{C}'(m_n) + \mathcal{C}(m_{n-1}).
\]

In particular, we have \( \mathcal{C}(m_n) \subseteq \mathcal{C}'(m_n) + \mathcal{C}(m_{n-1}) \). This implies that \( \mathcal{C}(m_n) = \mathcal{C}'(m_n) \). Indeed, if \( P \in \mathcal{C}(m_n) \), then there exist \( Q \in \mathcal{C}'(m_n) \) and \( R \in \mathcal{C}(m_{n-1}) \) such that \( P = Q + R \). Then we see that \( R = P - Q \in \mathcal{C}(m_n) \cap \mathcal{C}(m_{n-1}) = \hat{E}(m_{n-1}) \). Note that \( \hat{E}(m_{n-1}) \subseteq \mathcal{C}'(m_n) \) since \( d_{-1} \in \mathcal{C}'(m_n) \). So we get \( P = Q + R \in \mathcal{C}'(m_n) \) and thus \( \mathcal{C}(m_n) = \mathcal{C}'(m_n) \). It is now clear that \( \mathcal{C}(m_n) + \mathcal{C}(m_{n-1}) = \mathcal{C}'(m_n) + \mathcal{C}'(m_{n-1}) = \hat{E}(m_n) \). \( \square \)
Remark 4.2.21. We check here that the norm subgroup $\mathcal{C}(m_n)$ is not a cyclic $\mathbb{Z}_p[G_n]$-module generated by $d_n$ if and only if $d = [k : \mathbb{Q}_p] \equiv 0 \pmod{4}$ and $n$ is even.

(1) When $n$ is odd or $d \not\equiv 0 \pmod{4}$, we see that $d_{-1}$ is automatically contained in $\langle d_n \rangle_{\mathbb{Z}_p[G_n]}$. Thus in these cases we see that the norm subgroup $\mathcal{C}(m_n)$ is a cyclic $\mathbb{Z}_p[G_n]$-module generated by $d_n$ for each $n$;

$$\mathcal{C}(m_n) = \langle d_n \rangle_{\mathbb{Z}_p[G_n]}.$$ 

Indeed, when $n$ is odd, we have

$$d_{-1} = (-1)^{n+1} \text{Tr}_{1/0} \cdots \text{Tr}_{n-2/n-3} \text{Tr}_{n/n-1} d_n \in \langle d_n \rangle_{\mathbb{Z}_p[G_n]}.$$ 

When $d \not\equiv 0 \pmod{4}$ and $n$ is even, we have

$$d_{-1} = (-1)^{n+2} (\varphi + \varphi^{-1})^{-1} \text{Tr}_{0/-1} \cdots \text{Tr}_{n-2/n-3} \text{Tr}_{n/n-1} d_n \in \langle d_n \rangle_{\mathbb{Z}_p[G_n]},$$

since $\varphi + \varphi^{-1} \in \mathbb{Z}_p[G_{-1}]$ by Lemma 4.2.10.

(2) When $d \equiv 0 \pmod{4}$, $d_{-1}$ cannot be contained in $\langle d_n \rangle_{\mathbb{Z}_p[G_n]}$ for any even $n$. Thus in this case the norm subgroup $\mathcal{C}(m_n)$ is not a cyclic $\mathbb{Z}_p[G_n]$-module generated by $d_n$ for each even $n$. Indeed, if $\hat{E}(m_0) = \langle d_0 \rangle_{\mathbb{Z}_p[G_0]}$, then $\hat{E}(m_{-1}) = \langle \text{Tr}_{0/-1}(d_0) \rangle_{\mathbb{Z}_p[G_{-1}]}$ since $\text{Tr}_{0/-1} : \hat{E}(m_0) \to \hat{E}(m_{-1})$ is surjective. Since $\hat{E}(m_{-1}) \cong \mathbb{Z}_p[G_{-1}]$, this means that $\mathbb{Z}_p[G_{-1}] = (\varphi + \varphi^{-1})\mathbb{Z}_p[G_{-1}]$, which is impossible by Lemma 4.2.10.

Definition 4.2.22. Define $d_n^\pm$ by

$$
\left\{ \begin{array}{ll}
(-1)^{n+2} d_n & \text{if $n$ is even,} \\
(-1)^{n+1} d_{n-1} & \text{if $n$ is odd,}
\end{array} \right.
$$

$$
\left\{ \begin{array}{ll}
(-1)^{\frac{n+1}{2}} d_n & \text{if $n$ is odd,} \\
(-1)^{\frac{n}{2}} d_{n-1} & \text{if $n$ is even.}
\end{array} \right.
$$

Remark 4.2.23. By the relation between $\mathcal{C}(m_n)$ and $\hat{E}^\pm(m_n)$ (cf. Lemma 4.2.19), we can translate Proposition 4.2.20 in terms of the plus and the minus systems of points $(d_n^+)_n$ and $(d_n^-)_n$ such that $\hat{E}^+(m_n) = \langle d_n^+ \rangle_{\mathbb{Z}_p[G_n]}$ and $\hat{E}^-(m_n) = \langle d_n^- \rangle_{\mathbb{Z}_p[G_n]}$. As in Remark 4.2.21, we see that the plus subgroups $\hat{E}^+(m_n)$ are cyclic $\mathbb{Z}_p[G_n]$-modules generated by $d_n^+$ for all $n$ if and only if $d \not\equiv 0 \pmod{4}$, on the other hand the minus subgroups $\hat{E}^-(m_n)$ are always cyclic $\mathbb{Z}_p[G_n]$-modules generated by $d_n^-$ for all $n$.

Let $\chi : \Delta \to \mathbb{Z}_p^\times$ be a character of $\Delta = \text{Gal}(k(\mu_p)/k)$. We denote $\varepsilon_\chi = \frac{1}{\varphi(p-1)} \sum_{\sigma \in \Delta} \chi(\sigma) \sigma^{-1} \in \mathbb{Z}_p[\Delta]$. If $M$ is a $\mathbb{Z}_p[\Delta]$-module, then $M$ can be decomposed into

$$M = \bigoplus_{\chi} \varepsilon_\chi M.$$
We denote by $M^\chi$ the $\chi$-component $\varepsilon_\chi M$.

Since we have $G_n \cong \Delta \times \Delta \times \text{Gal}(k_n/k_0)$, we can regard a $\mathbb{Z}_p[G_n]$-module as a $\mathbb{Z}_p[\Delta]$-module.

**Corollary 4.2.24.** Let $\chi : \Delta \to \mathbb{Z}_p^\times$ be a character and $q_n = \sum_{i=0}^{n}(-1)^i p^{n-i}$.

Then we have

$$\text{rank}_{\mathbb{Z}_p} C(m_n)^\chi = \begin{cases} d(q_n + 1) & \text{if } n: \text{odd and } \chi = 1, \\ dq_n & \text{otherwise}, \end{cases}$$

for each $n \geq 0$ and

$$\text{rank}_{\mathbb{Z}_p} C(m_{-1})^\chi = \begin{cases} d & \text{if } \chi = 1, \\ 0 & \text{if } \chi \neq 1. \end{cases}$$

**Proof.** Since $C(m_{-1}) = \hat{E}(m_{-1}) \cong \mathbb{Z}_p[G_{-1}]$, we obtain the latter statement. Moreover, from the exact sequence (4.2.2) we get a recurrence sequence

$$\text{rank}_{\mathbb{Z}_p} C(m_n)^\chi + \text{rank}_{\mathbb{Z}_p} C(m_{n-1})^\chi = \text{rank}_{\mathbb{Z}_p} \hat{E}(m_{-1})^\chi + \text{rank}_{\mathbb{Z}_p} \hat{E}(m_n)^\chi.$$

By the theory of formal groups, we have

$$\begin{cases} \hat{E}(m_r)^\chi \cong (m_r^\chi) \chi \text{ (as } \mathbb{Z}_p[G_n]\text{-modules), and} \\ \#\hat{E}(m_n)^\chi / \hat{E}(m_r)^\chi = \#m_r^\chi / (m_r^\chi) < \infty \end{cases}$$

for $r$ sufficiently large. Thus we have

$$\text{rank}_{\mathbb{Z}_p} \hat{E}(m_n)^\chi = \text{rank}_{\mathbb{Z}_p} \hat{E}(m_r)^\chi$$

$$= \text{rank}_{\mathbb{Z}_p} (m_r^\chi) \chi = \text{rank}_{\mathbb{Z}_p} m_r^\chi = dp^n$$

for each $n \geq 0$. Therefore we obtain the former statement.

