

## ON ZETA FUNCTIONS AND IWASAWA MODULES

JANGHEON OH

ABSTRACT. We study the relation between zeta-functions and Iwasawa modules. We prove that the Iwasawa modules  $X_{k(\zeta_p)}^-$  for almost all  $p$  determine the zeta function  $\zeta_k$  when  $k$  is a totally real field. Conversely, we prove that the  $\lambda$ -part of the Iwasawa module  $X_k$  is determined by its zeta-function  $\zeta_k$  up to pseudo-isomorphism for any number field  $k$ . Moreover, we prove that arithmetically equivalent CM fields have also the same  $\mu^-$ -invariant.

### 0. INTRODUCTION

Let  $\zeta_k(s)$  be the zeta function attached to a number field  $k$ . When two number fields share a common zeta function, they are said to be arithmetically equivalent. Isomorphic fields have identical zeta functions. The first non-isomorphic arithmetically equivalent fields were discovered in 1925 by Gassmann [3]. If  $k$  is isomorphic to any field  $L$  with the same zeta function, that is, if  $\zeta_k = \zeta_L \Rightarrow k \simeq L$ , then  $k$  is said to be arithmetically solitary. Robert Perlis [9] proved that any field  $k$  of degree  $[k : \mathbb{Q}] \leq 6$  is solitary. However, there are infinite families of  $k, k'$  of non-isomorphic arithmetically equivalent fields (see Perlis [9]).

In 1958, with the motivation from the theory of function fields, Iwasawa introduced his theory of  $\mathbb{Z}_p$ -extensions, and a few years later Kubota and Leopoldt invented  $p$ -adic  $L$ -functions. Iwasawa [5] interprets these  $p$ -adic  $L$ -functions in terms of  $\mathbb{Z}_p$ -extensions. In 1979, Mazur and Wiles proved the Main Conjecture, showing that  $p$ -adic  $L$ -functions are essentially the characteristic power series of certain Galois actions arising in the theory of  $\mathbb{Z}_p$ -extensions.

In Tate [12] and Turner [13], the following result is proved: let  $k$  and  $k'$  be function fields in one variable over a finite constant field  $F$  and  $\zeta_k, \zeta_{k'}$  be Dedekind zeta functions of  $k, k'$ , respectively. Let  $C, C'$  be complete non-singular curves defined over  $F$  with function fields isomorphic to  $k, k'$ , and  $J(C), J(C')$  the Jacobian varieties of  $C, C'$ . Then the following are equivalent:

$$(1) \zeta_k = \zeta_{k'},$$

$$(2) J(C) \text{ and } J(C') \text{ are } F\text{-isogenous.}$$

---

Received by the editors April 16, 1996 and, in revised form, June 7, 1996 and October 23, 1996.

1991 *Mathematics Subject Classification*. Primary 11R23.

*Key words and phrases*. Iwasawa module, zeta function,  $p$ -adic  $L$ -function.

This paper is part of the author's Ph.D thesis. I would like to thank my adviser, W. Sinnott, for introducing me to this subject, for pointing out to me the key idea and for many valuable comments.

Komatsu [8] proved analogous results in the number field case. More explicitly, he proved the following result: Let  $p$  be a rational prime number,  $k$  and  $k'$  be number fields. Let  $k_\infty$  and  $k'_\infty$  be the basic  $\mathbb{Z}_p$ -extensions of  $k$  and  $k'$ , respectively. Let  $X_k$  the Galois group of the maximal unramified abelian  $p$ -extension of  $k_\infty$  over  $k_\infty$ . Then  $\zeta_k = \zeta_{k'}$  implies that  $X_k$  and  $X_{k'}$  are isomorphic as  $\Lambda$ -modules for almost all prime numbers  $p$ . Adachi and Komatsu [1] proved a weaker converse statement of the above result: Let  $k$  and  $k'$  be totally real number fields. Let  $K_\infty$  be the cyclotomic  $\mathbb{Z}_p$ -extension of  $k(\zeta_p)$ ,  $\Omega$  the maximal abelian  $p$ -extension of  $K_\infty$  unramified outside  $p$ , and  $Y_{k(\zeta_p)}$  the Galois group of  $\Omega$  over  $K_\infty$ . If  $Y_{k(\zeta_p)}$  is isomorphic to  $Y_{k'(\zeta_p)}$  for every prime  $p$ , then  $\zeta_k = \zeta_{k'}$ .

In this paper, we will improve their results. First, we will prove that the Iwasawa modules  $X_{k(\zeta_p)}$  for almost all primes  $p$  determine the field  $k$  up to arithmetic equivalence when  $k$  is a totally real number field. In this case, the Main Conjecture relates the  $p$ -adic  $L$ -functions of  $k$  and the Iwasawa module  $X_k$ . The  $p$ -adic  $L$ -functions give us enough information on the values of the zeta function of  $k$  at negative integers. Combining this information and the functional equation, we can reconstruct the zeta function  $\zeta_k$ . The improvements in this paper of the result of Adachi and Komatsu are as follows: In this paper, we use a pseudo-isomorphism instead of an isomorphism, which seems to be natural in Iwasawa theory, and use the module  $X_{k(\zeta_p)}^-$  (see §2 for its definition), contained in the torsion part of  $Y_{k(\zeta_p)}$ , instead of  $Y_{k(\zeta_p)}$ . It is well-known that the rank of the free part of  $Y_{k(\zeta_p)}$  determines the degree  $[k : \mathbb{Q}]$  which we need in the proof of Theorem 1 of this paper. Here we prove that the smaller module  $X_{k(\zeta_p)}^-$  determines the degree  $[k : \mathbb{Q}]$ . The Main Conjecture is proved for odd primes, so the main point of Theorem 1 (see §1) is to prove the result of Adachi and Komatsu under the condition “for almost all prime  $p$ ” instead of “for every prime  $p$ ”.

Secondly, we will prove that the  $\lambda$ -parts of  $X_k$  and  $X_{k'}$  are pseudo-isomorphic for any prime  $p$  if number fields  $k$  and  $k'$  are arithmetically equivalent. It is well-known that arithmetically equivalent number fields  $k$  and  $k'$  have the same normal closure  $L$  over  $\mathbb{Q}$ .

Let  $G = \text{Gal}(L/\mathbb{Q})$ , and  $L_n$  be the  $n$ -th layer of the basic  $\mathbb{Z}_p$ -extension  $L_\infty$ . Komatsu proved that  $X_k$  is isomorphic to  $X_{k'}$  when  $p$  does not divide  $[L : \mathbb{Q}]$ . The real obstruction in the case  $p \mid [L : \mathbb{Q}]$  occurs when the basic  $\mathbb{Z}_p$ -extension  $\mathbb{Q}_\infty$  of  $\mathbb{Q}$  and  $L$  are not linearly disjoint over  $\mathbb{Q}$ , since then the Galois group  $G$  does not act on  $X_{L,\lambda}$ . To overcome the obstruction, we make  $X_{L,\lambda}$  into a  $\mathbb{Z}_p[G]$ -module by tensoring so that we can show that  $X_{k,\lambda}$  and  $X_{k',\lambda}$  are pseudo-isomorphic as  $\mathbb{Z}_p[[\text{Gal}(L_\infty/L)]]$ -modules. (Here the  $\lambda$ -part  $X_{k,\lambda}$  is defined to be  $X_k/\mathbb{Z}_p$ -torsion( $X_k$ .) Further, we can show that  $X_k$  is isomorphic to  $X_{k'}$  as an Iwasawa module when  $p$  does not divide the order  $[L : k] = [L : k']$ . Moreover, we can strengthen our result when  $k$  is a CM field. In fact, we prove that the characteristic polynomials of the modules  $X_k^-$  are the same for arithmetically equivalent CM fields  $k$ . This implies at least that their  $\mu^-$ -invariants are the same.

## 1. STATEMENT OF THE MAIN THEOREMS

Let  $k$  be a number field, and  $S$  be a finite set of rational primes. Let  $p$  be a prime not in  $S$ , let  $\zeta_p$  be a  $p$ -th root of unity, denote  $\text{Gal}(k(\zeta_p)/k)$  by  $\Delta$ , and write  $\mathbb{Z}_p[[\text{Gal}(k(\mu_{p^\infty})/k)]]$  by  $\Lambda[\Delta]$ , where  $k(\mu_{p^\infty})$  is the field obtained by adjoining all the  $p$ -power roots of unity to  $k$ .

**Theorem 1.** *Let  $S$  be a finite set of primes. Let  $k$  be a totally real number field. Suppose we know  $X_{k(\zeta_p)}^-$  as a  $\Lambda[\Delta]$ -module up to pseudo-isomorphism for all  $p \notin S$ ; then we can determine the zeta function  $\zeta_k$  of  $k$ .*

Arithmetically equivalent fields  $k$  and  $k'$  have the same normal closure  $L$ , and  $k \cap \mathbb{Q}_\infty = k' \cap \mathbb{Q}_\infty$ , so that the Galois groups of the basic  $\mathbb{Z}_p$ -extensions  $k_\infty/k$  and  $k'_\infty/k'$  can be identified. Let

$$\Lambda = \mathbb{Z}_p[[\text{Gal}(k_\infty/k)]] = \mathbb{Z}_p[[\text{Gal}(k'_\infty/k')]] = \mathbb{Z}_p[[T]] ,$$

and denote  $\mathbb{Z}_p[[ (1+T)^{p^t} - 1 ]]$  by  $\Lambda_t$ . By the structure theorem of  $\Lambda$ -modules, every finitely generated torsion  $\Lambda$ -module  $X$  is pseudo-isomorphic to a module of the form  $\bigoplus_i \Lambda/p^{m_i} \bigoplus_j \Lambda/f_j^{n_j}(T)$ , where  $f_j \in \Lambda$  is a distinguished and irreducible polynomial prime to  $p$ . Define

$$X_\lambda = X/(\mathbb{Z}_p - \text{torsion}(X)) .$$

Note that  $X_\lambda$  is pseudo-isomorphic to  $\bigoplus_j \Lambda/f_j^{n_j}(T)$ .

