Osaka University Knowledge Archive

Title	ON TAMELY RAMIFIED IWASAWA MODULES FOR THE CYCLOTOMIC Z_p-EXTENSION OF ABELIAN FIELDS
Author(s)	Itoh, Tsuyoshi
Citation	Osaka Journal of Mathematics. 2014, 51(2), p. 513-536
Version Type	VoR
URL	https://doi.org/10.18910/29204
rights	
Note	

Osaka University Knowledge Archive : OUKA

https://ir.library.osaka-u.ac.jp/

Osaka University

Itoh, T.
Osaka J. Math.
51 (2014), 513–536

ON TAMELY RAMIFIED IWASAWA MODULES FOR THE CYCLOTOMIC $\mathbb{Z}_p$-EXTENSION OF ABELIAN FIELDS

TSUYOSHI ITOH

(Received May 18, 2012, revised September 19, 2012)

Abstract

Let p be an odd prime, and k_∞ the cyclotomic $\mathbb{Z}_p$-extension of an abelian field k. For a finite set S of rational primes which does not include p, we will consider the maximal S-ramified abelian pro-p extension $M_S(k_\infty)$ over k_∞. We shall give a formula of the $\mathbb{Z}_p$-rank of $\mathrm{Gal}(M_S(k_\infty)/k_\infty)$. In the proof of this formula, we also show that $M_{\{q\}}(k_\infty)/L(k_\infty)$ is a finite extension for every real abelian field k and every rational prime q distinct from p, where $L(k_\infty)$ is the maximal unramified abelian pro-p extension over k_∞.

1. Introduction

Let k be an algebraic number field, and p a prime number. We denote by k_∞/k the cyclotomic $\mathbb{Z}_p$-extension (i.e. the unique $\mathbb{Z}_p$-extension contained in the field generated by all p-power roots of unity over k). Let S be a finite set of *rational* primes, and $\tilde{M}_S(k_\infty)$ the maximal pro-p extension of k_∞ unramified outside S (i.e., the primes of k_∞ lying above the primes in S are only allowed to ramify in $\tilde{M}_S(k_\infty)/k_\infty$).

When $p \in S$, the structure of $\tilde{X}_S(k_\infty) = \mathrm{Gal}(\tilde{M}_S(k_\infty)/k_\infty)$ is already studied (see, e.g., Iwasawa [8], Neukirch–Schmidt–Wingberg [11]). In particular, $\tilde{X}_S(k_\infty)$ is a free pro-p group under certain conditions.

Recently, the structure of $\tilde{X}_S(k_\infty)$ for the case that $p \notin S$ is also studied by several authors (Salle [12], Mizusawa–Ozaki [10], ...). In this case, it seems that $\tilde{X}_S(k_\infty)$ does not have a simple structure. Then, to study $\tilde{X}_S(k_\infty)$, it is important to study the structure of its abelian quotient. Let $M_S(k_\infty)/k_\infty$ be the maximal abelian pro-p extension unramified outside S. In the present paper, we shall consider $X_S(k_\infty) = \mathrm{Gal}(M_S(k_\infty)/k_\infty)$ for the case that $p \notin S$. Since $\mathrm{Gal}(k_\infty/k)$ acts on $X_S(k_\infty)$, we can use Iwasawa theoretic arguments. $X_S(k_\infty)$ is called the S-ramified Iwasawa module. (See, e.g., [12], [6]. This is also called a "tamely ramified Iwasawa module" when $p \notin S$.)

If a $\mathbb{Z}_p$-module M satisfies $\dim_{\mathbb{Q}_p} M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = r < \infty$, we say that the $\mathbb{Z}_p$-rank of M is r, and we write $\mathrm{rank}_{\mathbb{Z}_p} M = r$. Our purpose of the present paper is giving a formula of $\mathrm{rank}_{\mathbb{Z}_p} X_S(k_\infty)$ when k is an abelian extension of $\mathbb{Q}$ (abelian field) and p is an odd prime. (In this case, we can show that $X_S(k_\infty)$ is finitely generated over $\mathbb{Z}_p$.)

2010 Mathematics Subject Classification. Primary 11R23; Secondary 11R18.

We shall give a remark about "giving a formula of $\mathrm{rank}_{\mathbb{Z}_p} X_S(k_\infty)$". Let $L(k_\infty)$ be the maximal unramified abelian pro-p extension of k_∞. We put $X(k_\infty) = \mathrm{Gal}(L(k_\infty)/k_\infty)$. Then $X(k_\infty)$ is the (usual) Iwasawa module, and $\lambda = \mathrm{rank}_{\mathbb{Z}_p} X(k_\infty)$ is called the Iwasawa λ-invariant. In general, it is hard to write λ explicitly. Since $X(k_\infty)$ is a quotient of $X_S(k_\infty)$, we consider it is sufficient to obtain a formula including λ at the present time. (That is, we will only give a formula of $\mathrm{rank}_{\mathbb{Z}_p} \mathrm{Gal}(M_S(k_\infty)/L(k_\infty))$, actually.) However, for abelian fields, the "plus part" of λ is conjectured to be 0 (Greenberg's conjecture), and the "minus part" of λ can be computed (at least theoretically) from the Kubota–Leopoldt p-adic L-functions (Stickelberger elements).

We also mention that formulas of $\mathrm{rank}_{\mathbb{Z}_p} X_S(k_\infty)$ are already obtained for several cases. In particular, it can be said that the $\mathbb{Z}_p$-rank of the "minus part" of $X_S(k_\infty)$ for CM-fields is already known (see Section 2). Salle [12] studied $X_S(k_\infty)$ for the case that k is an imaginary quadratic field (or $\mathbb{Q}$) with $p = 2$. Moreover, when $k = \mathbb{Q}$, a formula of $\mathrm{rank}_{\mathbb{Z}_p} X_S(\mathbb{Q}_\infty)$ (including the case that $p = 2$) is shown by Mizusawa, Ozaki, and the author [6] (as a corollary, a general formula for imaginary quadratic fields is also given). In the present paper, we shall extend the method given in [6] for abelian fields. The following theorem is crucial to prove the formula of $\mathrm{rank}_{\mathbb{Z}_p} X_S(\mathbb{Q}_\infty)$.

Theorem A (see [6, Theorem 3.1]). *Let q be a rational prime distinct from p. Then $M_{\{q\}}(\mathbb{Q}_\infty)/\mathbb{Q}_\infty$ is a finite extension.*

At first, we will generalize Theorem A to real abelian fields (under the condition that p is an odd prime).

Theorem 1.1. *Assume that p is odd. Let k be a real abelian field, and q a rational prime distinct from p. Then $M_{\{q\}}(k_\infty)/L(k_\infty)$ is a finite extension.*

We remark that $M_{\{q\}}(k_\infty)/L(k_\infty)$ can be infinite when k is an imaginary abelian filed. (For example, see [12], [9], [6], or Section 6 of the present paper.) Similar to [6], Theorem 1.1 plays an important role to prove our formula of $\mathrm{rank}_{\mathbb{Z}_p} X_S(k_\infty)$ for abelian fields.

In Section 2, we shall state some basic facts, and give preparations for proving Theorem 1.1. We will prove Theorem 1.1 in Sections 3 and 4. In Section 5, we shall give a simple remark about a generalization of Theorem 1.1. In Section 6, we shall give a formula of $\mathrm{rank}_{\mathbb{Z}_p} X_S(K_\infty)$ for abelian fields (Theorem 6.4). The formula is given as the "χ-quotient" version. We also give examples with applying this formula for some simple cases.

2. Preliminaries

Firstly, we shall recall some basic facts from class field theory. Let p be an odd prime number, and k an algebraic number field. (In the following of the present paper, we assume that p is odd.) We denote by k_∞/k the cyclotomic $\mathbb{Z}_p$-extension. For a

non-negative integer n, let k_n be the nth layer of k_∞/k (that is, the unique subfield of k_∞ such that k_n/k is a cyclic extension of degree p^n). Let S be a finite set of rational primes which does not include p. For an algebraic extension (not necessary finite) $\mathcal{K}$ of $\mathbb{Q}$, let $M_S(\mathcal{K})$ be the maximal abelian (pro-)p-extension of $\mathcal{K}$ unramified outside S, and $L(\mathcal{K})$ the maximal unramified abelian (pro-)p-extension of $\mathcal{K}$. For an abelian group G, let $\hat{G}$ be the p-adic completion of G (that is, $\hat{G} = \varprojlim G/G^{p^n}$).