We introduce here some notation that will be used throughout the remainder of the thesis. Let $\omega_n(X) := (1 + X)^p^n - 1$ and $\Phi_n(X) := \sum_{i=0}^{p-1} X^{ip^n-1}$ be the $p^n$th cyclotomic polynomial. We define $\tilde{\omega}_0^+(X) := 1$ and

$$\tilde{\omega}_n^+(X) = \prod_{1 \leq m \leq n, m: \text{even}} \Phi_m(1 + X), \quad \omega_n^+(X) = X \tilde{\omega}_n^+(X),$$

$$\tilde{\omega}_n^-(X) = \prod_{1 \leq m \leq n, m: \text{odd}} \Phi_m(1 + X), \quad \omega_n^-(X) = X \tilde{\omega}_n^-(X).$$
Note that $\omega_n(X) = \hat{\omega}_n^\pm(X)\omega_n^\pm(X)$ for all $n \geq 0$. We write $\omega_n(X)$, $\hat{\omega}_n^\pm(X)$ and $\omega_n^\pm(X)$ simply by $\omega$, $\hat{\omega}_n^\pm$ and $\omega_n^\pm$ respectively.

We identify $\mathbb{Z}_p[G_n]$ with $\mathbb{Z}_p[G_0][X]/\langle \omega_n \rangle_{\mathbb{Z}_p[G_0][X]}$ by sending $\gamma_n$ to $1 + X$, where $\gamma_n$ is the image of $\gamma$ in $\mathbb{Z}_p[G_n]$.

Set $q_n = \sum_{i=0}^n (-1)^i p^{n-i}$ as in Corollary 4.2.24 and $q_{-1} := 0$. Put

$$q_n^+ := \begin{cases} q_n & \text{if } n \text{ is even}, \\ q_{n-1} & \text{if } n \text{ is odd}, \end{cases}$$

$$q_n^- := \begin{cases} q_n & \text{if } n \text{ is odd}, \\ q_{n-1} & \text{if } n \text{ is even}. \end{cases}$$

Note that $q_n^+ + q_n^- = p^n$ for all $n \geq 0$.

For later use, we rephrase Corollary 4.2.24 in terms of $\hat{E}^\pm(\mathfrak{m}_n)^\chi$ and $q_n^\pm$ as in the following corollary.

**Corollary 4.2.25.** Let $\chi : \Delta \to \mathbb{Z}_p^\times$ be a character. Then we have

$$\text{rank}_{\mathbb{Z}_p}(\hat{E}^+(\mathfrak{m}_n)^\chi) = dq_n^+,$$

$$\text{rank}_{\mathbb{Z}_p}(\hat{E}^-(\mathfrak{m}_n)^\chi) = \begin{cases} d(q_n^- + 1) & \text{if } \chi = 1, \\ dq_n^- & \text{if } \chi \neq 1. \end{cases}$$

For a character $\chi$ of $\Delta$, we define $\mathbb{Z}_p[\chi]$ to be the $\mathbb{Z}_p[\Delta]$-module which is $\mathbb{Z}_p$ as a $\mathbb{Z}_p$-module, and on which $\Delta$ acts via $\chi$, namely $\sigma \cdot x = \chi(\sigma)x$ for $\sigma \in \Delta$ and $x \in \mathbb{Z}_p[\chi]$.

**Proposition 4.2.26.** Let $\chi : \Delta \to \mathbb{Z}_p^\times$ be a character. We have

$$\hat{E}^+(\mathfrak{m}_n)^\chi \cong \begin{cases} \mathbb{Z}_p[G_{-1}][X] \oplus \mathbb{Z}_p[G_{-1}] & \text{if } \chi = 1, \\ \mathbb{Z}_p[\chi] \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[G_{-1}][X]/(\omega_n^-)_{\mathbb{Z}_p[G_{-1}][X]} & \text{if } \chi \neq 1, \end{cases}$$

$$\hat{E}^-(\mathfrak{m}_n)^\chi \cong \begin{cases} \mathbb{Z}_p[G_{-1}][X]/(\omega_n^-)_{\mathbb{Z}_p[G_{-1}][X]} & \text{if } \chi = 1, \\ \mathbb{Z}_p[\chi] \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[G_{-1}][X]/(\omega_n^-)_{\mathbb{Z}_p[G_{-1}][X]} & \text{if } \chi \neq 1, \end{cases}$$

as $\mathbb{Z}_p[G_n]$-modules.

**Proof.** There is a surjective homomorphism

$$\psi : \frac{\mathbb{Z}_p[G_0][X]}{\langle \omega_n \rangle_{\mathbb{Z}_p[G_0][X]}^+ \oplus \mathbb{Z}_p[G_{-1}]} \to \langle d_n^+, d_{i-1}^- \rangle_{\mathbb{Z}_p[G_n]} = \hat{E}^+(\mathfrak{m}_n)$$
obtained by sending \((1, 0)\) to \(d_n^+\) and \((0, 1)\) to \(\frac{d_n}{p-1} (= \frac{d-1}{p-1})\). We have a relation
\[
\omega_n^+ d_n^+ = \omega_n^+ d_{n-2}^+ = \cdots = \omega_0^+ d_0^+ = X d_0^+ = 0.
\]
Since \(\varepsilon_1 = \frac{1}{p-1} \sum_{\sigma \in \Delta} \sigma^{-1} = \frac{1}{p-1} \Tr_{0/-1} \in \mathbb{Z}_p[\Delta]\), we also have another relation
\[
\varepsilon_1 \tilde{\omega}_n^+ d_n^+ = \frac{1}{p-1} \Tr_{0/-1} \tilde{\omega}_n^+ d_n^+ = \frac{1}{p-1} \Tr_{0/-1} d_0^+ = (\varphi + \varphi^{-1}) \frac{d_0}{p-1}.
\]
Thus the map \(\psi\) induces a surjective homomorphism
\[
\overline{\psi} : \mathbb{Z}_p[G]][X] \oplus \mathbb{Z}_p[G^{-1}] \to \langle d_n^+, d_0^+ \rangle_{\mathbb{Z}_p[G_n]} = \hat{E}^+(m_n).
\]
This map \(\overline{\psi}\) is injective since the source and the target of \(\overline{\psi}\) are free \(\mathbb{Z}_p\)-modules of the same \(\mathbb{Z}_p\)-rank \(d(p-1)q_n^+\) (cf. Corollary 4.2.25). Thus we have
\[
\hat{E}^+(m_n) \cong \frac{\mathbb{Z}_p[G]][X] \oplus \mathbb{Z}_p[G^{-1}]}{\langle (\varepsilon_1 \omega_n^+, \varphi, \varphi^{-1}) \rangle_{\mathbb{Z}_p[G_0][X]}},
\]
\[
\cong \frac{\mathbb{Z}_p[G_0][X] \oplus \mathbb{Z}_p[G^{-1}]}{\langle (\omega_n^+, 0), (\varepsilon_1 \omega_n^+, \varphi, \varphi^{-1}) \rangle_{\mathbb{Z}_p[G_0][X]}},
\]
\[
\cong \bigoplus_{\chi} \frac{\varepsilon_\chi \mathbb{Z}_p[G_0][X] \oplus \varepsilon_\chi \mathbb{Z}_p[G^{-1}]}{\langle (\varepsilon_\chi \omega_n^+, 0), (\varepsilon_\chi \varepsilon_1 \omega_n^+, \varphi, \varphi^{-1}) \rangle_{\mathbb{Z}_p[G_0][X]}},
\]
as \(\mathbb{Z}_p[G_n]\)-modules, where the last isomorphism is obtained by the character decomposition. Since we have
\[
\varepsilon_\chi \mathbb{Z}_p[G_0][X] \oplus \varepsilon_\chi \mathbb{Z}_p[G^{-1}] \cong \begin{cases} \mathbb{Z}_p[G^{-1}][X] \oplus \mathbb{Z}_p[G^{-1}] & \text{if } \chi = 1, \\ \mathbb{Z}_p[G^{-1}][X] & \text{if } \chi \neq 1, \end{cases}
\]
and
\[
\langle (\varepsilon_\chi \omega_n^+, 0), (\varepsilon_\chi \varepsilon_1 \omega_n^+, \varphi, \varphi^{-1}) \rangle_{\mathbb{Z}_p[G_0][X]} \cong \begin{cases} \langle (\omega_n^+, 0), (\omega_n^+, \varphi, \varphi^{-1}) \rangle_{\mathbb{Z}_p[G^{-1}][X]} & \text{if } \chi = 1, \\ \langle \omega_n^+ \rangle_{\mathbb{Z}_p[G^{-1}][X]} & \text{if } \chi \neq 1 \end{cases}
\]
.
as $\mathbb{Z}_p[G_{-1}[X]]$-modules, we have