**Theorem 2.** *Let  $p$  be a prime number. Let  $k$  and  $k'$  be number fields such that  $\zeta_k = \zeta_{k'}$ . Then the Iwasawa modules  $X_{k,\lambda}$  and  $X_{k',\lambda}$  are pseudo-isomorphic as  $\Lambda_t$ -modules for some  $t$ . Moreover,  $X_k$  is isomorphic to  $X_{k'}$  as a  $\Lambda$ -module if  $p$  does not divide the degree  $[L : k] = [L : k']$ . If  $k$  is a CM field and  $\zeta_k = \zeta_{k'}$  for a number field  $k'$ , then  $k'$  is also a CM field and  $\text{char} X_k^- = \text{char} X_{k'}^-$  for any odd prime  $p$ .*

## 2. THE MAIN CONJECTURE

A  $\mathbb{Z}_p$ -extension of a number field  $k$  is an extension  $k_\infty/k$  with

$$\text{Gal}(k_\infty/k) = \Gamma \simeq \mathbb{Z}_p$$

the additive group of  $p$ -adic integers. Let  $\gamma$  be a topological generator of  $\Gamma$ . Let  $A_n$  be the  $p$ -Sylow subgroup of the ideal class group of the unique  $n$ -th layer  $k_n$  of the  $\mathbb{Z}_p$ -extension  $k_\infty/k$ . Then  $X_k = \varprojlim A_n$  is isomorphic to the Galois group of the maximal unramified abelian  $p$ -extension  $L_{\infty,k}$  over  $k_\infty$ . Extend  $\gamma$  to  $\tilde{\gamma} \in \text{Gal}(L_{\infty,k}/k)$ . Let  $x \in X_k$ . Then  $\gamma$  acts on  $x$  by  $x^\gamma = \tilde{\gamma}x\tilde{\gamma}^{-1}$ . Since  $\text{Gal}(L_{\infty,k}/k_\infty)$  is abelian,  $x^\gamma$  is well-defined. In some cases, we will use the additive notation  $\gamma x$  instead of the multiplicative one  $x^\gamma$ . We make  $X_k$  into a  $\Lambda = \mathbb{Z}_p[[T]]$ -module in the following way;

$$(1+T)x = \gamma x .$$

Iwasawa proved the following theorem. The idea to prove the theorem is to make  $X_k$  into a  $\Lambda$ -module.

**Theorem 3** (L. Washington [14, page 67]). *Let  $k_\infty/k$  be a  $\mathbb{Z}_p$ -extension. Let  $p^{e_n}$  be the exact power of  $p$  dividing the class number of  $k_n$ . Then there exist integers  $\lambda \geq 0, \mu \geq 0$ , and  $\nu$ , all independent of  $n$ , and an integer  $n_0$ , such that*

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

for all  $n \geq n_0$ .

Let  $\mathbb{Q}_\infty/\mathbb{Q}$  be the unique  $\mathbb{Z}_p$ -extension of  $\mathbb{Q}$ . Then the compositum  $k\mathbb{Q}_\infty$  is a  $\mathbb{Z}_p$ -extension of  $k$ , which is said to be the basic  $\mathbb{Z}_p$ -extension of  $k$ . Ferrero and Washington [2] proved that the  $\mu$ -invariant is zero for the basic  $\mathbb{Z}_p$ -extension  $k_\infty/k$  when  $k$  is abelian over  $\mathbb{Q}$ . Iwasawa [7] constructed a non-basic  $\mathbb{Z}_p$ -extension whose  $\mu$ -invariant is not zero. It has been conjectured that we always have  $\mu = 0$  for the basic  $\mathbb{Z}_p$ -extension.

Two  $\Lambda$ -modules  $M$  and  $M'$  are pseudo-isomorphic, written  $M \sim M'$ , if there is a  $\Lambda$ -module map between them with finite kernel and cokernel. The relation  $\sim$  is not reflexive in general. However, it can be shown that it is reflexive for finitely generated  $\Lambda$ -torsion modules. A non-constant polynomial  $g(T) \in \Lambda$  is called distinguished if

$$g(T) = T^n + a_{n-1}T^{n-1} + \dots + a_0, p|a_i, 0 \leq i \leq n - 1 .$$

By the structure theorem of  $\Lambda$ -modules, every finitely generated  $\Lambda$ -module  $M$  is pseudo-isomorphic to a module of the form

$$\Lambda^r \oplus \left( \bigoplus_{i=1}^s \Lambda/p^{n_i} \right) \oplus \left( \bigoplus_{j=1}^t \Lambda/f_j^{m_j}(T) \right) ,$$

where  $r, s, t, n_i, m_j \in \mathbb{Z}$ , and  $f_j$  is distinguished and irreducible. The characteristic ideal  $(\prod f_j^{m_j})(\prod p^{n_i})\Lambda$  is an invariant of  $M$ , which we will denote by  $char(M)$ . Define the  $\mu$ -invariant of  $M$  by  $\mu = \sum_{i=1}^s n_i$ , and the  $\lambda$ -invariant of  $M$  by  $\sum_{j=1}^t m_j deg(f_j)$ .

**Theorem 4.** *Suppose  $k_\infty/k$  is a  $\mathbb{Z}_p$ -extension and assume  $\mu = 0$ . Then*

$$X_k \simeq \mathbb{Z}_p^\lambda \oplus (\text{finite } p \text{ group})$$

as a  $\mathbb{Z}_p$ -module.

*Proof.* See Washington [14, page 286]. □

Let  $k$  be a totally real number field. Fix a rational odd prime  $p$ , and for every integer  $n \geq 0$ , let  $K_n = k(\zeta_{p^{n+1}})$ ,  $K_\infty = \bigcup K_n$ , where  $\zeta_{p^n}$  is a  $p^n$ -th root of unity. Put  $\Delta = Gal(K_0/k)$  and  $\Gamma = Gal(K_\infty/K_0) \simeq \mathbb{Z}_p$  then  $Gal(K_\infty/k) = \Delta \times \Gamma$ . Let  $A_n$  be the Sylow  $p$ -subgroup of the ideal class group of  $K_n$ , and  $Y_n$  be the Galois group  $M_n/K_n$ , where  $M_n$  is the maximal abelian  $p$ -extension of  $K_n$  unramified outside primes above  $p$ . Define

$$X_{k(\zeta_p)} = \varprojlim A_n ,$$

$$Y_{k(\zeta_p)} = \varprojlim Y_n ,$$

$$A_\infty = \varinjlim A_n ,$$

all inverse limits with respect to the norm maps, the direct limit with respect to the induced map of lifting of ideals. The Iwasawa module  $X_{k(\zeta_p)}$  is isomorphic to the Galois group of the maximal unramified abelian  $p$ -extension of  $K_\infty$  over  $K_\infty$  and  $Y_{k(\zeta_p)} \simeq Gal(M_\infty/K_\infty)$ , where  $M_\infty$  is the maximal abelian  $p$ -extension of  $K_\infty$  unramified outside primes above  $p$ .

Define the Iwasawa algebra

$$\mathbb{Z}_p[[\Gamma]] = \varprojlim \mathbb{Z}_p[Gal(K_n/K_0)] .$$

Fix a topological generator  $\gamma_0$  of  $\Gamma$ . We identify  $\mathbb{Z}_p[[\Gamma]]$  with formal power series ring  $\Lambda = \mathbb{Z}_p[[T]]$  by  $\gamma_0 \rightarrow 1 + T$ . Write  $\theta$  for the character with values in  $\mathbb{Z}_p^\times$  giving the action of  $\Delta$  on  $\zeta_p$ . Let  $\kappa$  be the character giving the action of  $\Gamma$  on the group of  $p$ -power roots of unity. Put

$$u = \kappa(\gamma_0).$$

For any integer  $i = 0, 1, \dots, |\Delta| - 1$ , define  $\theta^i$ -idempotent

$$e_i = \frac{1}{|\Delta|} \sum_{\delta \in \Delta} \theta^{-i}(\delta) \delta.$$

The Iwasawa module  $Y_{k(\zeta_p)}$  is a finitely generated  $\Lambda$ -module and  $X_{k(\zeta_p)}$  is a finitely generated torsion  $\Lambda$ -module.