As noted in Section 1, we shall mainly consider the $\mathbb{Z}_p$-rank of $\mathrm{Gal}(M_S(k_\infty)/L(k_\infty))$. We will write several facts which is also stated in [6]. In this paragraph, assume that S is not empty. By class field theory, we have the following exact sequence:

$$\hat{E}_{k_n} \xrightarrow{\eta_n} \bigoplus_{q\in S} \widehat{(O_{k_n}/q)^\times} \to \mathrm{Gal}(M_S(k_n)/L(k_n)) \to 0,$$

where E_{k_n} is the group of units of k_n, O_{k_n} is the ring of integers of k_n, and η_n is the natural homomorphism induced from the diagonal embedding. (We will give a remark on the structure of $\widehat{(O_{k_n}/q)^\times}$. Assume that the prime decomposition of qO_{k_n} is $\mathfrak{q}_1^{e_1}\cdots\mathfrak{q}_r^{e_r}$. Then

$$\widehat{(O_{k_n}/q)^\times} \cong \bigoplus_{i=1}^{r} \widehat{(O_{k_n}/\mathfrak{q}_i)^\times}$$

because $\widehat{(O_{k_n}/\mathfrak{q}_i^{e_i})^\times} \cong \widehat{(O_{k_n}/\mathfrak{q}_i)^\times}$.) We put $E_\infty = \varprojlim \hat{E}_{k_n}$, and $R_q = \varprojlim \widehat{(O_{k_n}/q)^\times}$, where the projective limits are taken with respect to the natural mappings induced from the norm mapping. Then we obtain the following exact sequence:

$$E_\infty \xrightarrow{\eta_\infty} \bigoplus_{q\in S} R_q \to \mathrm{Gal}(M_S(k_\infty)/L(k_\infty)) \to 0.$$

In the cyclotomic $\mathbb{Z}_p$-extension, all (finite) primes of k are finitely decomposed. Then R_q is a finitely generated $\mathbb{Z}_p$-module. From this, we also see $\mathrm{Gal}(M_S(k_\infty)/L(k_\infty))$ is finitely generated over $\mathbb{Z}_p$. On the other hand, the theorem of Ferrero–Washington [2] implies that $\mathrm{Gal}(L(k_\infty)/k_\infty)$ is a finitely generated $\mathbb{Z}_p$-module, if k is an abelian field. Hence, we see that for every abelian field k, $X_S(k_\infty)$ is finitely generated over $\mathbb{Z}_p$. (We can see that the $\mathbb{Z}_p$-rank of $X_S(k_\infty)$ is always finite in general.) It seems hard to determine the cokernel of η_∞ directly.

REMARK. When the base field k is a CM-field, the minus part of E_∞ is easy to compute (we are also able to compute the minus part of R_q). Hence we can obtain a formula of the $\mathbb{Z}_p$-rank of the minus part of $\mathrm{Gal}(M_S(k_\infty)/L(k_\infty))$. This idea is already known (see, e.g., [12], [9], [6]).

Secondly, we shall give some preparations to prove Theorem 1.1. Let be a prime number satisfying $q \neq p$. For simplicity, we will write $M_p(\cdot)$, $M_q(\cdot)$ instead of $M_{\{p\}}(\cdot)$, $M_{\{q\}}(\cdot)$, respectively.

Lemma 2.1. *Let k'/k be a finite extension of algebraic number fields. If* $\mathrm{Gal}(M_q(k'_\infty)/L(k'_\infty))$ *is finite, then* $\mathrm{Gal}(M_q(k_\infty)/L(k_\infty))$ *is also finite.*

Proof. We may assume that $k' \cap k_\infty = k$. Let

$$N_n : \widehat{(O_{k'_n}/q)^\times} \to \widehat{(O_{k_n}/q)^\times}$$

be the homomorphism induced from the norm mapping. We can see that the order of the cokernel $\mathrm{Coker}(N_n)$ is bounded as $n \to \infty$. (Proof: Since there are only finitely many primes in k_∞ lying above q, the p-rank of $\widehat{(O_{k_n}/q)^\times}$ is bounded. Moreover, the exponent of $\mathrm{Coker}(N_n)$, is also bounded.) Since $\mathrm{Gal}(M_q(k'_n)/L(k'_n))$ (resp. $\mathrm{Gal}(M_q(k_n)/L(k_n))$) is isomorphic to a quotient of $\widehat{(O_{k'_n}/q)^\times}$ (resp. $\widehat{(O_{k_n}/q)^\times}$), N_n induces the homomorphism $\mathrm{Gal}(M_q(k'_n)/L(k'_n)) \to \mathrm{Gal}(M_q(k_n)/L(k_n))$. From the above fact, the order of the cokernel is bounded as $n \to \infty$.

Assume that $\mathrm{Gal}(M_q(k'_\infty)/L(k'_\infty))$ is finite. Then we can show that the order of $\mathrm{Gal}(M_q(k'_n)/L(k'_n))$ is bounded as $n \to \infty$. From the above fact, we see that the order of $\mathrm{Gal}(M_q(k'_n)/L(k'_n))$ is also bounded. Hence $\mathrm{Gal}(M_q(k_\infty)/L(k_\infty))$ is finite. □

From Lemma 2.1 and the theorem of Kronecker–Weber, we may replace a real abelian field k to the maximal real subfield of a cyclotomic filed containing k to show Theorem 1.1. For a positive integer d, let μ_d be the set of all dth roots of unity, and $\mathbb{Q}(\mu_d)$ the dth cyclotomic field.

Lemma 2.2. *Let f be a positive integer which is prime to p, and m a positive integer. We put $K = \mathbb{Q}(\mu_{fp^m})$ and $k = K^+$ (the maximal real subfield of K). If q does not split in K/k, then $M_q(k_\infty) = L(k_\infty)$.*

Proof. Let $\mathfrak{q}$ be an arbitrary prime of k lying above q. It is well known that if $\mathfrak{q}$ does not split in K, then the order of $(O_k/\mathfrak{q})^\times$ is not divisible by p. (Proof: We denote by $k_\mathfrak{q}$ the completion of k at $\mathfrak{q}$. Under the assumption, $k_\mathfrak{q}$ does not contain μ_p. By the structure of the group of units in $k_\mathfrak{q}$, we obtain the assertion.) Since $\mathrm{Gal}(M_q(k)/L(k))$ is isomorphic to a quotient of $(O_k/\mathfrak{q})^\times$, we see $M_q(k) = L(k)$.

We note that the nth layer k_n of k_∞/k is the maximal real subfield of $\mathbb{Q}(\mu_{fp^{m+n}})$. Hence by using the same argument, we also see $M_q(k_n) = L(k_n)$ for all $n \geq 1$. This implies that $M_q(k_\infty) = L(k_\infty)$. □

From the above arguments, it is sufficient to prove Theorem 1.1 under the following conditions:

(A) k is the maximal real subfield of $K = \mathbb{Q}(\mu_{fp^m})$, where f and m are positive integers and f is prime to p. Every prime lying above q splits in K/k, and is not decomposed in k_∞/k (the latter can be satisfied by taking m sufficiently large).

3. Properties of certain Kummer extensions

In this section, we shall give some key results to prove Theorem 1.1. Assume that K, k, and q satisfy (A) in Section 2. We will construct certain infinite Kummer extensions over K_∞. We shall use some fundamental results given in Khare–Wintenberger [9].

We define the terms Case NS and Case S as follows:

CASE NS: every prime lying above p does not split in K/k.

CASE S: every prime lying above p splits in K/k.

Moreover, we use the following notation (in Sections 3 and 4):

- J: complex conjugation,
- $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$: prime ideals of k lying above q,
- $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$: prime ideals of k lying above p,
- $\mathfrak{Q}_i, \mathfrak{Q}_i^J$ $(i = 1, \ldots, r)$: prime ideals of K lying above $\mathfrak{q}_i$,
- $\mathfrak{P}_j$ $(j = 1, \ldots, t)$: (unique) prime ideal of K lying above $\mathfrak{p}_j$ (Case NS),
- $\mathfrak{P}_j, \mathfrak{P}_j^J$ $(j = 1, \ldots, t)$: prime ideals of K lying above $\mathfrak{p}_j$ (Case S).

Following Greenberg [3], we denote by s the number of primes of k which is lying above p and splits in K. Hence we see that $s = 0$ for Case NS, and $s = t$ for Case S. Note that every prime lying above p are totally ramified in k_∞/k by the assumption on k. Hence s is also the number of primes of k_∞ which is lying above p and splits in K_∞.