\[
\hat{E}^+(m_n)^\chi \cong \frac{\varepsilon_\text{x} \mathbb{Z}_p[G_0][X] \oplus \varepsilon_\text{x} \mathbb{Z}_p[G_{-1}]}{\langle (\varepsilon_\text{x} \omega_n^+, 0), (\varepsilon_\text{x} \varepsilon_1 \omega_n^+, -\varepsilon_\text{x}(\varphi + \varphi^{-1})) \rangle_{\mathbb{Z}_p[G_0][X]}}
\]

\[
\|2\left\{ \begin{array}{ll}
\mathbb{Z}_p[G_{-1}][X] \oplus \mathbb{Z}_p[G_{-1}] & \text{if } \chi = 1, \\
\mathbb{Z}_p[\chi] \otimes \mathbb{Z}_p \mathbb{Z}_p[G_{-1}][X] & \text{if } \chi \neq 1
\end{array} \right.
\]

as $\mathbb{Z}_p[G_{-1}]$-modules. Since $(\omega_n^+, 0) = X(\tilde{\omega}_n^+, -(\varphi + \varphi^{-1}))$, we get the conclusion for $\hat{E}^+(m_n)^\chi$.

Similarly to the above, we have

\[
\hat{E}^-(m_n) = \langle d_n^- \rangle_{\mathbb{Z}_p[G_n]}
\]

\[
\cong \mathbb{Z}_p[G_0][X]/\langle \omega_n^-, (\sigma - 1)\tilde{\omega}_n^- | \sigma \in \Delta, Z_{\mathbb{Z}_p[G_0][X]} \rangle
\]

\[
\cong \frac{\mathbb{Z}_p[G_{-1}][X]}{\langle \omega_n^- \rangle_{\mathbb{Z}_p[G_{-1}][X]} \oplus \bigoplus_{\chi \neq 1} \left( \mathbb{Z}_p[\chi] \otimes \mathbb{Z}_p \frac{\mathbb{Z}_p[G_{-1}][X]}{\langle \omega_n^- \rangle_{\mathbb{Z}_p[G_{-1}][X]}} \right)}
\]

as $\mathbb{Z}_p[G_{-1}]$-modules. So we get the conclusion for $\hat{E}^-(m_n)^\chi$. \qed

Remark 4.2.27. When $d \not\equiv 0 \pmod{4}$ and $\chi = 1$, the description of the Galois module $\hat{E}^+(m_n)^\chi$ in Proposition 4.2.26 can be made more simpler. Explicitly, we claim that the homomorphism

\[
\mathbb{Z}_p[G_{-1}][X]/\langle \omega_n^+ \rangle \rightarrow \mathbb{Z}_p[G_{-1}][X] \oplus \mathbb{Z}_p[G_{-1}]
\]

\[
\langle (\omega_n^+, -(\varphi + \varphi^{-1})) \rangle
\]

given by $x \mapsto (x, 0)$ is an isomorphism. Indeed, since $\varphi + \varphi^{-1} \in \mathbb{Z}_p[G_{-1}]^\chi$ in this case (see Lemma 4.2.10), $(x, y) \in \mathbb{Z}_p[G_{-1}][X] \oplus \mathbb{Z}_p[G_{-1}]$ is equivalent to $(x + y(\varphi + \varphi^{-1})^{-1}\tilde{\omega}_n^+, 0)$ and thus the map is surjective. On the other hand, if $(x, 0) \in \langle (\omega_n^+, -(\varphi + \varphi^{-1})) \rangle$ for $x \in \mathbb{Z}_p[G_{-1}][X]$, then there exists $a(X) \in \mathbb{Z}_p[G_{-1}][X]$ such that $x = a(X)\tilde{\omega}_n^+$ and $0 = -a(0)(\varphi + \varphi^{-1})$. Again by Lemma 4.2.10, we see that $a(0) = 0$. So we get $x = \frac{a(X)}{X} \omega_n^+ \in \langle \omega_n^+ \rangle$ and thus the map is injective.

In the rest of this thesis, we abbreviate $\mathbb{Z}_p[G_{-1}][X]$-modules $\langle S \rangle_{\mathbb{Z}_p[G_{-1}][X]}$ generated by some set $S$ to $\langle S \rangle$ as in the above remark.
4.2.4 The plus and the minus local conditions

In this subsection, we study the $\Lambda$-module $(\hat{E}_+^{\pm}(m_\infty)^\chi \otimes Q_p/Z_p)^\vee$ and prove Proposition 4.2.31. We also study the $\Lambda$-module

$$\left( \frac{H^1(k_\infty, E[p^\infty])}{\hat{E}_+^{\pm}(m_\infty) \otimes Q_p/Z_p} \right)^\vee$$

and prove Proposition 4.2.35.

We first study $(\hat{E}_+^{\pm}(m_\infty) \otimes Q_p/Z_p)$.

Since $\hat{E}_+^{\pm}(m_\infty)$ are $Z_p$-torsion-free, we have an exact sequence

$$0 \rightarrow \hat{E}_+^{\pm}(m_\infty)^\chi \rightarrow \hat{E}_+^{\pm}(m_\infty)^\chi \otimes Q_p \rightarrow \hat{E}_+^{\pm}(m_\infty)^\chi \otimes Q_p/Z_p \rightarrow 0.$$

From this exact sequence, we get the $\Gamma_n$-invariant-coinvariant exact sequence

$$0 \rightarrow \hat{E}_+^{\pm}(m_n)^\chi \otimes Q_p/Z_p \rightarrow \left( \hat{E}_+^{\pm}(m_\infty)^\chi \otimes Q_p/Z_p \right)^{\Gamma_n} \rightarrow \left( \hat{E}_+^{\pm}(m_\infty)^\chi \right)^{\Gamma_n} [p^\infty] \rightarrow 0$$

(4.2.4)

for each $n \geq 0$. We will compute the rightmost modules $\left( \hat{E}_+^{\pm}(m_\infty)^\chi \right)^{\Gamma_n} [p^\infty]$ for all $n \geq 0$ to study the $\Lambda$-module $(\hat{E}_+^{\pm}(m_\infty)^\chi \otimes Q_p/Z_p)^\vee$.