For every odd integer  $i$ , there exists a fraction of power series  $G(T, \theta^i)$  in the field of fractions of  $\Lambda$  satisfying

$$G(u^s - 1, \theta^i) = L_p(\theta^{1-i}, s),$$

where  $L_p(\theta^{1-i}, s)$  is the  $p$ -adic  $L$ -function of  $\theta^{1-i}$ . Hence  $G(T, \theta^i)$  is characterized by the following relation:

$$G(u^s - 1, \theta^i) = L_k(\theta^{-i+s}, s) \prod_{\mathfrak{p}|p} (1 - \theta^{-i+s}(\mathfrak{p}) N\mathfrak{p}^{-s})$$

for every negative integer  $s$ . For every odd integer  $i$ , let

$$H(T, \theta^i) = \begin{cases} G(T, \theta^i), & i \not\equiv 1 \pmod{|\Delta|}, \\ (1 + T - u)G(T, \theta), & i \equiv 1 \pmod{|\Delta|}. \end{cases}$$

Let

$$\tau = \varprojlim \mu_{p^n}.$$

By Kummer theory, we can prove that

$$e_{1-i} Y_{k(\zeta_p)}(-1) \stackrel{\text{def}}{=} e_{1-i} Y_{k(\zeta_p)} \otimes_{\mathbb{Z}_p} \text{Hom}_{\mathbb{Z}_p}(\tau, \mathbb{Z}_p) \simeq \text{Hom}(e_i A_\infty, \mathbb{Q}_p/\mathbb{Z}_p).$$

Let  $G_i(T)$  be a power series such that  $G_i((1 + T)^{-1} - 1)$  is a characteristic power series of  $\text{Hom}(e_i A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$ . The following theorem is proved by Wiles [15](the ‘‘Main Conjecture’’).

**Theorem 5.** For each odd integer  $i$ ,  $H(T, \theta^i)\Lambda = G_i(T)\Lambda$ .

Let  $\text{char}(e_i X_{k(\zeta_p)}) = F_i(T)\Lambda$ . By Iwasawa [6],  $\text{char}(\text{Hom}(e_i A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)) = \text{char}(e_i X_{k(\zeta_p)})$ . Hence we have the following equivalent form of the Main Conjecture.

**Theorem 6.** For each odd integer  $i$ ,  $F_i((1 + T)^{-1} - 1)\Lambda = H(T, \theta^i)\Lambda$ .

### 3. PROOF OF THEOREMS

Notations are the same as in section 1. We define the minus-part of  $X_{k(\zeta_p)}$  by

$$X_{k(\zeta_p)}^- = \sum_{i=1}^{|\Delta|} \sum_{\text{odd}} e_i X_{k(\zeta_p)}.$$

We state the main theorem of this chapter.

**Theorem 7** (= Theorem 1). *Let  $S$  be a finite set of primes. Let  $k$  be a totally real number field. Suppose we know  $X_{k(\zeta_p)}^-$  as a  $\Lambda[\Delta]$ -module up to pseudo-isomorphism for all  $p \notin S$ ; then we can determine the zeta function  $\zeta_k$  of  $k$ .*

We let  $ord_p$  denote the usual valuation on  $\overline{\mathbb{Q}_p}$ , normalized by  $ord_p(p) = 1$ , and let  $|x| = p^{-ord_p(x)}$ .

**Lemma 1.** *Let  $\{x_n\}$  be a sequence in  $\mathbb{C}_p$ , which converges to  $x_0 \neq 0$ . Then  $ord_p(x_n) = ord_p(x_0)$  for  $n$  sufficiently large.*

*Proof.* Since  $x_n$  approaches  $x_0$ ,  $|x_n - x_0|$  is strictly less than  $|x_0|$  for  $n$  sufficiently large. Therefore  $|x_n| = \max\{|x_n - x_0|, |x_0|\} = |x_0|$  for  $n$  sufficiently large.  $\square$

Let  $\delta_i = \#Gal(k(\zeta_{p_i})/k)$  for an odd prime  $p_i$ . Then  $\delta_i$  is an even integer since  $k$  is a totally real number field. When  $p = 2$ ,  $\Delta = Gal(k(\zeta_4)/k)$  so that  $\delta = 2$ . Let  $S$  be a finite set of primes which contains the prime number 2.

**Proposition 1.** *The Iwasawa modules  $X_{k(\zeta_p)}^-$ , for all primes not in  $S$ , determine the absolute value of  $\zeta_k$  at negative integers, up to primes in  $S$ .*

*Proof.* If  $n$  is a negative even integer, then  $\zeta_k(n) = 0$ . Fix a negative odd integer  $n$ . Let  $p$  be a prime number not in  $S$ . Then  $n \equiv i_n \pmod{|\Delta|}$ , for some odd integer  $i_n$ ,  $0 \leq i_n \leq |\Delta| - 1$ . It is well-known that the values  $\zeta_k(n)$  are in  $\mathbb{Q}$ . By Theorem 6, we know the value

$$\begin{aligned} ord_p(G(u^n - 1, \theta^{i_n})) &= ord_p L_k(\theta^{-i_n+n}, n) \prod_{\mathfrak{p}|p} (1 - \theta^{-i_n+n}(\mathfrak{p})N\mathfrak{p}^{-n}) \\ &= ord_p L_k(1, n) = ord_p \zeta_k(n). \end{aligned}$$

Hence the absolute value of  $\zeta_k(n)$  is determined up to primes in  $S$ .  $\square$

*Remark.* By definition, the  $p$ -adic  $L$ -function  $L_p(\theta^i, s)$  of  $\theta^i$  is the continuous function from  $\mathbb{Z}_p \setminus \{1\}$  to  $\mathbb{C}_p$  satisfying  $L_p(\theta^i, s) = L_k(\theta^i, s) \prod_{\mathfrak{p}|p} (1 - \theta^i(\mathfrak{p})N\mathfrak{p}^{-s})$  for all rational integers  $s \leq 0$  with  $s \equiv 1 \pmod{\delta}$ , where  $\delta = \#Gal(k(\zeta_p)/k)$ , for an odd integer  $p$ . For all integers  $i$  and  $n > 1$ ,  $L_k(\theta^i, 1 - n)$  is non-zero if and only if  $i$  and  $n$  have the same parity.

Let  $\sigma_i = p_i - 1$  for an odd prime  $p_i$ , and  $\sigma_i = 2$  if  $p_i = 2$ . Then  $\delta_i$  divides  $\sigma_i$ .

**Proposition 2.** *Let  $S = \{p_1, \dots, p_t\}$  be any finite set of primes. Then there is a sequence  $\{a_n\}$  of odd integers such that  $ord_p(\zeta_k(a_n))$  is constant for  $n$  sufficiently large for all primes  $p$  in  $S$ .*

*Proof.* Let  $a_n = 1 - 2\sigma_1 \cdots \sigma_t - 2\sigma_1 \cdots \sigma_t p_1^n \cdots p_t^n$ ; then

$$L_{p_i}(1, a_n) = \left( \prod_{\mathfrak{p}|p_i} (1 - N\mathfrak{p}^{-a_n}) \right) \zeta_k(a_n),$$

so we know that  $\zeta_k(a_n)$  approaches  $L_{p_i}(1, 1 - 2\sigma_1 \cdots \sigma_t)$   $p_i$ -adically with  $n$ . By the remark above,  $L_{p_i}(1, 1 - 2\sigma_1 \cdots \sigma_t) \neq 0$ . Therefore there exists a positive integer  $N$  such that  $ord_{p_i} \zeta_k(a_n) = ord_{p_i} \zeta_k(1 - 2\sigma_1 \cdots \sigma_t)$  for every integer  $n > N$ , and  $i = 1, \dots, t$ . This completes the proof.  $\square$

By the functional equation, we have the following equation.

$$A^s \Gamma(s/2)^N \zeta_k(s) = A^{1-s} \Gamma((1-s)/2)^N \zeta_k(1-s),$$

where  $A = d_k^{1/2} \pi^{-N/2}$ ,  $N = [k : \mathbb{Q}]$ , and  $d_k$  is the absolute value of the discriminant of  $k$ . Hence we have

$$\begin{aligned} \zeta_k(1-s) &= A^{2s-1} \Gamma(s/2)^N \Gamma((1-s)/2)^{-N} \zeta_k(s) \\ (1) \quad &= A^{2s-1} (\Gamma(s/2)/\Gamma((1-s)/2))^N \zeta_k(s) \\ &= A^{2s-1} (\Gamma(s) 2^{1-s} \pi^{-1/2} \cos((s\pi)/2))^N \zeta_k(s) . \end{aligned}$$

Finally, we get the following equation.

$$(2) \quad |\zeta_k(1-\ell)| = A^{2\ell-1} \Gamma(\ell)^N (2^{1-\ell})^N \pi^{-N/2} |\zeta_k(\ell)|$$

for any positive even integer  $\ell$ .