By the assumption, K_∞ contains all p^nth roots of unity. For an element x of $K^\times$, we define

$$K_\infty(\sqrt[p^\infty]{x}) = \bigcup_{n \geq 1} K_\infty(\sqrt[p^n]{x}).$$

More precisely, $K_\infty(\sqrt[p^\infty]{x})$ is the union of all finite Kummer extensions $K_n(\sqrt[p^n]{x})$ for $n \geq 1$ (note that K_n contains μ_{p^n}). Similarly, for a finitely generated subgroup T of $K^\times$, we define the extension $K_\infty(\sqrt[p^\infty]{T})/K_\infty$ by adjoining all p^nth roots of the elements contained in T. As noted in [9], $K_\infty(\sqrt[p^\infty]{x}) = K_\infty$ if and only if x is a root of unity.

The following result is helpful to prove the results stated in this section.

Theorem B (see Khare–Wintenberger [9, Lemma 2.5]). *Let T be a finitely generated subgroup of $K^\times$, and S a finite set of (finite) primes of K. Let $\mathcal{I}$ be the subgroup of* $\mathrm{Gal}(K_\infty(\sqrt[p^\infty]{T})/K_\infty)$ *generated by the inertia subgroups for the primes in S. For a prime $\mathfrak{r} \in S$, let $K_\mathfrak{r}$ be the completion of K at $\mathfrak{r}$. We denote by $\mathcal{T}$ the closure of the diagonal image of T in $\prod_{\mathfrak{r} \in S} \hat{K}_\mathfrak{r}^\times$. (Recall that $\hat{K}_\mathfrak{r}^\times$ is the p-adic completion of $K_\mathfrak{r}^\times$.) Then* $\mathrm{rank}_{\mathbb{Z}_p} \mathcal{I} = \mathrm{rank}_{\mathbb{Z}_p} \mathcal{T}$.

We shall construct several Kummer extensions unramified outside $\{p, q\}$ over K_∞ by following the method given in [6]. (See also Greenberg [4].) Let k^D be the decomposition field of $K/\mathbb{Q}$ for q. By the assumption, k^D is an imaginary abelian field and $[k^D : \mathbb{Q}] = 2r$. Let $Q_1, \ldots, Q_r, Q_1^J, \ldots, Q_r^J$ be the primes of k^D lying below $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_r, \mathfrak{Q}_1^J, \ldots, \mathfrak{Q}_r^J$ respectively. We can take a positive integer h such that

- Q_1^h is a principal ideal generated by α_1, and
- $\alpha_1 - 1 \in P$ for every prime ideal P of k^D lying above p.

We note that Q_1^σ ($\sigma \in \mathrm{Gal}(k^D/\mathbb{Q})$) is the complete set of primes in k^D lying above q, and $(Q_1^\sigma)^h = (\alpha_1^\sigma)$. We write all conjugates of α_1 for $\mathrm{Gal}(k^D/\mathbb{Q})$ as the following:

$$\alpha_1, \alpha_2, \ldots, \alpha_r, \alpha_1^J, \alpha_2^J, \ldots, \alpha_r^J$$

(these are distinct elements because q splits completely in k^D). Moreover, we put $\beta_i = \alpha_i/\alpha_i^J$ for $i = 1, \ldots, r$.

For Case S (i.e. p splits in K/k), we define $\rho_1, \ldots, \rho_t \in K^\times$ as follows. We can take an integer h' such that $\mathfrak{P}_j^{h'} = (\pi_j)$ for all $j = 1, \ldots, t$. We put $w_j = |(O_K/\mathfrak{P}_j)^\times|$ and $\rho_j = (\pi_j/\pi_j^J)^{w_j}$ for $j = 1, \ldots, t$.

DEFINITION. We put

$$T_q = \langle \beta_i \mid i = 1, \ldots, r \rangle,$$

which is a subgroup of $(k^D)^\times$ (and hence also a subgroup of $K^\times$). For Case NS, we put $T = T_q$. For Case S, we put

$$T = \langle \beta_i, \rho_j \mid i = 1, \ldots, r,\ j = 1, \ldots, t \rangle.$$

Moreover, we put $N_q = K_\infty(\sqrt[p^\infty]{T_q})$ and $N = K_\infty(\sqrt[p^\infty]{T})$. (Of course, $N = N_q$ for Case NS.)

Lemma 3.1. (1) *N and N_q are abelian extensions over k_∞.*
(2) *N/K_∞ and N_q/K_∞ are unramified outside $\{p, q\}$.*
(3) $\mathrm{Gal}(N/K_\infty) \cong \mathbb{Z}_p^{\oplus r+s}$ *and* $\mathrm{Gal}(N_q/K_\infty) \cong \mathbb{Z}_p^{\oplus r}$. (*Recall that $s = 0$ for* Case NS, *and $s = t$ for* Case S.)

Proof. (1) Since J acts on T as -1, then J acts on $\mathrm{Gal}(N/K_\infty)$ and the action is trivial. This implies that N/k_∞ is an abelian extension. The assertion for N_q follows similarly.

(2) Note that all elements contained in T (resp. T_q) are $\{p, q\}$-units. Hence N/K_∞ (resp. N_q/K_∞) is unramified outside $\{p, q\}$. (See, e.g., [9, Proposition 2.4].)

(3) It is easy to see that T is a free $\mathbb{Z}$-module of rank $r + s$. Let $\hat{T}$ be the closure of T in $\hat{K}^\times$. Then the $\mathbb{Z}_p$-rank of $\hat{T}$ is $r + s$. As noted in [9] (see Remarks

after the proof of [9, Lemma 2.2]), this fact implies that $\mathrm{rank}_{\mathbb{Z}_p} \mathrm{Gal}(N/K_\infty) = r + s$. Since $\mathrm{Gal}(N/K_\infty)$ is generated by $r + s$ elements, we see that $\mathrm{Gal}(N/K_\infty) \cong \mathbb{Z}_p^{\oplus r+s}$. The assertion for $\mathrm{Gal}(N_q/K_\infty)$ can be proven quite similarly. □

Lemma 3.2 (cf. Greenberg [4]). (1) *For every $i = 1, \ldots, r$, the unique prime lying above $\mathfrak{Q}_i$ is ramified in $K_\infty(\sqrt[p^\infty]{\beta_i})/K_\infty$.*
(2) *$N_q \cap M_p(K_\infty)$ is a finite extension over K_∞.*

Proof. The assertions can be shown easily by using Theorem B. Note that (2) is already mentioned in [4, p. 149]. □

Proposition 3.3. *Let $\mathcal{I}_p$ be the subgroup of $\mathrm{Gal}(N/K_\infty)$ generated by all inertia groups for the prime lying above p. Then $\mathcal{I}_p$ has finite index in $\mathrm{Gal}(N/K_\infty)$.*

Proof. First, we consider Case NS. We assume that p does not split in K/k. Hence $s = 0$, $T = T_q$, $N = N_q$, and there are just t primes in K lying above p. By Lemma 3.1, it is sufficient to show that $\mathrm{rank}_{\mathbb{Z}_p} \mathcal{I}_p = r$. Let $\mathcal{T}_q$ be the closure of the diagonal image of T_q in $\prod_{j=1}^t \hat{K}_{\mathfrak{P}_j}^\times$. By Theorem B, we see that $\mathrm{rank}_{\mathbb{Z}_p} \mathcal{I}_p = \mathrm{rank}_{\mathbb{Z}_p} \mathcal{T}_q$, hence we shall show $\mathrm{rank}_{\mathbb{Z}_p} \mathcal{T}_p = r$.

Recall that k^D is the decomposition field of $K/\mathbb{Q}$ for q, and T_q is also a subgroup of $(k^D)^\times$. We denote by $P_1, \ldots, P_u$ the primes of k^D lying above p (where $u \le t$). Let $\mathcal{T}_q'$ be the closure of the diagonal image of T_q in $\prod_{h=1}^u \widehat{(k_{P_h}^D)^\times}$.

We claim that $\mathrm{rank}_{\mathbb{Z}_p} \mathcal{T}_q' = \mathrm{rank}_{\mathbb{Z}_p} \mathcal{T}_q$. By the definition of T_q, every element x of T_q satisfies $x - 1 \in P_h$ for all $h = 1, \ldots, u$. Let $\mathcal{U}_{P_h}^1$ be the group of principal units of $k_{P_h}^D$. We see that $\mathcal{T}_q'$ is contained in $\prod_{h=1}^u \mathcal{U}_{P_h}^1$. Let ι be the homomorphism

$$\prod_{h=1}^u \mathcal{U}_{P_h}^1 \to \prod_{j=1}^t \mathcal{U}_{\mathfrak{P}_j}^1$$

induced from the diagonal embedding $\mathcal{U}_{P_h}^1 \to \prod_{\mathfrak{P}|p_h} \mathcal{U}_{\mathfrak{P}}^1$. We can see that ι is injective, and $\iota(\mathcal{T}_q') = \mathcal{T}_q$. Then the claim follows.