Define $\delta$ by

$$\delta = \begin{cases} 0 & \text{if } d \not\equiv 0 \pmod{4} \text{ or } \chi \neq 1, \\ 2 & \text{otherwise}. \end{cases}$$

Proposition 4.2.28. Let $\chi : \Delta \rightarrow Z_p^\times$ be a character. Then $\left( \hat{E}_+^{\pm}(m_\infty)^\chi \right)^{\Gamma_n} [p^\infty]$ are free $Z_p$-modules for all $n$, and we have

$$\text{rank}_{Z_p} \left( \hat{E}_+^{\pm}(m_\infty)^\chi \right)^{\Gamma_n} [p^\infty] = dq_n^\mp + \delta,$$

$$\text{rank}_{Z_p} \left( \hat{E}_-^{\pm}(m_\infty)^\chi \right)^{\Gamma_n} [p^\infty] = \begin{cases} dq_n^+ - 1 & \text{if } \chi = 1, \\ dq_n^+ & \text{if } \chi \neq 1. \end{cases}$$

44
More precisely, we have
\[
\left( \hat{E}^+(m_\infty)^\chi \right)_{\Gamma_n} [p^\infty]
\]
\[\begin{cases}
\mathbb{Z}_p[G_{-1}]/X \oplus \text{Ann}_{\mathbb{Z}_p[G_{-1}]}(\varphi + \varphi^{-1}) \otimes \mathbb{Q}_p/\mathbb{Z}_p & \text{if } \chi = 1, \\
\mathbb{Z}_p[G_{-1}]/\langle \omega_n^+ \rangle \otimes \mathbb{Q}_p/\mathbb{Z}_p & \text{if } \chi \neq 1,
\end{cases}
\]
\[\left( \hat{E}^- (m_\infty)^\chi \right)_{\Gamma_n} [p^\infty]
\]
\[\begin{cases}
\mathbb{Z}_p[G_{-1}]/X \langle \omega_n^+ \rangle \otimes \mathbb{Q}_p/\mathbb{Z}_p & \text{if } \chi = 1, \\
\mathbb{Z}_p[G_{-1}]/\langle \omega_n^+ \rangle \otimes \mathbb{Q}_p/\mathbb{Z}_p & \text{if } \chi \neq 1
\end{cases}
\]
as \mathbb{Z}_p\text{-modules}.

**Proof.** We prove the claim for \(\left( \hat{E}^+(m_\infty)^\chi \right)_{\Gamma_n} [p^\infty]\) in the case when \(\chi = 1\). We can prove the rest of the claims similarly.

Since we have
\[
\left( \hat{E}^+(m_\infty)^\chi \right)_{\Gamma_n} [p^\infty] = \left( \hat{E}^+(m_\infty)^\chi / \omega_n \hat{E}^+(m_\infty)^\chi \right) [p^\infty]
\]
\[\cong \lim_{m \geq n} \left( \hat{E}^+(m_m)^\chi / \omega_n \hat{E}^+(m_m)^\chi \right) [p^\infty], \quad (4.2.5)
\]
where the transition maps
\[
\left( \hat{E}^+(m_m)^\chi / \omega_n \hat{E}^+(m_m)^\chi \right) [p^\infty] \rightarrow \left( \hat{E}^+(m_{m+1})^\chi / \omega_n \hat{E}^+(m_{m+1})^\chi \right) [p^\infty]
\]
are multiplication-by-\(p\) maps when \(m\) is odd and identity maps when \(m\) is even, we will calculate \(\left( \hat{E}^+(m_m)^\chi / \omega_n \hat{E}^+(m_m)^\chi \right) [p^\infty]\) for each \(n\) and \(m\). Since \(\hat{E}^+(m_m) = \hat{E}^+(m_{m-1})\) if \(m\) is odd, we may assume \(m\) is even.

We consider the case when \(n\) is even. By Proposition 4.2.26 we have
\[
\hat{E}^+(m_m)^\chi / \omega_n \hat{E}^+(m_m)^\chi \cong \frac{\mathbb{Z}_p[G_{-1}]/X \oplus \mathbb{Z}_p[G_{-1}]}{\langle (\omega_n^+, -\varphi + \varphi^{-1})(\omega_n, 0) \rangle} \quad (4.2.6)
\]
We can show that
\[
\frac{\mathbb{Z}_p[G_{-1}]/X \oplus \mathbb{Z}_p[G_{-1}]}{\langle (\omega_n^+, -\varphi + \varphi^{-1})(\omega_n, 0) \rangle} [p^\infty]
\]
\[\cong \frac{\mathbb{Z}_p[G_{-1}]/X \oplus \text{Ann}_{\mathbb{Z}_p[G_{-1}]}(\varphi + \varphi^{-1})}{\langle p^{\frac{n-1}{2}}, (\omega_n, 0) \rangle}. \quad (4.2.7)
\]
Indeed, since we have \( \omega^+_m \equiv p^{\frac{m-n}{2}} \omega^+_n \pmod{\omega_n} \) and \( \omega_n = \bar{\omega}_n \omega^+_n \), there is an exact sequence

\[
0 \rightarrow \mathbb{Z}_p[G^{-1}][X] / \langle p^{\frac{m-n}{2}}, \omega_n \rangle \oplus \text{Ann}_{\mathbb{Z}_p[G^{-1}]}(\varphi + \varphi^{-1}) / \langle p^{\frac{m-n}{2}} \rangle \rightarrow \mathbb{Z}_p[G^{-1}][X] \oplus \mathbb{Z}_p[G^{-1}] / \langle (\bar{\omega}_m^+, - (\varphi + \varphi^{-1})), (\omega_n, 0) \rangle \rightarrow \mathbb{Z}_p[G^{-1}] / \langle (\bar{\omega}_m^+, - (\varphi + \varphi^{-1})), (\omega_n^+, 0), (\alpha \bar{\omega}_n^+, 0) \rangle \rightarrow 0, \tag{4.2.8}
\]

where the first map is \( (x, y) \mapsto (x \omega_n^+ + y \bar{\omega}_n^+, 0) \) and \( \alpha \) is a generator of the \( \mathbb{Z}_p[G^{-1}] \)-module \( \text{Ann}_{\mathbb{Z}_p[G^{-1}]}(\varphi + \varphi^{-1}) \) (cf. Lemma 4.2.12). There is another exact sequence

\[
0 \rightarrow \mathbb{Z}_p[G^{-1}][X] / \langle \omega_n^+, \alpha \bar{\omega}_n^+ \rangle \rightarrow \mathbb{Z}_p[G^{-1}][X] \oplus \mathbb{Z}_p[G^{-1}] / \langle (\bar{\omega}_m^+, - (\varphi + \varphi^{-1})), (\omega_n^+, 0), (\alpha \bar{\omega}_n^+, 0) \rangle \rightarrow \mathbb{Z}_p[G^{-1}] / \langle \varphi + \varphi^{-1} \rangle \rightarrow 0, \tag{4.2.9}
\]

whose leftmost and rightmost modules are both \( \mathbb{Z}_p \)-free, where the first map is \( x \mapsto (x, 0) \) and the second map is \( (x, y) \mapsto y \). Thus the rightmost module in (4.2.8), which is the same as the middle module in (4.2.9), is \( \mathbb{Z}_p \)-free. Our claim (4.2.7) follows from this.