Now we are ready to prove Theorem 7 by following the idea of Goss and Sinnott [4]. Let  $n$  be a rational number,  $S$  be a finite set of primes. We define  $(n)_{S-part} = \prod_{p \in S} p^{ord_p(n)}$ , and  $(n)_{non-S-part} = n/(n)_{S-part}$ . Let  $x > 0$  be a real number. Then from the equation (2), we have the following equation;

$$(3) \quad |\zeta_k(1-\ell)|/\Gamma(\ell)^x = (A^2 2^{-N})^\ell \Gamma(\ell)^{N-x} 2^N \pi^{-N/2} A^{-1} |\zeta_k(\ell)| .$$

By Stirling's formula,

$$B^s/\Gamma(s) \rightarrow 0 \text{ as } s \rightarrow \infty$$

for any real  $B > 0$ . Moreover,  $\zeta_k(\ell) \rightarrow 1$  as  $\ell \rightarrow \infty$ . Choose a sequence  $\{a_n\}$  as in Proposition 2, and let  $a_n = 1 - \ell_n$ . By Propositions 1 and 2, we know the value of

$$(4) \quad |\zeta_k(1-\ell_n)|/\Gamma(\ell_n)^x$$

up to an (unknown) constant independent of  $n$ , as long as  $n$  is sufficiently large. The right-hand side of the equation (3) approaches 0 as  $\ell$  goes to  $\infty$  if  $N < x$ , and goes to  $\infty$  if  $N > x$ . Hence the same is true of (4). Hence we can read off  $N$ . Going back to the equation (2) with  $\ell = \ell_n$ , we can determine  $A$ ;

$$\begin{aligned} A &= \lim_{n \rightarrow \infty} \exp\left[\frac{1}{2\ell_n - 1} \log\left[\frac{|\zeta_k(1-\ell_n)|_{non-S-part} |\zeta_k(1-\ell_n)|_{S-part}}{\Gamma(\ell_n)^N (2^{1-\ell_n})^N \pi^{-N/2} |\zeta_k(\ell_n)|}\right]\right] \\ &= \lim_{n \rightarrow \infty} \exp\left[\frac{1}{2\ell_n - 1} \log\left[\frac{|\zeta_k(1-\ell_n)|_{non-S-part}}{\Gamma(\ell_n)^N (2^{1-\ell_n})^N \pi^{-N/2} |\zeta_k(\ell_n)|}\right]\right] \end{aligned}$$

by Propositions 1 and 2. Hence we know the discriminant  $d_k$ . Here  $1 - a_n$  is a multiple of 4 since  $\sigma_i$  is even. Since the value  $\cos(4m\pi/2)$  for integer  $m$  and the values of zeta function at positive integers not equal to 1 are positive, we know, by the equation (1), the values  $\zeta_k(a_n)$  are positive. By Proposition 1, we know the non- $S$ -part of the values of zeta function at  $a_n$ , and by Proposition 2, the  $S$ -part is constant for  $n$  sufficiently large. Hence, with the functional equation, we can determine the  $S$ -part of the values of the zeta function at the sequence  $a_n$  for large  $n$ , i.e., we have:

$$\begin{aligned} \zeta_k(1-\ell_n)_{S-part} &= \lim_{m \rightarrow \infty} \frac{A^{2\ell_m-1} (\Gamma(\ell_m) 2^{1-\ell_m} \pi^{-1/2} \cos((\ell_m \pi)/2))^N \zeta_k(\ell_m)}{\zeta_k(1-\ell_m)_{non-S-part}} \\ &= \lim_{m \rightarrow \infty} \frac{A^{2\ell_m-1} (\Gamma(\ell_m) 2^{1-\ell_m} \pi^{-1/2})^N}{\zeta_k(1-\ell_m)_{non-S-part}} \end{aligned}$$

for  $n$  sufficiently large. Therefore, by Proposition 1, we know the values  $\zeta_k(1-\ell_n)$  for  $n$  sufficiently large.

Let

$$\zeta_k(s) = \sum b_n/n^s .$$

Then we have

$$\sum_{m=1}^{\infty} b_m/m^{\ell_n} = A^{2(1-\ell_n)-1} \Gamma((1-\ell_n)/2)^N \Gamma((\ell_n)/2)^{-N} \zeta_k(1-\ell_n) .$$

We know the values of the right-hand side of the above equation for  $n$  sufficiently large, which will be denoted by  $c_n$ . We know  $b_1 = 1$ , and

$$b_2 = \lim_{n \rightarrow \infty} (c_n - 1)2^{\ell_n} .$$

Continuing the above process, we can determine all the coefficients  $b_m$ 's, so we can determine the zeta function  $\zeta_k(s)$ . This completes the proof of Theorem 7.

Let  $k, k'$  be totally real number fields, and let  $S$  be a finite set of primes containing all the primes which are ramified in  $k$  and  $k'$ . Then the number fields  $k$  and  $k'$  are linearly disjoint with  $\mathbb{Q}(\mu_{p^\infty})$  over  $\mathbb{Q}$  for  $p \notin S$ . Let  $K_\infty = k(\mu_{p^\infty})$ , and let  $K'_\infty = k'(\mu_{p^\infty})$ . Then we may identify  $Gal(K_\infty/k)$  and  $Gal(K'_\infty/k')$  (they are both naturally isomorphic to  $Gal(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ ), so that we may compare the Iwasawa modules  $X_{k(\zeta_p)}^-$  and  $X_{k'(\zeta_p)}^-$  as  $\Lambda[\Delta]$ -modules. Then, from Theorem 7, we have the following corollary.

**Corollary 1.** *Let  $k$  and  $k'$  be totally real number fields. Let  $S$  be a finite set of primes containing all the primes which are ramified in  $k$  and  $k'$ . Assume that the two Iwasawa modules*

$$X_{k(\zeta_p)}^- \sim X_{k'(\zeta_p)}^-$$

*are pseudo-isomorphic as  $\Lambda[\Delta]$ -modules for all  $p \notin S$ ; then*

$$\zeta_k = \zeta_{k'} .$$

#### 4. ARITHMETIC EQUIVALENCE

Let  $k$  be a number field, and  $\mathfrak{o}_k$  be its ring of integers. Let  $p\mathfrak{o}_k = \mathfrak{p}_g^{e_g} \cdots \mathfrak{p}_1^{e_1}$  be the decomposition of a prime number  $p \in \mathbb{Z}$ , let  $f_i = [(\mathfrak{o}_k/\mathfrak{p}_i) : \mathbb{Z}/p]$  be the degree of  $\mathfrak{p}_i$ , and  $e_i$  be the ramification indices, numbered so that  $f_i \leq f_{i+1}$ . Then the tuple  $A = (f_1, \dots, f_g)$  is called the splitting type of  $p$  in  $k$ . We define a set  $P_k(A)$  by  $P_k(A) = \{p \in \mathbb{Z} : p \text{ has splitting type } A \text{ in } k\}$ . The notation  $S \doteq T$  will be used to indicate that these two sets differ by at most a finite number of elements. Two subgroups  $H, H'$  of a finite group  $G$  are said to be Gassmann equivalent in  $G$  when

$$|c^G \cap H| = |c^G \cap H'|$$

for every conjugacy class  $c^G = \{g c g^{-1} | g \in G\}$  in  $G$  and  $c$  in  $G$ . Let  $k$  and  $k'$  be number fields, and  $L$  be a Galois extension of  $\mathbb{Q}$  containing  $k$  and  $k'$ . Write  $H = Gal(L/k)$ ,  $H' = Gal(L/k')$  and  $G = Gal(L/\mathbb{Q})$ . The normal core of  $k$  is the largest subfield of  $k$  normal over  $\mathbb{Q}$ . It is the fixed field of the subgroup  $\langle H^\sigma | \sigma \in Gal(L/\mathbb{Q}) \rangle$  generated by all conjugates of  $H$ . We call  $k, k'$  arithmetically equivalent if  $H$  and  $H'$  are Gassmann equivalent in  $G$ . Note that this definition is independent of the choice of  $L$  and that if  $k, k'$  are arithmetically equivalent, then they have the same normal closure.

**Lemma 2** (Perlis [10]). *Two arithmetically equivalent number fields  $k$  and  $k'$  have the same normal core.*

With this notation we have the following theorem.

**Theorem 8.** *The following are equivalent.*

- (a)  $\zeta_k(s) = \zeta_{k'}(s)$ .
- (b)  $P_k(A) = P_{k'}(A)$  for every tuple  $A$ .
- (c)  $P_k(A) \doteq P_{k'}(A)$  for every tuple  $A$ .
- (d)  $H = \text{Gal}(L/k)$  and  $H' = \text{Gal}(L/k')$  are Gassmann equivalent in  $G$ .
- (e)  $\mathbb{Q}[H \backslash G]$  is isomorphic to  $\mathbb{Q}[H' \backslash G]$  as a  $\mathbb{Q}[G]$ -module.

*Proof.* See Komatsu [8]. □

Let  $H$  and  $H'$  be Gassmann equivalent. Let  $\{\rho_1, \dots, \rho_t\}$  and  $\{\rho'_1, \dots, \rho'_t\}$  be right coset representatives of  $H \backslash G$  and  $H' \backslash G$ , respectively. Then we have two homomorphisms  $\pi, \pi'$  from  $G$  into symmetric group  $S_t$  given by  $\pi_g(i) = j$ , where  $H\rho_i g = H\rho_j$ , and  $\pi'_g(i) = j$ , where  $H'\rho'_i g = H'\rho'_j$ . Let  $D$  and  $D'$  be the linear representations of  $G$  induced from the unit representations of  $H$  and  $H'$ . Their characters  $\chi, \chi'$  are given by

$$\chi(g) = |g^G \cap H| |C_G(g)| / |H|,$$

$$\chi'(g) = |g^G \cap H'| |C_G(g)| / |H'|,$$

for  $g \in G$ , where  $C_G(g)$  is the centralizer. By Theorem 8,  $\chi = \chi'$  so that the representations  $D, D' : G \rightarrow GL_t(\mathbb{Q})$  are isomorphic. Thus there is a rational  $t \times t$  matrix  $M \in GL_t(\mathbb{Q})$  satisfying the following relation :

$$D(g)M = MD'(g)$$

for every  $g \in G$ . By clearing the denominators, we may assume that  $M$  is in  $GL_t(\mathbb{Z})$ . A matrix  $M = (m_{ij})$  satisfies the above equation if and only if  $m_{ij} = m_{\pi_g(i), \pi'_g(j)}$  for all  $g \in G$ . With the same notation as in Theorem 8, we have the following proposition.