We shall recall the argument given in Brumer's proof of Leopoldt's conjecture for abelian fields (see [1], [15]). Assume that $\mathrm{rank}_{\mathbb{Z}_p} \mathcal{T}_q' < r$. Then there are elements $a_1, \ldots, a_r$ of $\mathbb{Z}_p$ which satisfies

$$\beta_1^{a_1} \beta_2^{a_2} \cdots \beta_r^{a_r} = 1 \quad \text{in} \quad \mathcal{U}_{P_h}^1$$

for all $h = 1, \ldots, u$, and $a_i \neq 0$ with some i. Since $\beta_i = \alpha_i/\alpha_i^J$ and α_i is a conjugate of α_1, we also see that

$$\prod_{\sigma \in \mathrm{Gal}(k^D/\mathbb{Q})} (\alpha_1^{\sigma\tau^{-1}})^{\chi(\sigma)} = 1 \quad \text{in} \quad \mathcal{U}_{P_1}^1$$

for all $\tau \in \mathrm{Gal}(k^D/\mathbb{Q})$, where $x(\sigma) \in \mathbb{Z}_p$ satisfying $x(\sigma) \neq 0$ with some σ. Fix an embedding $k^D_{P_1} \to \mathbb{C}_p$. By taking the p-adic logarithm of the above equation, we see

$$\sum_{\sigma \in \mathrm{Gal}(k^D/\mathbb{Q})} x(\sigma) \log_p \alpha_1^{\sigma\tau^{-1}} = 0.$$

This implies that the determinant of the matrix $(\log_p \alpha_1^{\sigma\tau^{-1}})_{\sigma,\tau}$ is 0.

On the other hand, $\alpha_1, \ldots, \alpha_r, \alpha_1^J, \ldots, \alpha_r^J$ are multiplicative independent in $(k^D)^\times$. Then we can see that $\log_p \alpha_1, \ldots, \log_p \alpha_r, \log_p \alpha_1^J, \ldots, \log_p \alpha_r^J$ are linearly independent over $\mathbb{Q}$. By Baker–Brumer's theorem (see Brumer [1], Washington [15, Theorem 5.29]), they are also linearly independent over $\overline{\mathbb{Q}}$ in $\mathbb{C}_p$. Hence the determinant of the matrix $(\log_p \alpha_1^{\sigma\tau^{-1}})_{\sigma,\tau}$ is *not* 0. (This follows from the argument given in the proof of [6, Lemma 3.4] which uses [15, Lemma 5.26 (a)].) It is a contradiction. Then we conclude that

$$\mathrm{rank}_{\mathbb{Z}_p} \mathcal{T}_q' = \mathrm{rank}_{\mathbb{Z}_p} \mathcal{T}_q = \mathrm{rank}_{\mathbb{Z}_p} \mathcal{I}_p = r.$$

Next, we shall consider Case S. Assume that p splits in K/k. That is, $s = t$ and the number of primes of K lying above p is $2t$. The outline of the proof is the same as Case NS. Let $\mathcal{T}$ be the closure of the diagonal image of T in $\prod_{j=1}^t \hat{K}^\times_{\mathfrak{P}_j} \times \prod_{j=1}^t \hat{K}^\times_{\mathfrak{P}_j^J}$. In this case, we shall show $\mathrm{rank}_{\mathbb{Z}_p} \mathcal{T} = r + t$.

Assume that $\mathrm{rank}_{\mathbb{Z}_p} \mathcal{T} < r + t$. Then there are elements $a_1, \ldots, a_{r+t}$ of $\mathbb{Z}_p$ which satisfies

$$\beta_1^{a_1} \beta_2^{a_2} \cdots \beta_r^{a_r} \rho_1^{a_{r+1}} \rho_2^{a_{r+2}} \cdots \rho_t^{a_{r+t}} = 1 \quad \text{in} \quad \hat{K}^\times_{\mathfrak{P}_j},$$

and

$$\beta_1^{a_1} \beta_2^{a_2} \cdots \beta_r^{a_r} \rho_1^{a_{r+1}} \rho_2^{a_{r+2}} \cdots \rho_t^{a_{r+t}} = 1 \quad \text{in} \quad \hat{K}^\times_{\mathfrak{P}_j^J}$$

for all $1 \leq j \leq t$, and $a_i \neq 0$ with some i. However, $v_{\mathfrak{P}_j}(\rho_j) \neq 0$ (for $1 \leq j \leq t$) by the definition of ρ_j. (Here, $v_{\mathfrak{P}_j}$ is the normalized additive valuation of K with respect to $\mathfrak{P}_j$.) This fact implies that a_{r+j} must be 0 for $1 \leq j \leq t$. Hence we obtain the equalities

$$\beta_1^{a_1} \beta_2^{a_2} \cdots \beta_r^{a_r} = 1 \quad \text{in} \quad \mathcal{U}^1_{\mathfrak{P}_j},$$

and

$$\beta_1^{a_1} \beta_2^{a_2} \cdots \beta_r^{a_r} = 1 \quad \text{in} \quad \mathcal{U}^1_{\mathfrak{P}_j^J}$$

for all $1 \leq j \leq t$. Recall that k^D is the decomposition field of $K/\mathbb{Q}$ for q. We denote by $P_1, \ldots, P_u$ the primes of k^D lying above p. As noted before (in the proof for Case NS), we can show $\mathcal{U}^1_{P_h} \to \prod_{\mathfrak{P}|P_h} \mathcal{U}^1_{\mathfrak{P}}$ is injective. Hence we see

$$\beta_1^{a_1} \beta_2^{a_2} \cdots \beta_r^{a_r} = 1 \quad \text{in} \quad \mathcal{U}^1_{P_h}$$

for all $1 \leq h \leq u$, and $a_i \neq 0$ with some i. The rest of the proof is quite same as that of for Case NS. $\square$

Since N is an abelian extension of k_∞, we can take a unique intermediate field N^+ of N/k_∞ which satisfies $\mathrm{Gal}(N^+/k_\infty) \cong \mathbb{Z}_p^{\oplus r+s}$. Similarly, we are also able to take a unique intermediate field N_q^+ of N_q/k_∞ satisfying $\mathrm{Gal}(N_q^+/k_\infty) \cong \mathbb{Z}_p^{\oplus r}$. (Note that $N_q^+ \subseteq N^+$, and $N_q^+ = N^+$ for Case NS.) Then we obtain the following:

Proposition 3.4. *N^+/k_∞ is unramified outside $\{p, q\}$, and a subgroup of $\mathrm{Gal}(N^+/k_\infty)$ generated by the inertia groups for the primes lying above p has finite index. $N_q^+ \cap M_p(k_\infty)/k_\infty$ is a finite extension.*

4. Proof of Theorem 1.1

We will use the same notation and symbols defined in Section 3. Our strategy of the proof of Theorem 1.1 is similar to that of Theorem A. However, our situation has a difficulty which comes from the fact that $\mathrm{Gal}(M_p(k_\infty)/k_\infty)$ can be non-trivial. Assume that K, k, and q satisfy (A) stated in Section 2.

We shall recall and define the following symbols:

- $M_{p,q}(k_\infty)$: the maximal abelian pro-p extension of k_∞ unramified outside $\{p, q\}$,
- $M_p(k_\infty)$: the maximal abelian pro-p extension of k_∞ unramified outside p,
- $M_q(k_\infty)$: the maximal abelian pro-p extension of k_∞ unramified outside q,
- $L(k_\infty)$: the maximal unramified pro-p abelian extension of k_∞,
- $\mathfrak{X}_{p,q}(k_\infty) = \mathrm{Gal}(M_{p,q}(k_\infty)/k_\infty)$,
- $\mathfrak{X}_p(k_\infty) = \mathrm{Gal}(M_p(k_\infty)/k_\infty)$,
- $X_q(k_\infty) = \mathrm{Gal}(M_q(k_\infty)/k_\infty)$,
- $X(k_\infty) = \mathrm{Gal}(L(k_\infty)/k_\infty)$.

We also define the following notation:

- $\Gamma = \mathrm{Gal}(K_\infty/K)$ (we often identify Γ with $\mathrm{Gal}(k_\infty/k)$),
- γ: fixed topological generator of Γ,
- κ: (p-adic) cyclotomic character of Γ,
- $\Lambda = \mathbb{Z}_p[[T]] \cong \mathbb{Z}_p[[\Gamma]]\colon 1 + T \leftrightarrow \gamma$,
- $\dot{T} = \kappa(\gamma)(1+T)^{-1} - 1 \in \Lambda$.