By (4.2.5), (4.2.6), and (4.2.7), we get

\[
\left( \bar{E}^+ (m_{\infty})^\chi \right)^{\mathbb{F}_p} \cong \lim_{m \to \infty} \left( \bar{E}^+ (m_m)^\chi / \omega_n \bar{E}^+ (m_m)^\chi \right)^{\mathbb{F}_p} \]

\[
\cong \lim_{m \to \infty} \frac{\mathbb{Z}_p[G^{-1}][X] \oplus \mathbb{Z}_p[G^{-1}]}{\langle (\bar{\omega}_m^+, - (\varphi + \varphi^{-1})), (\omega_n, 0) \rangle^{\mathbb{F}_p}} \]

\[
\cong \lim_{m \to \infty} \frac{\mathbb{Z}_p[G^{-1}][X] \oplus \text{Ann}_{\mathbb{Z}_p[G^{-1}]}(\varphi + \varphi^{-1})}{\langle p^{\frac{m-n}{2}}, \omega_n \rangle} \]

\[
\cong \left( \frac{\mathbb{Z}_p[G^{-1}][X]}{\langle \omega_n \rangle} \oplus \text{Ann}_{\mathbb{Z}_p[G^{-1}]}(\varphi + \varphi^{-1}) \right) \otimes \mathbb{Q}_p / \mathbb{Z}_p
\]

when \( n \) is even. By replacing \( p^{\frac{m-n}{2}} \) with \( p^{\frac{m-(n-1)}{2}} \) in the above discussion, we get the statement also in the case when \( n \) is odd.
From this description, we see that \( \left( (\hat{E}^+(m_\infty)\chi)_{\Gamma_n}[p^\infty] \right)^\vee \) is \( \mathbb{Z}_p \)-free and

\[
\text{rank}_{\mathbb{Z}_p} \left( (\hat{E}^+(m_\infty)\chi)_{\Gamma_n}[p^\infty] \right)^\vee = \text{rank}_{\mathbb{Z}_p} \left( \frac{\mathbb{Z}_p[G^-][X]}{(\omega_n^-)} \right) + \text{rank}_{\mathbb{Z}_p} \left( \text{Ann}_{\mathbb{Z}_p[G^-]}(\varphi + \varphi^{-1}) \right) = dq_n^- + \delta.
\]

\[\square\]

**Corollary 4.2.29.** Let \( \chi : \Delta \to \mathbb{Z}_p^\times \) be a character. Then the \( \Gamma_n \)-coinvariants \( (\hat{E}^\pm(m_\infty)\chi \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\vee}_{\Gamma_n} \) are free \( \mathbb{Z}_p \)-modules for all \( n \), and we have

\[
\text{rank}_{\mathbb{Z}_p} \left( (\hat{E}^+(m_\infty)\chi \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\vee}_{\Gamma_n} \right) = dp^n + \delta, \\
\text{rank}_{\mathbb{Z}_p} \left( (\hat{E}^-(m_\infty)\chi \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\vee}_{\Gamma_n} \right) = dp^n.
\]

**Proof.** It follows from Corollary 4.2.24, Proposition 4.2.28 and the exact sequence (4.2.4). \[\square\]

**Proposition 4.2.30.** Let \( \chi : \Delta \to \mathbb{Z}_p^\times \) be a character. There exist injective homomorphisms of \( \Lambda \)-modules

\[
\left( \hat{E}^+(m_\infty)\chi \otimes \mathbb{Q}_p/\mathbb{Z}_p \right)^{\vee} \to \Lambda^\oplus d \oplus (\Lambda / X)^{\oplus \delta}, \\
\left( \hat{E}^-(m_\infty)\chi \otimes \mathbb{Q}_p/\mathbb{Z}_p \right)^{\vee} \to \Lambda^\oplus d
\]

with finite cokernels.

**Proof.** We prove the claim for \( (\hat{E}^+(m_\infty)\chi \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\vee} \). We can prove the rest of the claims similarly.

We note that \( (\hat{E}^+(m_\infty)\chi \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\vee} \) has no nontrivial finite \( \Lambda \)-submodule since its \( \Gamma_n \)-coinvariants are free \( \mathbb{Z}_p \)-modules for all \( n \geq 0 \) (see Corollary 4.2.29). Thus by the structure theorem for \( \Lambda \)-modules, there exist irreducible distinguished polynomials \( f_j \), nonnegative integers \( r, s, t, m_i, n_j \), and an injective homomorphism

\[
f : \left( \hat{E}^+(m_\infty)\chi \otimes \mathbb{Q}_p/\mathbb{Z}_p \right)^{\vee} \to \Lambda^{\oplus r} \oplus \bigoplus_{i=1}^{s} \Lambda / p^{m_i} \oplus \bigoplus_{j=1}^{t} \Lambda / f^{n_j}_j =: \mathcal{E}
\]

with finite cokernel \( \mathcal{E} \).

47
We show that
\[
\begin{cases}
    r = d, \\
    s = 0 \text{ (in other words } m_i = 0 \text{ for all } i), \\
    t = \begin{cases} 0 & \text{if } d \not\equiv 0 \pmod{4} \text{ or } \chi \neq 1, \\
                      2 & \text{otherwise}, \end{cases} \\
    (f_1^{n_1}, \ldots, f_t^{n_t}) = (2, \{X, X\}) \text{ if } t = 2.
\end{cases}
\]

From the exact sequence
\[
0 \rightarrow \left( \hat{E}^+(m_\infty) \times \mathbb{Q}_p / \mathbb{Z}_p \right)^{\vee} \xrightarrow{f} \mathcal{E} \rightarrow \mathbb{Z} \rightarrow 0,
\]
we get the \(\Gamma_n\)-invariant-coinvariant exact sequences
\[
\begin{align*}
Z^{\Gamma_n} \rightarrow & \left( \left( \hat{E}^+(m_\infty) \times \mathbb{Q}_p / \mathbb{Z}_p \right)^{\vee} \right)^{\Gamma_n} \\
& \rightarrow \mathcal{E} / \omega_n \mathcal{E} \rightarrow \mathbb{Z} / \omega_n \mathbb{Z} \rightarrow 0
\end{align*}
\]
for all \(n\). Note that, the first maps in (4.2.10) are 0-maps for all \(n\), since \(\left( \left( \hat{E}^+(m_\infty) \times \mathbb{Q}_p / \mathbb{Z}_p \right)^{\vee} \right)^{\Gamma_n}\) is \(\mathbb{Z}_p\)-free. Then we see that \(m_i = 0\) and \(f_j^{n_j} | \omega_n\) (and \(n_j \leq 1\)) for all \(n\) sufficiently large since \(\mathbb{Z} / \omega_n \mathbb{Z}\) is bounded as \(n \rightarrow \infty\).

Thus we get \(s = 0\) here. We now have
\[
dp^n + \delta = \text{rank}_{\mathbb{Z}_p} \left( \left( \hat{E}^+(m_\infty) \times \mathbb{Q}_p / \mathbb{Z}_p \right)^{\vee} \right)^{\Gamma_n}
\]
\[
= \text{rank}_{\mathbb{Z}_p}(\mathcal{E} / \omega_n \mathcal{E}) = rp^n + \sum_{j=1}^t n_j \deg f_j
\]
for all \(n\) sufficiently large. Thus we get \(r = d\).

In the case when \(d \not\equiv 0 \pmod{4}\) or \(\chi \neq 1\), we get \(0 = \sum_{j=1}^t n_j \deg f_j\) from the above discussion. Thus we get \(n_j = 0\) which is the desired result, i.e. \(t = 0\).

We finally consider the case when \(d \equiv 0 \pmod{4}\) and \(\chi = 1\). We may assume \(n_j = 1\) for all \(j\). In this case, we have
\[
2 = \sum_{j=1}^t \deg f_j
\]
\[
f_j | \omega_n (= (1 + X)^{p^n} - 1)
\]
for all \(n\) sufficiently large. We narrow down the possible combinations of \((t, \{f_1, \ldots, f_t\})\) satisfying these two conditions (4.2.12) and (4.2.13). If \(p \geq 5\), there is a unique combination \((t, \{f_1, \ldots, f_t\}) = (2, \{X, X\})\), since \(\deg f_j \leq 2\). If \(p = 3\), since \(\omega_1 = X(X^2 + 3X + 3)\), there are two possible combinations.
(t, \{f_1, \ldots, f_t\}) = (2, \{X, X\}), (1, \{X^2 + 3X + 3\}). By showing that the last combination is impossible, we complete the proof. Indeed, we have \( \operatorname{rank}_{\mathbb{Z}/p} \mathcal{E}/(\omega_0 \mathcal{E}) = d + 1 \) with the combination \( (t, \{f_1, \ldots, f_t\}) = (1, \{X^2 + 3X + 3\}) \). On the other hand, from the exact sequence (4.2.10) for \( n = 0 \), we must have \( \operatorname{rank}_{\mathbb{Z}/p} \mathcal{E}/(\omega_0 \mathcal{E}) = d + 2 \) and thus we get the desired conclusion. \( \square \)

We now get the following proposition which is an important ingredient for the proof of Proposition 4.2.35.