**Proposition 3.** *Let  $k$  and  $k'$  be arithmetically equivalent fields. Then there is an exact sequence of right  $\mathbb{Z}_p[G]$ -modules*

$$0 \rightarrow \mathbb{Z}_p[H \backslash G] \rightarrow \mathbb{Z}_p[H' \backslash G] \rightarrow A \rightarrow 0,$$

where  $A$  is a finite right- $\mathbb{Z}_p[G]$ -module.

*Proof.* Let  $M$  be a matrix satisfying the condition

$$(5) \quad m_{ij} = m_{\pi_g(i), \pi'_g(j)}.$$

Define a map  $\varphi$  from  $\mathbb{Z}_p[H \backslash G] \rightarrow \mathbb{Z}_p[H' \backslash G]$  by

$$\varphi(H\rho_i) = m_{i1}H'\rho'_1 + \dots + m_{it}H'\rho'_t, \quad i = 1, \dots, t,$$

so  $\varphi$  may be represented by a matrix  $M$  with a basis  $\{\rho_1, \dots, \rho_t\}$  and  $\{\rho'_1, \dots, \rho'_t\}$ . By the equation (5),  $\varphi$  is a right- $\mathbb{Z}_p[G]$ -module homomorphism. Since  $M$  is invertible,  $\varphi$  is injective. Moreover, we have the following equation.

$$\det M \begin{pmatrix} H'\rho'_1 \\ \vdots \\ H'\rho'_t \end{pmatrix} = (\det M)M^{-1} \begin{pmatrix} \varphi(H\rho_1) \\ \vdots \\ \varphi(H\rho_t) \end{pmatrix}$$

Hence cokernel  $\varphi$  is killed by  $\det M$ , but cokernel  $\varphi$  is a finitely generated  $\mathbb{Z}_p$ -module. Therefore cokernel  $\varphi$  is finite. This completes the proof.  $\square$

*Remark.* If  $p$  does not divide the order of  $H$ , then we can take  $A$  to be zero. In the case, both  $\mathbb{Z}_p[H \setminus G]$  and  $\mathbb{Z}_p[H' \setminus G]$  are projective  $\mathbb{Z}_p[G]$ -modules. A projective module is determined by its character  $\chi$ ; hence, they are isomorphic. For details, see Komatsu [8].

Write

$$\Lambda_t = \mathbb{Z}_p[[ (1 + T)^{p^t} - 1 ]],$$

where  $\Lambda_0 = \Lambda = \mathbb{Z}_p[[T]]$ . For the rest of this paper,  $p$  is a fixed prime number, and let  $L$  be a normal closure of  $k$  and  $k'$ . Let  $L_0 \subset L_1 \subset L_2 \subset \dots \subset L_\infty$  be the basic  $\mathbb{Z}_p$ -extension over the field  $L = L_0$ . Put  $\Gamma = Gal(L_\infty/L) \simeq \mathbb{Z}_p$ . When  $p$  does not divide  $[L : \mathbb{Q}]$ , we can identify the following Galois groups  $Gal(k_\infty/k)$ ,  $Gal(k'_\infty/k')$  and  $Gal(L_\infty/L)$ . Komatsu proved that two Iwasawa modules  $X_k$  and  $X_{k'}$  are isomorphic as  $\mathbb{Z}_p[[\Gamma]] = \Lambda_L$ -modules when  $p$  does not divide  $[L : \mathbb{Q}]$ . Let  $\Lambda_k = \mathbb{Z}_p[[Gal(k_\infty/k)]]$ . Now for any prime  $p$  including the above exceptional case, regarding  $\Lambda_L$  as a subring of  $\Lambda_k$ , we have  $\Lambda_L = \Lambda_{k,t}$  for some  $t \geq 0$ . In this chapter, we will prove that the Iwasawa modules  $X_{k,\lambda}$  and  $X_{k',\lambda}$  are pseudo-isomorphic as  $\Lambda_L$ -modules for any prime  $p$ .

### 5. PROOF OF THEOREMS

Let  $k$  be a number field, and let  $L$  be the Galois closure of  $k$  over  $\mathbb{Q}$ . In addition, we assume that  $L \cap k_\infty = k$ . Write  $Gal(L/k) = H$ . Since  $L \cap k_\infty = k$ , the group  $H$  can be considered as  $Gal(L_n/k_n)$  for any  $n \geq 0$ , and it commutes with  $\Gamma$ . Hence the group  $H$  acts on  $X_L$ . Regard  $\Lambda_L$  as a subring of  $\Lambda_k$ , so that  $\Lambda_L$  acts on  $X_k$ . Recall that  $X_\lambda = X/(\mathbb{Z}_p - torsion(X))$  for a  $\Lambda$ -module  $X$ .

**Proposition 4.** *The Iwasawa modules  $X_{L,\lambda}^H$  and  $X_{k,\lambda}$  are pseudo-isomorphic as  $\Lambda_L$ -modules.*

*Proof.* Let  $|H| = [L : k] = p^\alpha m$ , where  $(m, p) = 1$ . For each  $n$ , we choose  $c_n |H| \equiv p^\alpha \pmod{p^{t_n}}$ , so that  $p^{t_n}$  exceeds the order of  $A_{n,L}$  and  $A_{n,k}$ , where  $A_{n,M}$  is the  $p$ -Sylow subgroup of the ideal class group of the  $n$ -th layer of the basic  $\mathbb{Z}_p$ -extension over a number field  $M$ . Let  $i$  be the lifting map from  $A_{n,k}$  to  $A_{n,L}^H$ , and  $N$  be the norm map on ideal classes. Let  $\beta_n$  be an element of the kernel of the map  $i$ . Then

$$(6) \quad 0 = c_n N \circ i(\beta_n) = p^\alpha \beta_n,$$

so that the kernel of  $i$  is killed by  $p^\alpha$  for any  $n$ . Let  $\gamma_n$  be in  $A_{n,L}^H$ . We have the following equation:

$$(7) \quad i(c_n N \gamma_n) = i(c_n |H|) \gamma_n = p^\alpha \gamma_n,$$

so that the cokernel of  $i$  is killed by  $p^\alpha$  for any  $n$ . The lifting map  $i$  commutes with the inverse limit, and the map  $i : \lim_{\leftarrow} A_{n,k} \rightarrow \lim_{\leftarrow} A_{n,L}^H$  is a  $\Lambda_L$ -homomorphism since  $H$  and  $\Gamma$  commute with each other. Define the induced map  $i^*$  of  $i$  from  $X_{k,\lambda}$  to  $X_{L,\lambda}^H$  by  $i^*(\bar{x}) = \overline{i(x)}$ , where  $\bar{x}$  is the reduction map from  $X$  to  $X_\lambda$ . The map  $i^*$  is well-defined since the image of the  $\mathbb{Z}_p$ -torsion of  $X_k$  is contained in the  $\mathbb{Z}_p$ -torsion of  $X_L^H$ . The map  $i^*$  is injective: if  $i^*(\bar{x}) = 0$ , then  $p^m i(x) = 0$  for some integer  $m$ ; hence, by (6),  $p^t x = 0$  for some integer  $t$ , which means that  $x$  is in the  $\mathbb{Z}_p$ -torsion of  $X_k$  i.e.  $x \equiv 0$  in  $X_{k,\lambda}$ . Let  $\bar{y}$  be any element of  $X_{L,\lambda}^H$ . Then, by the above formula

(7),  $p^\alpha \bar{y} = \overline{p^\alpha y} = \overline{i(x)} = i^*(\bar{x})$  for some  $\bar{x}$  in  $X_{k,\lambda}$ . Since  $X_{k,\lambda}$  and  $X_{L,\lambda}^H$  are finitely generated  $\mathbb{Z}_p$ -modules, the induced map  $i^*$  is a pseudo-isomorphism.  $\square$

**Lemma 3.** *Let  $G$  be a group. For any prime number  $p$ , for any  $\mathbb{Z}_p[G]$ -module  $A$ , and a subgroup  $H < G$ ,*

$$\text{Hom}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[H \setminus G], A) \simeq A^H,$$

where  $A^H$  is the subset of elements of  $A$  fixed under  $H$ .

*Proof.* The isomorphism is given by

$$\phi \longrightarrow \phi(He) \text{ for } \phi \in \text{Hom}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[H \setminus G], A).$$

$\square$

*Remark.* Let  $R$  be a ring, and assume that  $A$  is also a  $R$ -module. Assume  $R$  commutes with the action of  $G$ . Then  $\text{Hom}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[H \setminus G], A) \simeq A^H$  as a  $R$ -module by making  $(r\phi)(x) = r(\phi(x))$ . The basic idea of the proof of the main theorem of this section is due to the above lemma which is used in Perlis and Colwell [11].