We note that $\mathfrak{X}_{p,q}(k_\infty)$, $\mathfrak{X}_p(k_\infty)$, $X_q(k_\infty)$, $X(k_\infty)$, and $\mathrm{Gal}(M_p(k_\infty)/L(k_\infty))$ are finitely generated torsion Λ-modules.

For a finitely generated torsion Λ-module A, we denote by $\mathrm{char}_\Lambda A$ the characteristic ideal of A. For finitely generated torsion Λ-modules A and B, we write $A \sim B$ when they are pseudo-isomorphic. We denote by $X(K_\infty)^- := X(K_\infty)^{1-J}$ the minus part of $X(K_\infty)$.

We recall the fact that $\mathfrak{X}_p(k_\infty)$ relates to $X(K_\infty)^-$ by Kummer duality (see, e.g., [15]). Let $f(T) \in \Lambda$ be a generator of $\mathrm{char}_\Lambda X(K_\infty)^-$. We note that $f(T)$ is not divisible by p because K is an abelian field (Ferrero–Washington's theorem [2]). It is

known that $f(\dot{T}) \in \Lambda$ generates $\mathrm{char}_\Lambda\, \mathfrak{X}_p(k_\infty)$. By a result of Greenberg [3], we know that the power of T dividing $f(T)$ is T^s, where $s = 0$ for Case NS, and $s = t$ for Case S. Hence the power of $\dot{T}$ dividing $f(\dot{T})$ is just $\dot{T}^s$. For Case NS, we see that $f(\dot{T})$ is prime to $\dot{T}$.

For $i = 1, \ldots, t$, let $k_{n,i}$ be the completion of k_n at the unique prime lying above $\mathfrak{p}_i$, and $\mathcal{U}^1(k_{n,i})$ the group of principal units in $k_{n,i}$. Let $\phi(E_{k_n})$ be the diagonal image of E_{k_n} in $\prod_i k_{n,i}^\times$, and $\mathcal{E}_n$ the closure of $\phi(E_{k_n}) \cap \prod_i \mathcal{U}^1(k_{n,i})$. We put $\mathcal{U} = \varprojlim \prod_i \mathcal{U}^1(k_{n,i})$, and $\mathcal{E} = \varprojlim \mathcal{E}_n$, where the projective limits are taken with respect to the norm mappings. Recall the exact sequence:

$$0 \to \mathrm{Gal}(M_p(k_\infty)/L(k_\infty)) \to \mathfrak{X}_p(k_\infty) \to X(k_\infty) \to 0,$$

and the fact that $\mathrm{Gal}(M_p(k_\infty)/L(k_\infty)) \cong \mathcal{U}/\mathcal{E}$ (see [15, Corollary 13.6]). We note that $\varprojlim \mathcal{U}^1(k_{n,i})$ contains $\varprojlim \mu_{p^n} \cong \Lambda/\dot{T}$ for Case S (see [13], etc.). Hence $\mathcal{U}$ contains a submodule which is isomorphic to $(\Lambda/\dot{T})^{\oplus s}$. We also note that $\mathcal{E}_n$ has no non-trivial $\mathbb{Z}_p$-torsion element (see, e.g., [14, Lemma 3.3]). From the above facts, we obtain the following:

Lemma 4.1. *There is a pseudo-isomorphism of finitely generated torsion Λ-modules*:

$$\mathrm{Gal}(M_p(k_\infty)/L(k_\infty)) \sim (\Lambda/\dot{T})^{\oplus s} \oplus E,$$

where E is an elementary torsion Λ-module (*see* [7], [11, (5.3.9) Definition], [15, Chapter 15]) *whose characteristic ideal is prime to* $(\dot{T})$. *Moreover, the characteristic ideal of $X(k_\infty)$ is prime to* $(\dot{T})$. (*See also* [14].)

Let N^+ and N_q^+ be extensions over k_∞ defined in Section 3 (see the paragraph before Proposition 3.4).

Lemma 4.2 (see also Greenberg [4]). $M_{p,q}(k_\infty) = M_p(k_\infty)N_q^+$.

Proof. Although this fact is already shown in [4, pp. 148–149], we will give a detailed proof for a convenient to the reader (and our proof is slightly different). Let $\tilde{M}_{p,q}(k_\infty)$ be the maximal pro-p extension of k_∞ unramified outside $\{p, q\}$. By Theorem 3 of Iwasawa [8] and Ferrero–Washington's theorem [2], we see that $\mathrm{Gal}(\tilde{M}_{p,q}(k_\infty)/k_\infty)$ is a free pro-p group whose minimal number of generators is $\lambda^- + r$, where $\lambda^- = \mathrm{rank}_{\mathbb{Z}_p} X(K_\infty)^-$. (Note that every prime lying above q actually ramifies in $\tilde{M}_{p,q}(k_\infty)/k_\infty$ by Lemma 3.2.) By taking the abelian quotient of $\mathrm{Gal}(\tilde{M}_{p,q}(k_\infty)/k_\infty)$, we see that $\mathfrak{X}_{p,q}(k_\infty) \cong \mathbb{Z}_p^{\oplus \lambda^- + r}$ as a $\mathbb{Z}_p$-module.

On the other hand, we see that $M_p(k_\infty) \cap N_q^+/k_\infty$ is a finite extension by Proposition 3.4. Hence

$$\mathrm{rank}_{\mathbb{Z}_p} \mathrm{Gal}(M_p(k_\infty)N_q^+/k_\infty) = \mathrm{rank}_{\mathbb{Z}_p} \mathfrak{X}_p(k_\infty) + r = \lambda^- + r.$$

Since N_q^+/k_∞ is unramified outside $\{p, q\}$, we see $M_{p,q}(k_\infty) \supseteq M_p(k_\infty)N_q^+$. Then we have a surjection of finitely generated $\mathbb{Z}_p$-modules $\mathfrak{X}_{p,q}(k_\infty) \to \mathrm{Gal}(M_p(k_\infty)N_q^+/k_\infty)$ whose kernel is finite. However $\mathfrak{X}_{p,q}(k_\infty)$ has no non-trivial $\mathbb{Z}_p$-torsion element, and hence we conclude that $M_{p,q}(k_\infty) = M_p(k_\infty)N_q^+$. □

For a finitely generated torsion Λ-module A, we can define the "multiplication by $\dot{T}$ endomorphism" of A, and we denote by $A[\dot{T}]$ (resp. $A/\dot{T}$) its kernel (resp. cokernel):

$$0 \to A[\dot{T}] \to A \xrightarrow{\dot{T}} A \to A/\dot{T} \to 0.$$

Note that Γ acts on $\mathrm{Gal}(M_{p,q}(k_\infty)/L(k_\infty))$ and then it is also a finitely generated torsion Λ-module. Let M' be the intermediate field of $M_{p,q}(k_\infty)/L(k_\infty)$ corresponding to $\dot{T}\,\mathrm{Gal}(M_{p,q}(k_\infty)/L(k_\infty))$. Hence $\mathrm{Gal}(M'/L(k_\infty))$ is isomorphic to

$$\mathrm{Gal}(M_{p,q}(k_\infty)/L(k_\infty))/\dot{T}.$$

Lemma 4.3. *$M_q(k_\infty)$ is contained in M'.*

Proof. By class field theory, $\mathrm{Gal}(M_q(k_\infty)/L(k_\infty))$ is isomorphic to a quotient of $\varprojlim \widehat{(O_{k_n}/q)}^\times$. As a Λ-module, $\varprojlim \widehat{(O_{k_n}/q)}^\times$ is isomorphic to $(\Lambda/\dot{T})^{\oplus r}$. Hence $\dot{T}$ annihilates $\mathrm{Gal}(M_q(k_\infty)/L(k_\infty))$, and then $\mathrm{Gal}(M_q(k_\infty)/L(k_\infty))/\dot{T} = \mathrm{Gal}(M_q(k_\infty)/L(k_\infty))$. From the restriction map

$$\mathrm{Gal}(M_{p,q}(k_\infty)/L(k_\infty)) \to \mathrm{Gal}(M_q(k_\infty)/L(k_\infty)) \to 0,$$

we obtain a surjection

$$\mathrm{Gal}(M_{p,q}(k_\infty)/L(k_\infty))/\dot{T} \to \mathrm{Gal}(M_q(k_\infty)/L(k_\infty)) \to 0.$$

By the definition of M', we see $M_q(k_\infty) \subseteq M'$. □

Lemma 4.4. *$L(k_\infty)N^+$ is contained in M'.*

Proof. Note that $\mathrm{Gal}(L(k_\infty)N^+/L(k_\infty)) \cong \mathrm{Gal}(N^+/N^+ \cap L(k_\infty))$, and $\mathrm{Gal}(N^+/N^+ \cap L(k_\infty))$ is a subgroup of $\mathrm{Gal}(N^+/k_\infty)$. By the construction of N^+, we see that $\dot{T}$ annihilates $\mathrm{Gal}(N^+/k_\infty)$, and hence it also annihilates $\mathrm{Gal}(L(k_\infty)N^+/L(k_\infty))$. The rest of the proof is similar to that of Lemma 4.3. □

Lemma 4.5. *$M'/L(k_\infty)N^+$ is a finite extension.*

Proof. We shall show that $\mathrm{rank}_{\mathbb{Z}_p}\mathrm{Gal}(M'/L(k_\infty)) = \mathrm{rank}_{\mathbb{Z}_p}\mathrm{Gal}(L(k_\infty)N^+/L(k_\infty))$. By Proposition 3.3, we see that $N^+ \cap L(k_\infty)/k_\infty$ is a finite extension. Hence $\mathrm{rank}_{\mathbb{Z}_p}\mathrm{Gal}(L(k_\infty)N^+/L(k_\infty))$ is equal to $\mathrm{rank}_{\mathbb{Z}_p}\mathrm{Gal}(N^+/k_\infty) = r+s$.