**Proposition 4.2.31.** Let \( \chi : \Delta \to \mathbb{Z}_p^\times \) be a character. Then \( (\hat{E}^{\pm}(m_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\vee \) has no nontrivial finite \( \Lambda \)-submodule and its \( \Lambda \)-rank is \( d \).

**Proof.** This follows from Proposition 4.2.30. \( \square \)

In the rest of this subsection, we study the \( \Lambda \)-module

\[
\left( \frac{H^1(k_\infty, E[p^\infty])}{\hat{E}^{\pm}(m_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right)^\vee.
\]

We consider the exact sequence

\[
0 \to \left( \frac{H^1(k_\infty, E[p^\infty])}{\hat{E}^{\pm}(m_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right)^\vee \to \left( H^1(k_\infty, E[p^\infty]) \right)^\vee \to \left( \hat{E}^{\pm}(m_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \right)^\vee \to 0. \tag{4.2.14}
\]

We studied the \( \Lambda \)-module structure of the rightmost module. We also know the \( \Lambda \)-module structure of the middle module by the following fact (Proposition 4.2.32).

**Proposition 4.2.32** (Greenberg [5] §3 Corollary 2). Let \( L \) be a finite extension of \( \mathbb{Q}_p \) and \( L_\infty \) some \( \mathbb{Z}_p \)-extension of \( L \). Put \( \Lambda_L = \mathbb{Z}_p[[\operatorname{Gal}(L_\infty/L)]] \). If \( E(L_\infty)[p^\infty] = 0 \), then \( H^1(L_\infty, E[p^\infty])^\vee \) is a free \( \Lambda_L \)-module and its \( \Lambda_L \)-rank is \( 2[L : \mathbb{Q}_p] \);

\[
H^1(L_\infty, E[p^\infty])^\vee \cong \Lambda_L^{\oplus 2[L : \mathbb{Q}_p]}.
\]

We can apply Proposition 4.2.32 in our setting as \( L = k_0, L_\infty = k_\infty \). Indeed we see that \( E(k_\infty)[p^\infty] = 0 \) by Proposition 4.2.3.

Here we recall the following useful lemma on equivalent conditions on freeness of \( \Lambda \)-modules and on triviality of finite \( \Lambda \)-submodules.
Lemma 4.2.33. Let $M$ be a finitely generated $\Lambda$-module.

(1) $M$ is a free $\Lambda$-module if and only if $M^\Gamma = 0$ and $M^\Gamma$ is a free $\mathbb{Z}_p$-module.

(2) $M$ has no nontrivial finite $\Lambda$-submodule if and only if $M^\Gamma$ is a free $\mathbb{Z}_p$-module.


Applying the following lemma to the exact sequence (4.2.14), we can now determine the $\Lambda$-module structure of $(H^1(k_\infty, E[p^\infty])/(\hat{E}^\pm(k_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p))^\vee$.

Lemma 4.2.34. Let $f : M \to N$ be a surjective homomorphism of $\Lambda$-modules. Suppose that $M$ is a free $\Lambda$-module of $\Lambda$-rank $r$, and that $N$ is a $\Lambda$-module of $\Lambda$-rank $s$ which has no non-trivial finite $\Lambda$-submodule. Then its kernel $\text{Ker} f$ is a free $\Lambda$-module of rank $r - s$.

Proof. We put $M_0 := \text{Ker} f$. Then by taking the invariant-coinvariant exact sequence, we have

$$0 \to M_0^\Gamma \to M^\Gamma \to N^\Gamma \to M_0^\vee \to M^\vee.$$ 

Since $M$ is a free $\Lambda$-module, we have $M^\Gamma = 0$ and $M^\Gamma$ is a free $\mathbb{Z}_p$-module by Lemma 4.2.33. Since $N$ has no non-trivial finite $\Lambda$-submodule, we see that $N^\Gamma$ is a free $\mathbb{Z}_p$-module by Lemma 4.2.33. Hence we have $M_0^\Gamma = 0$ and $M_0^\vee$ is a free $\mathbb{Z}_p$-module. Thus $M_0$ is a free $\Lambda$-module again by Lemma 4.2.33. It is easy to see that the $\Lambda$-rank of $M_0$ is $r - s$.

Proposition 4.2.35. We have

$$\left( \frac{H^1(k_\infty, E[p^\infty])}{E^\pm(k_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right)^\vee \cong \Lambda^\oplus[k_0: \mathbb{Q}_p].$$

Proof. It follows from Proposition 4.2.31, Proposition 4.2.32, and Lemma 4.2.34 for the exact sequence (4.2.14).

4.2.5 More on the plus and the minus local conditions

The discussion in the previous subsections is enough to prove our main theorem. In this subsection, we further determine the explicit structure of the $\Lambda$-module $(\hat{E}^\pm(m_\infty)^x \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\vee$. For that purpose, we show the following lemma.
Lemma 4.2.36. Let $f : M \to N$ be an injective homomorphism of \( \Lambda \)-modules with finite cokernel. Suppose that $M/\omega_n M$ is $\mathbb{Z}_p$-free and $N_{\Lambda \text{-tors}} = \{ x \in N \mid \omega_n x = 0 \}$ for all $n$ sufficiently large. Then $f$ induces an isomorphism

$$\overline{f} : M / M_{\Lambda \text{-tors}} \cong N / N_{\Lambda \text{-tors}}.$$ 

Proof. We regard $M$ as a $\Lambda$-submodule of $N$ by $f$. Since $N / M$ is finite, we see that $\omega_n N \subset M$ for all $n$ sufficiently large. We thus have

$$\text{Coker}(\overline{f}) = N / (M + N_{\Lambda \text{-tors}})$$

$$\overset{x \omega_n}{\cong} \omega_n N / \omega_n M$$

$$\hookrightarrow M / \omega_n M$$

for all $n$ sufficiently large. Since $M / \omega_n M$ is $\mathbb{Z}_p$-free for all $n$ sufficiently large, we get $M / M_{\Lambda \text{-tors}} \cong N / N_{\Lambda \text{-tors}}$ for such $n$. \hfill \Box

Theorem 4.2.37. Let $\chi : \Delta \to \mathbb{Z}_p^\times$ be a character. We have

$$\left( \hat{E}^+(m_\infty)^\chi \otimes \mathbb{Q}_p / \mathbb{Z}_p \right)^\vee \cong \Lambda^\oplus d \oplus (\Lambda / X)^\oplus \delta,$$

$$\left( \hat{E}^-(m_\infty)^\chi \otimes \mathbb{Q}_p / \mathbb{Z}_p \right)^\vee \cong \Lambda^\oplus d.$$ 

Proof. We prove this theorem for $\left( \hat{E}^+(m_\infty)^\chi \otimes \mathbb{Q}_p / \mathbb{Z}_p \right)^\vee$. We can prove the rest of the claim similarly.

Let $M = \left( \hat{E}^+(m_\infty)^\chi \otimes \mathbb{Q}_p / \mathbb{Z}_p \right)^\vee$, $N = \Lambda^\oplus d \oplus (\Lambda / X)^\oplus \delta$, $f$ be the map obtained in Proposition 4.2.30. Then the assumptions in Lemma 4.2.36 are satisfied (see Proposition 4.2.30, Corollary 4.2.29). Thus we have $M / M_{\Lambda \text{-tors}} \cong \Lambda^\oplus d$ by Lemma 4.2.36.