Let  $k$  and  $k'$  be two isomorphic number fields and  $\phi$  be an automorphism of  $\overline{\mathbb{Q}}$  such that  $\phi(k) = k'$ . Let  $\gamma$  be a topological generator of  $\text{Gal}(k_\infty/k)$ . Then  $\gamma' = \phi\gamma\phi^{-1}$  is a topological generator of  $\text{Gal}(k'_\infty/k')$ . We make  $X_k$  and  $X_{k'}$  into  $\Lambda = \mathbb{Z}_p[[T]]$ -modules in the following way.

$$\gamma x = (1 + T)x \quad \text{and} \quad \gamma' x' = (1 + T)x',$$

where  $x \in X_k$  and  $x' \in X_{k'}$ .

**Proposition 5.** *Let  $k$  and  $k'$  be two isomorphic number fields. Then the Iwasawa modules  $X_k$  and  $X_{k'}$  are isomorphic as  $\Lambda$ -modules for any prime number  $p$ .*

*Proof.* Let  $e$  be an integer such that  $\mathbb{Q}_\infty \cap k = \mathbb{Q}_e$  and  $k_n = k\mathbb{Q}_{n+e}$  be the  $n$ -th layer of the basic  $\mathbb{Z}_p$ -extension of  $k$ . Since  $\mathbb{Q}_{n+e}$  is the normal extension of  $\mathbb{Q}$ ,  $\phi(k_n) = k'_n$ . Let  $x = (x_1, \dots, x_n, \dots) \in X_k$ . Let the fractional ideal  $\mathfrak{a}_n$  be a representative of  $x_n$ . Define  $\phi(x_n)$  to be the class of  $\mathfrak{a}_n^\phi$ . Then

$$\begin{aligned} N\gamma'_n \circ \phi(x_n) &= (1 + \gamma'_n + \dots + \gamma_n^{p-1})\phi(x_n) \\ &= \phi(1 + \gamma_n + \dots + \gamma_n^{p-1})(x_n) = \phi \circ N\gamma_n(x_n). \end{aligned}$$

Hence  $\phi$  induces a map from  $X_k$  to  $X_{k'}$  which is also denoted by  $\phi$ . Moreover, it is a  $\Lambda$ -module homomorphism;

$$\begin{aligned} T \cdot \phi(x) &= (\gamma' - 1)\phi(x) = \gamma' \phi(x) / \phi(x) \\ &= \phi(\gamma x) / \phi(x) = \phi((\gamma - 1)x) = \phi(T \cdot x). \end{aligned}$$

The map  $\phi$  is trivially bijective. This completes the proof.  $\square$

**Lemma 4** (Komatsu). *Let  $k$  and  $k'$  be number fields such that  $\zeta_k = \zeta_{k'}$ . Let  $K$  be a finite Galois extension of  $\mathbb{Q}$ . Then we have  $\zeta_{kK} = \zeta_{k'K}$ .*

*Proof.* See Komatsu [8].  $\square$

Let  $L$  be the Galois closure of  $k$  and  $k'$ , and  $L_\infty/L$  be the basic  $\mathbb{Z}_p$ -extension. Put  $\Gamma = \text{Gal}(L_\infty/L)$  and  $\Lambda_L = \mathbb{Z}_p[[\Gamma]]$ .

Now we restate the main theorem of this section.

**Theorem 9.** *Let  $p$  be a prime number. Let  $k$  and  $k'$  be number fields such that  $\zeta_k = \zeta_{k'}$ . Then the Iwasawa modules*

$$X_{k,\lambda} \sim X_{k',\lambda}$$

as  $\Lambda_L = \Lambda_{k,t}$ -modules for some integer  $t \geq 0$ .

*Proof.* Let  $L$  be the Galois closure of  $k$  and  $k'$ . Let  $e$  be an integer such that  $k \cap \mathbb{Q}_\infty = \mathbb{Q}_e$ . By Lemma 2,  $k' \cap \mathbb{Q}_\infty = \mathbb{Q}_e$ . Let  $m$  be the largest integer such that  $\mathbb{Q}_m \subset L$ , where  $\mathbb{Q}_m$  is the  $m$ -th layer of the basic  $\mathbb{Z}_p$ -extension  $\mathbb{Q}_\infty$  of  $\mathbb{Q}$ . Put  $k_m = k\mathbb{Q}_m$  and  $k'_m = k'\mathbb{Q}_m$ . By Lemma 4,

$$(8) \quad \zeta_{k_m} = \zeta_{k'_m}.$$

Let  $G = \text{Gal}(L/\mathbb{Q})$ ,  $K = \text{Gal}(L/\mathbb{Q}_m)$ ,  $H = \text{Gal}(L/k_m)$ , and  $H' = \text{Gal}(L/k'_m)$ . By the above equation (8) and Theorem 8, two subgroups  $H$  and  $H'$  of  $G$  are Gassmann equivalent in  $G$ . Hence we have an exact sequence by Proposition 3:

$$(9) \quad 0 \rightarrow \mathbb{Z}_p[H \backslash G] \rightarrow \mathbb{Z}_p[H' \backslash G] \rightarrow A \rightarrow 0,$$

where  $A$  is a finite  $\mathbb{Z}_p[G]$ -module. Also note that  $K$  is normal in  $G$ , and that  $H$  and  $H'$  act on  $X_L$ . Since  $L \cap \mathbb{Q}_\infty = \mathbb{Q}_m$ ,  $K$  acts on  $X_{L,\lambda}$  so that  $X_{L,\lambda}$  is a right  $\mathbb{Z}_p[K]$ -module. Consider  $\mathbb{Z}_p[G]$  as a left  $\mathbb{Z}_p[K]$ -module. Then we can form the tensor product:

$$X' = X_{L,\lambda} \otimes_{\mathbb{Z}_p[K]} \mathbb{Z}_p[G].$$

Then  $X'$  is a right  $\mathbb{Z}_p[G]$ -module via the action of  $\mathbb{Z}_p[G]$  on the second factor. We have an exact sequence from the equation (9).

$$\begin{aligned} 0 &\rightarrow \text{Hom}_{\mathbb{Z}_p[G]}(A, X') \\ &\rightarrow \text{Hom}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[H' \backslash G], X') \\ &\rightarrow \text{Hom}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[H \backslash G], X') \\ &\rightarrow \text{Ext}_{\mathbb{Z}_p[G]}^1(A, X') \rightarrow \cdots \end{aligned}$$

First, we will prove that

$$\text{Hom}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[H \backslash G], X') \sim \bigoplus_{p^m\text{-copies}} X_{k,\lambda}$$

as a  $\Lambda = \mathbb{Z}_p[[\text{Gal}(L_\infty/L)]]$ -module, where  $p^m = [G : K]$ . Let  $\{\rho_1, \dots, \rho_{p^m}\}$  be right coset representatives of  $K \backslash G$  with  $\rho_1 = 1$ . Then

$$X' \simeq X_{L,\lambda} \otimes \rho_1 + \cdots + X_{L,\lambda} \otimes \rho_{p^m},$$

as a  $\Lambda_L$ -module. Note that this is a direct sum. Let  $h \in H$ . Since  $h \in K$  and  $K$  is normal in  $G$ ,  $\rho_i h \rho_i^{-1} \in K$  for any  $\rho_i \in G$ . Let  $x \in X_{L,\lambda}$ .

$$\begin{aligned} (10) \quad (x \otimes \rho_i)h &= x \otimes \rho_i h \\ &= x \otimes \rho_i h \rho_i^{-1} \rho_i \\ &= x^{\rho_i h \rho_i^{-1}} \otimes \rho_i \in X_{L,\lambda} \otimes \rho_i. \end{aligned}$$

Let  $x_1 \otimes \rho_1 + \cdots + x_{p^m} \otimes \rho_{p^m} \in X'$ ,  $g \in G$  and  $\gamma \in \Gamma$ . Then  $\rho_i g = k_i \rho_{\pi_g(i)}$  for some permutation  $\pi_g$  on  $\{1, \dots, p^m\}$ , where  $k_i \in K$ . Since  $\gamma$  commutes with  $k_i$ ,

we have the following equation:

$$\begin{aligned} \left(\sum x_i \otimes \rho_i\right)g\gamma &= \left(\sum x_i^{k_i} \otimes \rho_{\pi_g(i)}\right)\gamma \\ &= \left(\sum x_i^{k_i\gamma} \otimes \rho_{\pi_g(i)}\right) = \left(\sum x_i^{\gamma k_i} \otimes \rho_{\pi_g(i)}\right) \\ &= \left(\sum x_i^\gamma \otimes \rho_i\right)g = \left(\sum x_i \otimes \rho_i\right)\gamma g . \end{aligned}$$

Therefore  $\Lambda$  commute with the action of  $G$  on  $X'$ . By Lemma 3, the remark below Lemma 3, and the above equation (10), we have:

$$Hom_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[H\backslash G], X') = (X')^H = \sum (X_{L,\lambda} \otimes \rho_i)^H .$$