On the other hand, $M_{p,q}(k_\infty) = M_p(k_\infty)N_q^+$ by Lemma 4.2, and $M_p(k_\infty) \cap N_q^+/k_\infty$ is a finite extension by Proposition 3.4. By using Lemma 4.1, we can obtain the following pseudo-isomorphisms:

$$\mathfrak{X}_{p,q}(k_\infty) \sim \mathfrak{X}_p(k_\infty) \oplus \mathrm{Gal}(N_q^+/k_\infty) \sim (\Lambda/\dot{T})^{\oplus r+s} \oplus E',$$

where E' is an elementary torsion Λ-module whose characteristic ideal is prime to $(\dot{T})$. Hence, $\mathrm{rank}_{\mathbb{Z}_p}\mathfrak{X}_{p,q}(k_\infty)/\dot{T} = r+s$.

The following exact sequence:

$$0 \to \mathrm{Gal}(M_{p,q}(k_\infty)/L(k_\infty)) \to \mathfrak{X}_{p,q}(k_\infty) \to X(k_\infty) \to 0$$

induces the exact sequence:

$$X(k_\infty)[\dot{T}] \to \mathrm{Gal}(M_{p,q}(k_\infty)/L(k_\infty))/\dot{T} \to \mathfrak{X}_{p,q}(k_\infty)/\dot{T} \to X(k_\infty)/\dot{T} \to 0.$$

Since $\mathrm{char}_\Lambda X(k_\infty)$ is prime to $(\dot{T})$ by Lemma 4.1, both of $X(k_\infty)[\dot{T}]$ and $X(k_\infty)/\dot{T}$ are finite. Hence $\mathrm{rank}_{\mathbb{Z}_p}\mathrm{Gal}(L(k_\infty)N^+/L(k_\infty))$ is equal to $\mathrm{rank}_{\mathbb{Z}_p}\mathfrak{X}_{p,q}(k_\infty)/\dot{T} = \mathrm{rank}_{\mathbb{Z}_p}\mathrm{Gal}(M'/L(k_\infty))$. □

For a Galois group G appeared below, we denote $\mathcal{I}(G)$ by the subgroup of G generated by the inertia groups for all primes lying above p.

Lemma 4.6. $\mathrm{rank}_{\mathbb{Z}_p}\mathcal{I}(\mathrm{Gal}(N^+L(k_\infty)/k_\infty)) = r+s$.

Proof. We shall take a prime $\mathcal{P}$ of k_∞ lying above p. Let $I_{\mathcal{P}}$ be the inertia subgroup of $\mathrm{Gal}(N^+/k_\infty)$ for $\mathcal{P}$. Similarly, let $I'_{\mathcal{P}}$ be the inertia subgroup of $\mathrm{Gal}(N^+L(k_\infty)/k_\infty)$ for $\mathcal{P}$. Then the restriction map induces a surjection $I'_{\mathcal{P}} \to I_{\mathcal{P}}$. Hence there is a surjection $\mathcal{I}(\mathrm{Gal}(N^+L(k_\infty)/k_\infty)) \to \mathcal{I}(\mathrm{Gal}(N^+/k_\infty))$. By Proposition 3.4, $\mathrm{rank}_{\mathbb{Z}_p}\mathcal{I}(\mathrm{Gal}(N^+/k_\infty)) = r+s$. We see that $\mathrm{rank}_{\mathbb{Z}_p}\mathcal{I}(\mathrm{Gal}(N^+L(k_\infty)/k_\infty)) \geq r+s$. Since $L(k_\infty)/k_\infty$ is an unramified extension, $\mathcal{I}(\mathrm{Gal}(N^+L(k_\infty)/k_\infty))$ is contained in $\mathrm{Gal}(N^+L(k_\infty)/L(k_\infty))$. By these results, we see that $\mathrm{rank}_{\mathbb{Z}_p}\mathcal{I}(\mathrm{Gal}(N^+L(k_\infty)/k_\infty)) = r+s$. □

We shall finish to prove Theorem 1.1. By Lemma 4.6,

$$\mathrm{rank}_{\mathbb{Z}_p}\mathcal{I}(\mathrm{Gal}(N^+L(k_\infty)/k_\infty)) = r+s.$$

Moreover, $\mathrm{rank}_{\mathbb{Z}_p}\mathcal{I}(\mathrm{Gal}(M'/k_\infty))$ is also $r+s$ because $M'/N^+L(k_\infty)$ is a finite extension (Lemma 4.5). Note that $\mathrm{rank}_{\mathbb{Z}_p}\mathrm{Gal}(M'/L(k_\infty))$ is $r+s$. Then $\mathcal{I}(\mathrm{Gal}(M'/k_\infty))$ is

a finite index subgroup of $\mathrm{Gal}(M'/L(k_\infty))$. By Lemma 4.3, $M_q(k_\infty)$ is an intermediate field of $M'/L(k_\infty)$. Since $M_q(k_\infty)/k_\infty$ is unramified at all primes lying above p, we can see that $M_q(k_\infty)$ is contained in the fixed field of $\mathcal{I}(\mathrm{Gal}(M'/k_\infty))$. This implies that $M_q(k_\infty)/L(k_\infty)$ is a finite extension.

We have shown Theorem 1.1 for k and q satisfying (A). Then, as noted in Section 2, we obtain Theorem 1.1 for general k and q. □

5. Slight generalization of Theorem 1.1

In this section, we shall give a simple remark that the converse of Lemma 2.1 holds under a (strict) condition. (In general, the converse of Lemma 2.1 does not hold.)

Lemma 5.1. *Let k'/k be a finite extension of algebraic number fields satisfying $k' \cap k_\infty = k$. Let*

$$I_n : \widehat{(O_{k_n}/q)}^\times \to \widehat{(O_{k'_n}/q)}^\times$$

be the homomorphism induced from the natural embedding. If $\mathrm{Gal}(M_q(k_\infty)/L(k_\infty))$ is finite and I_n is an isomorphism for all n, then $\mathrm{Gal}(M_q(k'_\infty)/L(k'_\infty))$ is also finite.

Proof. By the assumption, we obtain the following isomorphism

$$I : \varprojlim \widehat{(O_{k_n}/q)}^\times \to \varprojlim \widehat{(O_{k'_n}/q)}^\times.$$

Hence the homomorphism

$$\mathrm{Gal}(M_q(k_\infty)/L(k_\infty)) \to \mathrm{Gal}(M_q(k'_\infty)/L(k'_\infty))$$

induced from I is surjective. The assertion follows. □

We shall give an example satisfying the assumption that I_n is an isomorphism for all n. Let k be an algebraic number field, and k' a quadratic extension of k. Assume that every prime of k lying above q is inert in k'_∞ (that is, every prime lying above q is inert in k' and k_∞). Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ be the primes of k lying above q. We also assume that p divides $N(\mathfrak{q}_i)-1$ for all i, where $N(\mathfrak{q}_i)$ is the absolute norm of $\mathfrak{q}_i$. Then $\widehat{(O_{k_n}/\mathfrak{q}_i)}^\times$ is not trivial for all i, n. Under these assumptions, we obtain that

$$N(\mathfrak{q}_i O_{k'_n}) - 1 = N(\mathfrak{q}_i O_{k_n})^2 - 1 = (N(\mathfrak{q}_i O_{k_n}) - 1)(N(\mathfrak{q}_i O_{k_n}) + 1).$$

We assumed that p is odd, and hence $N(\mathfrak{q}_i O_{k_n}) + 1$ is prime to p. This implies that $|\widehat{(O_{k'_n}/\mathfrak{q}_i)}^\times| = |\widehat{(O_{k_n}/\mathfrak{q}_i)}^\times|$ for all i, n. From this, we obtain that

$$|\widehat{(O_{k'_n}/q)}^\times| = \prod_{i=1}^{r} |\widehat{(O_{k'_n}/\mathfrak{q}_i)}^\times| = \prod_{i=1}^{r} |\widehat{(O_{k_n}/\mathfrak{q}_i)}^\times| = |\widehat{(O_{k_n}/q)}^\times|.$$

Since I_n is injective, we see that I_n is an isomorphism for all n. Under the above assumptions, if $\mathrm{Gal}(M_q(k_\infty)/L(k_\infty))$ is finite, then $\mathrm{Gal}(M_q(k'_\infty)/L(k'_\infty))$ is also finite by Lemma 5.1. (For the case that k'/k is an imaginary quadratic extension of $\mathbb{Q}$, see also [12], [6].)