We now consider the commutative diagram

$$\begin{array}{ccc}
0 & \longrightarrow & M_{\Lambda \text{-tors}} \\
\downarrow f_0 & & \downarrow f \\
0 & \longrightarrow & (\Lambda / X)^\oplus \delta \\
\downarrow \cong & & \downarrow \cong \\
0 & \longrightarrow & \Lambda^\oplus d \oplus (\Lambda / X)^\oplus \delta \\
\downarrow & & \downarrow \\
0 & \longrightarrow & \Lambda^\oplus d \\
\end{array}$$

We see that $M_{\Lambda \text{-tors}} \cong (\Lambda / X)^\oplus \delta$, since Coker($f_0$) is finite. Therefore, the above horizontal exact sequence splits and thus we get

$$M \cong M / M_{\Lambda \text{-tors}} \cong \Lambda^\oplus d \oplus (\Lambda / X)^\oplus \delta.$$ 

\hfill \Box

51
4.3 Finite $\Lambda$-submodules

We use the notations and the assumptions which are described in Section 4.1.

Let $\Gamma = \text{Gal}(F_\infty/F_0)$ and $\Lambda = \mathbb{Z}_p[[\Gamma]]$. We fix a topological generator $\gamma \in \Gamma$. Then we identify the completed group ring $\mathbb{Z}_p[[\Gamma]]$ with the ring of power series $\mathbb{Z}_p[[X]]$ by identifying $\gamma$ with $1 + X$.

4.3.1 Finite $\Lambda$-submodules of $\text{Sel}(F_\infty,E[p^\infty])^\vee$

In this subsection, we study finite $\Lambda$-submodules of the Pontryagin dual of the $p$-primary Selmer group. The aim of this subsection is to prove Theorem 4.3.5.

The following proposition was essentially proved by Hachimori and Matsuno in [7].

**Proposition 4.3.1.** Let $L$ be a finite extension of $\mathbb{Q}$, $L_\infty/L$ a $\mathbb{Z}_p$-extension, $L_n$ its $n$-th layer, and $E$ an elliptic curve defined over $L$. Put $\Gamma_L = \text{Gal}(L_\infty/L)$ and $\Lambda_L = \mathbb{Z}_p[[\Gamma_L]]$. Let $X_n$ be the kernel of the restriction map

$$\text{Sel}(L_n,E[p^\infty]) \longrightarrow \text{Sel}(L_\infty,E[p^\infty])$$

and $X_\infty := \varprojlim X_n$ where the projective limit is taken with respect to the corestriction maps.

Assume that the $\mathbb{Z}_p$-rank of $\text{Sel}(L_n,E[p^\infty])^\vee$ is bounded as $n \to \infty$. Then the maximal finite $\Lambda_L$-submodule of $\text{Sel}(L_\infty,E[p^\infty])^\vee$ is isomorphic to $X_\infty$.

In particular if we further assume that $E(L)[p] = 0$, then $\text{Sel}(L_\infty,E[p^\infty])^\vee$ has no nontrivial finite $\Lambda_L$-submodule.

**Proof.** The proof in [7] works as well if the assumption on the $\Lambda_L$-torsionness of $\text{Sel}(L_\infty,E[p^\infty])^\vee$ is replaced by the assumption on the boundedness of the $\mathbb{Z}_p$-ranks of $\text{Sel}(L_n,E[p^\infty])^\vee$, as Takeji pointed out in [34].

We check that we can apply the above proposition in our setting $L = F_0$ and $L_\infty = F_\infty$.

**Lemma 4.3.2.** The morphisms $\text{Sel}^\pm(F_n,E[p^\infty]) \rightarrow \text{Sel}^\pm(F_\infty,E[p^\infty])$ are injective for all $n \geq 0$.

**Proof.** We can prove this by the same method as the proof of Lemma 9.1 in [17].
We assume from here that both $Sel^\pm(F_\infty, E[p^\infty])^\vee$ are $\Lambda$-torsion. We denote the Iwasawa $\lambda$-invariant of $Sel^\pm(F_\infty, E[p^\infty])^\vee$ by $\lambda^\pm$.

Let $Sel^1(F_n, E[p^\infty]) := \text{Ker} \left( \frac{Sel(F_n, E[p^\infty])}{\prod_{v \in S_{p,F}} H^1(F_{n,v}, E[p^\infty])} \right)$, where $S_{p,F}$ is the set of all primes of $F$ lying above $p$ where $E$ has supersingular reduction.

By the exact sequence (4.2.2), we have an exact sequence

$$0 \rightarrow H^1(F_{n,v}, E[p^\infty]) \rightarrow H^1(F_{n,v}, E[p^\infty]) \rightarrow \bigoplus_{v \in S_{p,F}} H^1(F_{n,v}, E[p^\infty]) \rightarrow 0$$

for each $n$ and for each prime $v$ of $F$ lying above $p$. Thus, for each $n$, we get the following exact sequence

$$0 \rightarrow Sel^1(F_n, E[p^\infty]) \xrightarrow{\iota} Sel^+(F_n, E[p^\infty]) \oplus Sel^-(F_n, E[p^\infty]) \xrightarrow{\eta} Sel(F_n, E[p^\infty]),$$

where $\iota$ is the diagonal embedding by inclusions and the map $\eta$ is $(x, y) \mapsto x - y$.

**Proposition 4.3.3.** The cokernel of $\eta$ in the exact sequence (4.3.1) is finite.

**Proof.** We can prove this by the same method as the proof of Lemma 10.1 in [17].

**Proposition 4.3.4.** The $\mathbb{Z}_p$-rank of $Sel(F_n, E[p^\infty])^\vee$ is bounded as $n \rightarrow \infty$.

More precisely, we have

$$\text{rank}_{\mathbb{Z}_p} Sel(F, E[p^\infty])^\vee + \text{rank}_{\mathbb{Z}_p} Sel(F_n, E[p^\infty])^\vee \leq \lambda^+ + \lambda^-$$

for every $n$.

**Proof.** Since the restriction map $Sel(F, E[p^\infty]) \rightarrow Sel^1(F_n, E[p^\infty])$ is injective, we have

$$\text{rank}_{\mathbb{Z}_p} Sel(F, E[p^\infty])^\vee \leq \text{rank}_{\mathbb{Z}_p} Sel^1(F_n, E[p^\infty])^\vee.$$
Hence by Lemma 4.3.2 and Proposition 4.3.3, we get
\[
\text{rank}_{\mathbb{Z}_p} \text{Sel}(F, E[p^\infty])^\vee + \text{rank}_{\mathbb{Z}_p} \text{Sel}(F_n, E[p^\infty])^\vee \\
\leq \text{rank}_{\mathbb{Z}_p} \text{Sel}^+(F_n, E[p^\infty])^\vee + \text{rank}_{\mathbb{Z}_p} \text{Sel}^-(F_n, E[p^\infty])^\vee \\
\leq \lambda^+ + \lambda^-
\]
for every \(n\) from (4.3.1). The boundedness of the \(\mathbb{Z}_p\)-ranks follows from this immediately.

From the above argument, we can prove the following theorem.

**Theorem 4.3.5.** Assume that both \(\text{Sel}^+(F_\infty, E[p^\infty])^\vee\) and \(\text{Sel}^-(F_\infty, E[p^\infty])^\vee\) are \(\Lambda\)-torsion. Then \(\text{Sel}(F_\infty, E[p^\infty])^\vee\) has no nontrivial finite \(\Lambda\)-submodule.