We have a  $\Lambda$ -module isomorphism:  $\phi : X_{L,\lambda} \otimes \rho_i \rightarrow X_{L,\lambda}$  by sending  $x \otimes \rho_i \rightarrow x$ . Again by (10),

$$\sum (X_{L,\lambda} \otimes \rho_i)^H \simeq \sum X_{L,\lambda}^{\rho_i H \rho_i^{-1}} .$$

Since  $H$  and  $\rho_i H \rho_i^{-1}$  are conjugate in  $G$ , their fixed fields are isomorphic. By Propositions 4 and 5, we have the following equation.

$$Hom_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[H\backslash G], X') \sim \bigoplus_{p^m\text{-copies}} X_{k,\lambda} .$$

By the same way, we have the following equation.

$$Hom_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[H'\backslash G], X') \sim \bigoplus_{p^m\text{-copies}} X_{k',\lambda} .$$

By Theorem 4,

$$X' \simeq \mathbb{Z}_p^{m\lambda} \oplus \text{finite } p\text{-group} .$$

Denote by  $\psi$  the map from

$$Hom_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[H'\backslash G], X')$$

to

$$Hom_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[H\backslash G], X') .$$

Since  $Hom_{\mathbb{Z}_p[G]}(A, X') \subseteq Hom_{\mathbb{Z}_p}(A, X')$  and the right-hand side is finite, the kernel of the map  $\psi$  is finite. The cokernel of the map  $\psi$ , which is a finitely generated  $\mathbb{Z}_p$ -module, is contained in  $Ext_{\mathbb{Z}_p[G]}^1(A, X')$ . By definition,  $Ext_{\mathbb{Z}_p[G]}^1(A, X')$  is killed by  $\#A$ . Hence, the cokernel is finite. Therefore we proved that  $\bigoplus_{p^m\text{-copies}} X_{k',\lambda}$  is pseudo-isomorphic to  $\bigoplus_{p^m\text{-copies}} X_{k,\lambda}$ . This implies, by the structure theorem of  $\Lambda$ -modules,  $X_{k,\lambda}$  is pseudo-isomorphic to  $X_{k',\lambda}$ . Hence we proved the theorem for  $t = m - e$ . □

*Remark.* If  $p$  does not divide  $[L : k] = [L : k']$ , then  $X_k$  is isomorphic to  $X_{k'}$ . In fact,  $p$  does not divide  $|H| = |H'|$  in the case, so  $\alpha$  in Proposition 4 is zero, and  $\mathbb{Z}_p[H\backslash G] \simeq \mathbb{Z}_p[H'\backslash G]$ , so that  $A$  is zero in the proof of Theorem 9. Therefore pseudo-isomorphisms can be replaced by isomorphisms in the above theorems and we can work with  $X_k$  instead of  $X_{k,\lambda}$ . Moreover  $t = 0$  in the case; in other words,  $X_k \simeq X_{k'}$  as  $\Lambda_k = \Lambda_{k'}$ -modules.

*Remark.* The ring  $\mathbb{Z}_p[Gal(L_\infty/L)] = \Lambda_L$  can be viewed as a subring  $\Lambda_{k,t}$  of

$$\mathbb{Z}_p[Gal(k_\infty/k)] \simeq \mathbb{Z}_p[Gal(k'_\infty/k')] = \Lambda_k$$

for some integer  $t \geq 0$ . The Iwasawa modules  $X_k$  and  $X_{k'}$  are actually  $\Lambda_k$ -modules. We showed that  $X_{k,\lambda} \sim X_{k',\lambda}$  as a  $\Lambda_L$ -module, not as a  $\Lambda_k$ -module. In general, two

$\Lambda$ -modules which are pseudo-isomorphic as  $\Lambda_t$ -modules are not necessarily pseudo-isomorphic as  $\Lambda$ -modules. Here is an example; let

$$X = \bigoplus_{p^t\text{-copies}} \Lambda/T$$

and

$$Y = \Lambda/((1 + T)^{p^t} - 1).$$

They are pseudo-isomorphic to

$$\bigoplus_{p^t\text{-copies}} \Lambda_t/Z$$

as

$$\Lambda_t = \mathbb{Z}_p[[Z]]$$

modules, where  $Z = (1 + T)^{p^t} - 1$ . However, there is a relation between the characteristic polynomials of two  $\Lambda = \mathbb{Z}_p[[T]]$ -modules which are pseudo-isomorphic as  $\Lambda_t = \mathbb{Z}_p[[ (1+T)^{p^t} - 1 ]]$ -modules. By the Weierstrass Preparation Theorem, every power series  $f(T) \in \Lambda$  can be expressed by the following way:

$$f(T) = p^m h(T)U(T),$$

where  $h(T)$  is a distinguished polynomial and  $U(T)$  is a unit in  $\Lambda$ . Let  $X$  be a finitely generated  $\Lambda$ -module. When  $X$  is considered as a  $\Lambda_t$ -module, we denote it by  $X_t$ , and its characteristic polynomial by  $char_Z(X_t)$ .

**Proposition 6.** *Let  $X$  and  $Y$  be finitely generated  $\Lambda$ -modules and let  $char(X) = p^{\mu_X} f_X(T)$  and  $char(Y) = p^{\mu_Y} f_Y(T)$ . Assume that they are pseudo-isomorphic as  $\Lambda_t$  modules. Then we have*

$$\mu_X = \mu_Y \text{ and } \prod_{\zeta} f_X(\zeta(1 + T) - 1) = \prod_{\zeta} f_Y(\zeta(1 + T) - 1),$$

where the product runs through all  $p^t$ -th roots of unity.

*Proof.* The  $\Lambda$ -module  $\Lambda/p^m$  is  $(\Lambda_t/p^m)^{p^t}$  as a  $\Lambda_t$ -module. This proves  $\mu_X = \mu_Y$ . Hence, by the structure theorem of  $\Lambda$ -modules, it is sufficient to prove the theorem in the cyclic case:  $X = \Lambda/f^n(T)$ , where  $f(T)$  is irreducible. Let  $Z = (1 + T)^{p^t} - 1$ . As a  $\Lambda_t$ -module,  $X_t$  is pseudo-isomorphic to a module of the form  $\bigoplus_{i=1}^s \Lambda_t/f_i(Z)$ . Consider  $\prod_{\zeta} f(\zeta(1 + T) - 1)$ . Then this function is in  $\mathbb{Z}_p[Z]$ . In fact, let  $f(T) = \prod_{i=0}^n (T - \alpha_i)$ ; then

$$\prod_{\zeta} f(\zeta(1 + T) - 1) = \prod_{i=0}^n (Z - w_i),$$

where  $w_i = (1 + \alpha_i)^{p^t} - 1$ . Then, we know that the  $w_i$ 's are conjugate to each other. Write  $g(Z) = \prod_{\zeta} f(\zeta(1 + T) - 1)$ . Note that  $deg_T(f) = deg_Z(g)$  and  $f^n(T)$  divides  $g^n(Z)$ . Since  $f(T)$  is irreducible,  $g(Z)$  is a power of an irreducible polynomial  $k(Z)$ , that is,  $g(Z) = k^d(Z)$ . The module  $X_t$  is killed by  $g^n(Z)$ , so each  $f_i(Z)$  divides  $g^n(Z)$ . Hence  $f_i(Z)$  is a power of the polynomial  $k(Z)$ . Therefore  $char_Z(X_t) = f_1(Z) \cdots f_s(Z)$  is a power of  $k(Z)$ . Let  $char_Z(X_t) = k^r(Z)$ . The  $\mathbb{Z}_p$ -rank of  $X$  is  $n[deg(f)]$ . As a  $\Lambda_t$ -module  $X_t$ , it has the same  $\mathbb{Z}_p$ -rank, that is,  $r[deg(k)]$ . Hence we have  $r[deg(k)] = n[deg(f)] = n[deg(g)] = nd[deg(k)]$ . From this, we have  $r = nd$ , so that  $char_Z(X_t) = k^r(Z) = k^{nd}(Z) = g^n(Z) = \prod_{\zeta} f^n(\zeta(1 + T) - 1)$ . This completes the proof, since  $X_t$  and  $Y_t$  are pseudo-isomorphic as  $\Lambda_t$ -modules, so their characteristic polynomials in  $Z$  are the same.  $\square$

*Remark.* W. Sinnott pointed out to me

$$f_i(T) = k(Z)^n \quad \text{and} \quad s = \text{deg}_T f(T) / \text{deg}_Z k(Z) .$$

The  $\mu$ -invariant is conjectured to be zero for every basic  $\mathbb{Z}_p$ -extension. Assuming the conjecture, we proved the following statement:

**Theorem 10.** *Assume that  $\mu$  is zero for every basic  $\mathbb{Z}_p$ -extension. Let  $k$  and  $k'$  be arithmetically equivalent fields, and  $p$  be a prime number. Then*

$$X_k \sim X_{k'} ,$$

as  $\Lambda_L = \Lambda_{k,t}$ -modules for some  $t$ .