The above lemma implies that Theorem 1.1 can be generalized for some non-abelian fields.

6. $\mathbb{Z}_p$-rank of S-ramified Iwasawa modules

We shall lead a formula of the $\mathbb{Z}_p$-rank of S-ramified Iwasawa modules (for general S) from Theorem 1.1. As same as Theorem 1.1, the strategy of our proof is quite similar to that of given in [6].

In this section, we will use the following notation (similar to Greither's [5] or Tsuji's [13] but slightly different):

- p: fixed odd rational prime,
- S: finite set of *rational* primes which does not include p,
- F: finite abelian extension of $\mathbb{Q}$ unramified at p,
- $K = F(\mu_p)$,
- $K_n = K(\mu_{p^{n+1}})$,
- $K_\infty = \bigcup_{n\geq 0} K_n$: the cyclotomic $\mathbb{Z}_p$-extension of K,
- $G = \mathrm{Gal}(K_\infty/\mathbb{Q}_\infty) \cong \mathrm{Gal}(K/\mathbb{Q})$,
- $\Gamma = \mathrm{Gal}(K_\infty/K)$,
- G_p: Sylow p-subgroup of G,
- G_0: non-p-part of G (the maximal subgroup of G consists of the elements having prime to p order),
- γ: fixed topological generator of Γ,
- κ: (p-adic) cyclotomic character,
- ω: (p-adic) Teichmüller character,
- $J \in G$: complex conjugation.

Let χ be a p-adic character of G. We denote by $\mathbb{Q}_p(\chi)$ the extension of $\mathbb{Q}_p$ by adjoining the values of χ, and O_χ the valuation ring of $\mathbb{Q}_p(\chi)$. We put $d_\chi = [\mathbb{Q}_p(\chi) : \mathbb{Q}_p]$. Let $\underline{O_\chi}$ be a free rank one O_χ-module such that $\sigma \in G$ acts as $\chi(\sigma)$. For a $\mathbb{Z}_p[G]$-module M, we put $M_\chi = M \otimes_{\mathbb{Z}_p[G]} \underline{O_\chi}$, which is called the "$\chi$-quotient" in [13] (or the "χ-part" in [5, p. 451]). The functor taking the χ-quotient is right exact. We also put

$$e_\chi = \frac{1}{|G|} \sum_{\sigma \in G} \mathrm{tr}_{\mathbb{Q}_p\chi)/\mathbb{Q}_p}(\chi(\sigma))\sigma^{-1} \in \mathbb{Q}_p[G].$$

If p does not divide $|G|$, then $M_\chi \cong e_\chi M$. In general, we see

$$M_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong (M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)_\chi \cong e_\chi(M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p).$$

For more informations about the χ-quotient, see [5], [13] for example.

We also give some simple remarks. For a $\mathbb{Z}_p[G]$-module M, we put $M^{\pm} = M^{1\pm J}$. Since p is odd, we have a decomposition $M \cong M^+ \oplus M^-$. For a character χ of G, we see that

$$\begin{aligned} M_\chi &\cong (M^+ \oplus M^-)_\chi \\ &= (M^+ \oplus M^-) \otimes_{\mathbb{Z}_p[G]} \underline{O_\chi} \\ &\cong (M^+ \otimes_{\mathbb{Z}_p[G]} \underline{O_\chi}) \oplus (M^- \otimes_{\mathbb{Z}_p[G]} \underline{O_\chi}) \\ &= M_\chi^+ \oplus M_\chi^-. \end{aligned}$$

We claim that if χ is odd, then M_χ^+ is trivial. Let

$$(a \otimes b) \in M^+ \otimes_{\mathbb{Z}_p[G]} \underline{O_\chi} = M_\chi^+.$$

Note that J acts trivially on M^+ and acts as -1 on $\underline{O_\chi}$. Hence the equality

$$(a \otimes b) = (Ja \otimes b) = (a \otimes Jb) = (a \otimes -b)$$

implies that $(a \otimes 2b) = 2(a \otimes b) = 0$. Since p is odd, we obtain the claim. Similarly, we can see that if χ is even, then M_χ^- is trivial.

For a rational prime q distinct from p, we put

$$R_q = \varprojlim \widehat{(O_{K_n}/q)^\times}.$$

Let r be the number of primes of K_∞ lying above q. Then $\mathrm{rank}_{\mathbb{Z}_p} R_q = r$. Since q is a rational prime, G acts on R_q. We shall determine the $\mathbb{Z}_p$-rank of $(R_q)_\chi$.

First, we assume that q is unramified in K (i.e., the conductor of F is prime to q). Let D be the decomposition subgroup of $\mathrm{Gal}(K_\infty/\mathbb{Q})$ for q. Then we can write $D \cong D_p \times D_0$, where $D_p \cong \mathbb{Z}_p$ and D_0 is a finite cyclic group whose order is prime to p. We may regard D_0 as a subgroup of G_0. Note that $\mathrm{Gal}(K_\infty/\mathbb{Q})$ is isomorphic to $\Gamma \times G_p \times G_0$. Then we can take a generator of D_p of the from $\gamma^{p^m}\sigma_p$ with some $m \geq 0$ and $\sigma_p \in G_p$. We also take a generator $\sigma_0 \in G_0$ of D_0. Hence D is a procyclic group generated by $\gamma^{p^m}\sigma_p\sigma_0$.

In the above choice of the generator of D_p, we can see that m and σ_p is uniquely determined. (Since $D_p \cong \mathbb{Z}_p$, every generator of D_p is written by the from $(\gamma^{p^m}\sigma_p)^\alpha$ with $\alpha \in \mathbb{Z}_p^\times$.)

Lemma 6.1. *R_q is a cyclic $\mathbb{Z}_p[G][[\Gamma]]$-module.*

Proof. Fix a sufficiently large integer n_0 such that every prime in K_{n_0} lying above q remains prime in K_m for all $m \geq n_0$. Let n be an integer which satisfies $n \geq n_0$.

We put $G^{(n)} = \mathrm{Gal}(K_n/\mathbb{Q})$. Let $\mathfrak{q}$ be a prime in K_n lying above q. We remark that $\mu_{p^{n+1}} \subset K_n$ and $\mu_{p^{n+2}} \not\subset K_n$. Under the assumption on n, we can see that the Sylow p-subgroup of $(O_{K_n}/\mathfrak{q})^\times$ is generated by $\zeta_{p^{n+1}} \pmod{\mathfrak{q}}$ with a generator $\zeta_{p^{n+1}}$ of $\mu_{p^{n+1}}$. Let $\{\mathfrak{q}_1, \mathfrak{q}_2, \dots, \mathfrak{q}_r\}$ be the set of primes of K_n lying above q. We assumed that q is unramified in $K_\infty/\mathbb{Q}$, then $qO_{K_n} = \mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_r$. We note that the action of $G^{(n)}$ on $\{\mathfrak{q}_1, \mathfrak{q}_2, \dots, \mathfrak{q}_r\}$ is transitive. Take an element α_n of O_{K_n} which satisfies

$$\alpha_n \equiv \zeta_{p^{n+1}} \pmod{\mathfrak{q}_1}, \quad \alpha_n \equiv 1 \pmod{\mathfrak{q}_2}, \dots, \alpha_n \equiv 1 \pmod{\mathfrak{q}_r}.$$

Then $\alpha_n \pmod q$ is a generator of the Sylow p-subgroup of $(O_{K_n}/q)^\times$ as a $\mathbb{Z}_p[G^{(n)}]$-module. Hence the Sylow p-subgroup of $(O_{K_n}/q)^\times$ (which is isomorphic to $\widehat{(O_{K_n}/q)^\times}$) is a cyclic $\mathbb{Z}_p[G^{(n)}]$-module.