**Proof.** The \(\mathbb{Z}_p\)-rank of \(\text{Sel}(F_n, E[p^\infty])^\vee\) is bounded as \(n \to \infty\) (cf. Proposition 4.3.4). Further, we have \(E(F_0)[p] = 0\) by Proposition 4.2.3. Thus we can apply Proposition 4.3.1 and get the desired result.

### 4.3.2 Finite \(\Lambda\)-submodules of \(\text{Sel}^\pm(F_\infty, E[p^\infty])^\vee\)

Finally, we study finite \(\Lambda\)-submodules of the Pontryagin duals of the plus and the minus Selmer groups. The aim of this subsection is to prove our main theorem (Theorem 4.3.8).

We prove that the triviality of finite \(\Lambda\)-submodules of \(\text{Sel}(F_\infty, E[p^\infty])^\vee\) is inherited to that of \(\text{Sel}^\pm(F_\infty, E[p^\infty])^\vee\).

Let us consider the following exact sequence of \(\Lambda\)-modules coming from the definition of the Selmer groups:

\[
\bigoplus_{v \in S_{p,F}^{ss}} \left( \frac{H^1(F_\infty,v,E[p^\infty])}{E^\pm(F_\infty,v) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right)^\vee \xrightarrow{\iota^\pm} \text{Sel}(F_\infty, E[p^\infty])^\vee \\
\rightarrow \text{Sel}^\pm(F_\infty, E[p^\infty])^\vee \rightarrow 0. \tag{4.3.2}
\]

**Proposition 4.3.6.** Assume that \(\text{Sel}^\pm(F_\infty, E[p^\infty])^\vee\) is \(\Lambda\)-torsion. Then the map \(\iota^\pm\) in (4.3.2) is injective.

**Proof.** We have \(\text{rank}_{\Lambda}(\text{Sel}(F_\infty, E[p^\infty])^\vee) \geq \sum_{v \in S_{p,F}^{ss}} [F_{0,v} : \mathbb{Q}_p]\) (cf. [6] Theorem 1.7). By Proposition 4.2.35, we have

\[
\left( \frac{H^1(F_\infty,v,E[p^\infty])}{E^\pm(F_\infty,v) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right)^\vee \cong \Lambda^\oplus[F_{0,v} : \mathbb{Q}_p]
\]

54
for each prime $v \in S_{p,F}^{\text{ss}}$. From this and the exact sequence (4.3.2), we see that

$$
\sum_{v \in S_{p,F}^{\text{ss}}} [F_{0,v} : \mathbb{Q}_p] = \text{rank}_\Lambda \left( \bigoplus_{v \in S_{p,F}^{\text{ss}}} \left( \frac{H^1(F_{\infty,v}, E[p^\infty])}{E^\pm(F_{\infty,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right)^\vee \right)
\geq \text{rank}_\Lambda \left( \text{Sel}(F_{\infty}, E[p^\infty])^\vee \right).
$$

Thus we get

$$
\text{rank}_\Lambda \left( \bigoplus_{v \in S_{p,F}^{\text{ss}}} \left( \frac{H^1(F_{\infty,v}, E[p^\infty])}{E^\pm(F_{\infty,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right)^\vee \right) = \text{rank}_\Lambda \left( \text{Sel}(F_{\infty}, E[p^\infty])^\vee \right).
$$

From this, we see that the kernel Ker $\iota^\pm$ is $\Lambda$-torsion. Therefore we get the conclusion since the leftmost direct sum in the exact sequence (4.3.2) is a torsion-free $\Lambda$-module.

The following proposition is a key tool for the proof of our main theorem.

**Proposition 4.3.7** (Greenberg [6] p.104–105). Let $f : M \to N$ be an injective homomorphism of $\Lambda$-modules. Suppose that $N$ is a finitely generated $\Lambda$-module which has no nontrivial finite $\Lambda$-submodule, and that $M$ is a free $\Lambda$-module. Then the cokernel $\text{Coker}(f)$ has no nontrivial finite $\Lambda$-submodule.

**Proof.** We put $N_1 := \text{Coker}(f)$. Then by taking the invariant-coinvariant exact sequence of $0 \to M \to N \to N_1 \to 0$, we get an exact sequence

$$
M^\Gamma \longrightarrow N^\Gamma \longrightarrow N_1^\Gamma \longrightarrow M^\Gamma.
$$

(4.3.3)

Since $M$ is a free $\Lambda$-module, we see that $M^\Gamma = 0$ and $M^\Gamma$ is a free $\mathbb{Z}_p^*$-module by Lemma 4.2.33. Since $N$ has no non-trivial finite $\Lambda$-submodule, we see that $N^\Gamma$ is a free $\mathbb{Z}_p^*$-module by Lemma 4.2.33. Thus from the exact sequence (4.3.3), we see that $N_1^\Gamma$ is a free $\mathbb{Z}_p^*$-module and therefore $N_1$ has no nontrivial finite $\Lambda$-submodule again by Lemma 4.2.33.

**Theorem 4.3.8.** Assume that both $\text{Sel}^+(F_{\infty}, E[p^\infty])^\vee$ and $\text{Sel}^-(F_{\infty}, E[p^\infty])^\vee$ are $\Lambda$-torsion. Then both $\text{Sel}^+(F_{\infty}, E[p^\infty])^\vee$ and $\text{Sel}^-(F_{\infty}, E[p^\infty])^\vee$ have no nontrivial finite $\Lambda$-submodule.

**Proof.** By Proposition 4.2.35, we have

$$
\left( \frac{H^1(F_{\infty,v}, E[p^\infty])}{E^\pm(F_{\infty,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right)^\vee \cong \Lambda^{\oplus[F_{0,v} : \mathbb{Q}_p]}
$$

for each prime $v \in S_{p,F}^{\text{ss}}$. Thus we can apply Proposition 4.3.6 and Proposition 4.3.7 for $f = \iota^\pm$. Thus, by Theorem 4.3.5, we get the desired result. 

Finally, we consider the following special setting. Let $E$ be an elliptic curve defined over $\mathbb{Q}$ such that $E$ has good supersingular reduction at a prime number $p$ with $a_p = 0$. Let $F = \mathbb{Q}(\mu_m)$ such that $\gcd(p, m) = 1$, $F_0 = F(\mu_p)$ and $F_\infty$ the cyclotomic $\mathbb{Z}_p$-extension of $F_0$. In this setting, we get unconditionally the following non-existence of nontrivial finite $\Lambda$-submodules.

**Corollary 4.3.9.** Both $\text{Sel}^+(F_\infty, E[p^\infty])^\vee$ and $\text{Sel}^-(F_\infty, E[p^\infty])^\vee$ have no nontrivial finite $\Lambda$-submodule.

**Proof.** It is actually proved that both $\text{Sel}^+(F_\infty, E[p^\infty])^\vee$ and $\text{Sel}^-(F_\infty, E[p^\infty])^\vee$ are $\Lambda$-torsion, due to Kobayashi and Kato. Therefore, the claim follows from Theorem 4.3.8. □
Acknowledgements

The author would like to express his sincere gratitude to his supervisor, Professor Masato Kurihara, for successive encouragement, helpful discussions, many suggestions, and comments. The author is deeply grateful to Dr. Rei Otsuki for his collaboration on the study of the non-existence of nontrivial finite $\Lambda$-submodules of Selmer groups. The author is also deeply grateful to Professors Hiroyasu Izeki, Kenichi Bannai, and Taka-aki Tanaka for their helpful comments on the manuscript of this thesis. The author would like to thank Dr. Chan-Ho Kim, Dr. Takashi Miura, Dr. Kazuaki Murakami, Dr. Jiro Nomura, and the other members of number theory for discussion, encouragements, and fruitful time in Keio.
Bibliography

[1] H. Bass, J. Milnor, J.P. Serre, Solution of the congruence subgroup problem for $SL_n$ ($n \geq 3$) and $Sp_{2n}$ ($n \geq 2$), IHES, Publications Mathématiques 33 (1967), 59–137.