6. IN THE CM FIELD CASE

A CM field is a totally imaginary quadratic extension of a totally real number field. Let  $k$  be CM,  $k_+$  its maximal real subfield. Let  $J$  denote complex conjugation. Fix an odd prime  $p$ . Recall that  $X_L$  is the Galois group of the maximal unramified abelian  $p$ -extension over the basic  $\mathbb{Z}_p$ -extension  $L_\infty$  of a number field  $L$ , and  $\Lambda = \mathbb{Z}_p[[T]]$ . Define

$$X_k^- = (1 - J)X_k .$$

In this section, we will prove

**Theorem 11.** *Let  $k$  be a CM field, and  $k'$  be a number field arithmetically equivalent to  $k$ . Then  $k'$  is a CM field, and*

$$\text{char}(X_k^-)\Lambda = \text{char}(X_{k'}^-)\Lambda .$$

Let  $\varepsilon$  be an odd quadratic Artin character of  $\text{Gal}(k/k_+)$ . Write

$$\Delta = \text{Gal}(k(\zeta_p)/k) ,$$

$$e_0 = 1/|\Delta| \sum_{\delta \in \Delta} \delta .$$

Let  $\gamma$  be a topological generator for  $\text{Gal}(k(\zeta_{p^\infty})/k(\zeta_p))$ , and let  $u \in \mathbb{Z}_p^\times$  be such that  $\zeta^\gamma = \zeta^u$  for any  $p$ -power roots of unity. There exists a quotient of power series  $G_\varepsilon(T) \in \Lambda$  such that

$$L_p(1 - s, \varepsilon\theta) = G_\varepsilon(u^s - 1) ,$$

for  $s \in \mathbb{Z}_p - \{0\}$ . Here the  $p$ -adic  $L$ -function  $L_p(s, \varepsilon\theta)$  is characterized by the following interpolation property:

$$L_p(1 - n, \varepsilon\theta) = L_{k_+}(1 - n, \varepsilon) \prod_{\mathfrak{p} \in S} (1 - \varepsilon(\mathfrak{p})N\mathfrak{p}^{n-1}) ,$$

for  $n \equiv 1 \pmod{p-1}$ , where  $S$  is the set of primes of  $k_+$  above  $p$ . To make sense of this recall that for a complex character  $\varepsilon$  we can write  $L_{k_+}(1 - n, \varepsilon)$  as a sum

$$L_{k_+}(1 - n, \varepsilon) = \sum_{\sigma \in \text{Gal}(k/k_+)} \varepsilon(\sigma) \zeta_{k_+}(\sigma, 1 - n) ,$$

where the partial zeta function  $\zeta_{k_+}(\sigma, 1 - n)$  is a rational number by a result of Klingen and Siegel. By a result of Wiles [15], we have the following

**Theorem 12.**

$$\text{char}(e_0 X_{k(\zeta_p)})^- \Lambda = G_\varepsilon(u(1 + T)^{-1} - 1)\Lambda .$$

**Lemma 5.** *Let  $k$  be a CM field, and  $k'$  be a number field arithmetically equivalent to  $k$ . Then  $k'$  is a CM field, and*

$$\zeta_{k_+} = \zeta_{k'_+} .$$

*Proof.* Let  $L$  be the Galois closure of  $k$ . Then  $L$  is a CM field. Write  $H = Gal(L/k)$  and  $H' = Gal(L/k')$ . Since the complex conjugation  $J$  is a center of  $Gal(L/\mathbb{Q})$ , the fixed field of  $H \times \langle J \rangle$  is the maximal real subfield  $k_+$ . We know that  $k'$  is totally imaginary because  $k'$  is arithmetically equivalent to  $k$ . By assumption,  $H$  and  $H'$  are Gassmann equivalent; hence

$$|c^G \cap H| = |c^G \cap H'|,$$

for any  $c \in G$ . Note that  $c^G \cap H \times \langle J \rangle$  is a disjoint union of  $c^G \cap H$  and  $c^G \cap HJ$  for any  $c \in G$ . Since the map given by  $gcg^{-1} \rightarrow gcJg^{-1}$  is injective, we have

$$|c^G \cap H| = |(cJ)^G \cap HJ| .$$

Therefore

$$\begin{aligned} |c^G \cap HJ| &= |((cJ)J)^G \cap HJ| = |(cJ)^G \cap H| \\ &= |(cJ)^G \cap H'| = |(cJJ)^G \cap H'J| = |c^G \cap H'J|. \end{aligned}$$

Hence

$$\begin{aligned} |c^G \cap H \langle J \rangle| &= |c^G \cap H| + |c^G \cap HJ| \\ &= |c^G \cap H'| + |c^G \cap H'J| = |c^G \cap H' \langle J \rangle|. \end{aligned}$$

Therefore,  $H \langle J \rangle$ ,  $H' \langle J \rangle$  are Gassmann equivalent, which means the number field  $k'$  has a totally real subfield  $k'_+$  arithmetically equivalent to  $k_+$ . This completes the proof. □

*Proof of Theorem 11.* By Theorem 12 and the discussion above Theorem 12,  $char(e_0X_{k(\zeta_p)})^-$  is determined by  $L$ -function  $L_{k_+}(s, \varepsilon)$ . By Lemma 5,

$$L_{k_+}(s, \varepsilon) = \zeta_k / \zeta_{k_+} = \zeta_{k'} / \zeta_{k'_+} = L_{k'_+}(s, \varepsilon).$$

This completes the proof by the lemma below. □

**Lemma 6.**

$$e_0X_{k(\zeta_p)} \simeq X_k.$$

*Proof.* Let  $L_{\infty, k(\zeta_p)}$  be the maximal unramified abelian  $p$ -extension of  $k(\zeta_p)_\infty$ . Let  $Y_0$  be the subfield of  $L_{\infty, k(\zeta_p)}$  fixed by the subgroup  $e_0X_{k(\zeta_p)}$  of  $X_{k(\zeta_p)}$ . Since  $Gal(k(\zeta_p)/k)$  acts trivially on  $e_0X_{k(\zeta_p)}$ ,  $Y_0$  is the maximal abelian extension of the basic  $\mathbb{Z}_p$ -extension  $k_\infty$  of  $k$  contained in  $L_{\infty, k(\zeta_p)}$ . Hence the compositum  $K_\infty L_{\infty, k}$  is contained in  $Y_0$ . Suppose it is properly contained in  $Y_0$ . Then we can construct an unramified abelian  $p$ -extension  $L'$  over  $k_\infty$  properly containing  $L_{\infty, k}$  since  $p \nmid |Gal(k(\zeta_p)/k)|$ , which contradicts the maximality of the extension  $L_{\infty, k}$ . This completes the proof. □

## REFERENCES

1. N.Adachi and K.Komatsu, *The Maximal  $p$ -extensions and Zeta-Functions of Algebraic Number Fields*, Memoirs of the School of Science & Engineering Waseda Univ. **51** (1987), 25–31. MR **90a**:11135
2. B. Ferrero and L.Washington, *The Iwasawa invariant  $\mu_p$  vanishes for abelian number fields*, Ann. of Math. **109** (1979), 377–395. MR **81a**:12005
3. F.Gassmann, *Bererkungen zu der vorstehenden arbeit von Hurwitz*, Math.Z. **25** (1926), 124–143.
4. D.Goss and W.Sinnott, *Special Values of Artin  $L$ -series*, Math. Ann. **275** (1986), 529–537. MR **87k**:11127
5. K.Iwasawa, *On  $p$ -adic  $L$ -functions*, Ann. of Math. **89** (1969), 198–205. MR **42**:4522
6. K.Iwasawa, *On  $\mathbb{Z}_\ell$ -extensions of algebraic number fields*, Ann. of Math. **98** (1973), 246–326. MR **15**:509d
7. K.Iwasawa, *On the  $\mu$ -invariants of  $\mathbb{Z}_\ell$ -extensions*, Number Theory, Algebraic Geometry and Commutative Algebra (in honor of Y. Akizuki), Kinokuniya, Tokyo, 1973, pp. 1–11. MR **50**:9839
8. K.Komatsu, *On Zeta-functions and cyclotomic  $\mathbb{Z}_p$ -extensions of algebraic number fields*, Tôhoku Math. Journ. **36** (1984), 555–562. MR **86a**:11046
9. R.Perlis, *On the equation  $\zeta_k = \zeta_{k'}$* , J. Number Theory **9** (1977), 342–360. MR **56**:5503
10. R.Perlis, *On the class numbers of arithmetically equivalent fields*, J. Number Theory **10** (1978), 489–509. MR **80c**:12014
11. R.Perlis and N.Colwell, *Iwasawa Invariants and Arithmetic Equivalence*, unpublished.
12. J.Tate, *Endomorphism of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144. MR **34**:5829
13. S.Turner, *Adele rings of global field of positive characteristic*, Bol. Soc. Brasil. Math. **9** (1978), 89–95. MR **80c**:12017
14. L.Washington, *Introduction to Cyclotomic Fields*, Springer, Berlin, Heidelberg, New York, 1982. MR **85g**:11001
15. A.Wiles, *The Iwasawa conjecture for totally real fields*, Ann. of Math. **131** (1990), 493–540. MR **91i**:11163

DEPARTMENT OF MATHEMATICS, OHIO STATE UNIVERSITY, COLUMBUS, OHIO 43210  
*Current address:* KIAS, 207-43 Cheongryangri-Dong, Dongdaemun-Gu, Seoul 130-012, Korea  
*E-mail address:* ohj@kias.kaist.ac.kr