We can choose a suitable set of generators $\{\alpha_n\}$ such that $N_{K_m/K_n}(\alpha_m) \equiv \alpha_n \pmod q$ for all $m > n \geq n_0$. Hence we obtain the following commutative diagram with exact raws:

$$\begin{array}{ccccc}
\mathbb{Z}_p[G^{(m)}] & \longrightarrow & \widehat{(O_{K_m}/q)^\times} & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \\
\mathbb{Z}_p[G^{(n)}] & \longrightarrow & \widehat{(O_{K_n}/q)^\times} & \longrightarrow & 0,
\end{array}$$

where the left vertical mapping is induced from the restriction mapping, and the right vertical mapping is induced from the norm mapping. Since $\varprojlim \mathbb{Z}_p[G^{(n)}] \cong \mathbb{Z}_p[G][[\Gamma]]$, we obtain the assertion. $\square$

Hence there is a surjection $\varphi\colon \mathbb{Z}_p[G][[\Gamma]] \to R_q$. We note that $\gamma^{p^m}\sigma_p\sigma_0$ acts on R_q as $\kappa(\gamma^{p^m}\sigma_p\sigma_0)$. (Recall that κ is the cyclotomic character.) Then the kernel of φ contains an ideal generated by $\gamma^{p^m}\sigma_p\sigma_0 - \kappa(\gamma^{p^m}\sigma_p\sigma_0)$.

By taking the χ-quotient, we obtain a surjection $\varphi_\chi\colon O_\chi[[\Gamma]] \to (R_q)_\chi$, and the kernel of φ_χ contains $\chi(\sigma_p\sigma_0)\gamma^{p^m} - \kappa(\gamma^{p^m}\sigma_p\sigma_0)$. We may regard $(R_q)_\chi$ as a $O_\chi[[T]]$-module via the isomorphism $O_\chi[[\Gamma]] \cong O_\chi[[T]]$ with $\gamma \mapsto 1 + T$. We put $\Lambda_\chi = O_\chi[[T]]$, and $\kappa_0 = \kappa(\gamma) \in 1 + p\mathbb{Z}_p$. Then we see that $(R_q)_\chi$ is annihilated by

$$f_{q,\chi}(T) = (1+T)^{p^m} - \chi^{-1}(\sigma_p\sigma_0)\kappa(\sigma_p\sigma_0)\kappa_0^{p^m} \in \Lambda_\chi.$$

Let $\mathfrak{P}$ be the maximal ideal of O_χ. Since $\kappa_0 \in 1 + p\mathbb{Z}_p$, if

$$\chi^{-1}(\sigma_p\sigma_0)\kappa(\sigma_p\sigma_0) \not\equiv 1 \pmod{\mathfrak{P}},$$

then $f_{q,\chi}(T)$ is a unit polynomial, and hence $(R_q)_\chi$ is trivial. We see

$$\chi^{-1}(\sigma_p\sigma_0)\kappa(\sigma_p\sigma_0) = \chi^{-1}\kappa(\sigma_0)\chi^{-1}\kappa(\sigma_p) = \chi^{-1}\omega(\sigma_0)\chi^{-1}\kappa(\sigma_p).$$

Note that $\chi^{-1}\kappa(\sigma_p)$ is a p-power root of unity, and then it is congruent to 1 modulo $\mathfrak{P}$. Moreover, $\chi^{-1}\omega(\sigma_0)$ is a root of unity whose order is prime to p. Then $\chi^{-1}\omega(\sigma_0) \equiv 1 \pmod{\mathfrak{P}}$ if and only if $\chi^{-1}\omega(\sigma_0) = 1$. Consequently, we showed that if $\chi^{-1}\omega(\sigma_0) \neq 1$, then $(R_q)_\chi$ is trivial.

We can see that the number of characters χ satisfying $\chi^{-1}\omega(\sigma_0) = 1$ is just $|G/D_0|$. (It is equal to the number of characters χ' of G satisfying $\chi'(D_0) = 1$.) Though if $(R_q)_\chi$ is non-trivial, it is annihilated by $f_{q,\chi}(T)$, and then $\mathrm{rank}_{\mathbb{Z}_p}(R_q)_\chi \leq d_\chi p^m$. By considering these facts, we obtain the inequality:

$$r = \mathrm{rank}_{\mathbb{Z}_p} R_q = \sum_\chi \mathrm{rank}_{\mathbb{Z}_p}(R_q)_\chi \leq \sum_\chi d_\chi p^m = |G/D_0| \times p^m,$$

where χ runs all representatives of the conjugacy classes satisfying $\chi^{-1}\omega(\sigma_0) = 1$ in the above sums. (We give some remarks. The second equation follows from the fact that $R_q \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong \bigoplus_\chi (R_q)_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Moreover, $\sum_\chi d_\chi = |G/D_0|$, and m is independent of χ.)

We claim that $r = |G/D_0| \times p^m$. Let K^D be the decomposition field of $K_\infty/\mathbb{Q}$ for q. Then the p-part of $[K^D : \mathbb{Q}]$ is equal to the p-part of $[K_m : \mathbb{Q}]$. Hence this is equal to $|G_p| \times p^m$. On the other hand, the non-p-part of $[K^D : \mathbb{Q}]$ is equal to $|G_0/D_0|$. We see

$$[K^D : \mathbb{Q}] = |G_p| \times p^m \times |G_0/D_0| = |G/D_0| \times p^m.$$

Since $r = [K^D : \mathbb{Q}]$, the claim follows.

From this claim, we see that the above inequality is just an equality. Hence for all character χ satisfying $\chi^{-1}\omega(\sigma_0) = 1$, the $\mathbb{Z}_p$-rank of $(R_q)_\chi$ is $d_\chi p^m$. We also note that $\kappa(\sigma_p) = 1$ because σ_p fixes all elements of μ_{p^n} for all n. Hence, when $\chi^{-1}\omega(\sigma_0) = 1$, we can write

$$f_{q,\chi}(T) = (1+T)^{p^m} - \chi^{-1}(\sigma_p)\kappa_0^{p^m}.$$

Next, we consider the case that q is ramified in K. Let I be the inertia subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ for q, and K^I the inertia field of $K/\mathbb{Q}$ for q. We remark that all primes lying above q are totally ramified in K_n/K_n^I. Hence $\widehat{(O_{K_n}/q)}^\times \cong \widehat{(O_{K_n^I}/q)}^\times$ for all n. We put

$$R_q^I = \varprojlim \widehat{(O_{K_n^I}/q)}^\times.$$

Since q is unramified in $\mathbb{Q}(\mu_{p^\infty})$ (where $\mu_{p^\infty} = \bigcup_{n\geq 1} \mu_{p^n}$), we see that K_∞^I contains μ_{p^∞}. Then the proof of Lemma 6.1 also works for K_∞^I.

Let χ be a character of G. If $\chi(I) = 1$, then χ is also a character of $\mathrm{Gal}(K^I/\mathbb{Q})$, and hence $(R_q)_\chi \cong (R_q^I)_\chi$. From this, if $\chi(I) \neq 1$, we see that $(R_q)_\chi$ is finite because

$$\mathrm{rank}_{\mathbb{Z}_p} R_q = \mathrm{rank}_{\mathbb{Z}_p} R_q^I = \sum_{\chi(I)=1} \mathrm{rank}_{\mathbb{Z}_p}(R_q^I)_\chi = \sum_{\chi(I)=1} \mathrm{rank}_{\mathbb{Z}_p}(R_q)_\chi.$$

We also determine the structure of $(R_q)_\chi$ for a general case. Assume that $\chi(I) = 1$. Then $\chi(\sigma)$ for $\sigma \in \mathrm{Gal}(K^I/\mathbb{Q}) \cong G/I$ is well defined. Repeating the argument given in the unramified case for K^I, we can take σ_0 and σ_p for q. (They are determined modulo I, and σ_p (mod I) is uniquely determined. Hence $\chi(\sigma_p)$ is dependent only on q.) We also assume that $\chi^{-1}\omega(\sigma_0) = 1$. Since $\mathbb{Z}_p[G/I]_\chi \cong O_\chi$, we can take

$$f_{q,\chi}(T) = (1+T)^{p^m} - \chi^{-1}(\sigma_p)\kappa_0^{p^m}$$

as an element of $\Lambda_\chi = O_\chi[[T]]$. We see that $(R_q)_\chi$ is annihilated by $f_{q,\chi}(T)$ because $(R_q)_\chi \cong (R_q^I)_\chi$.

As a consequence, we obtained the following result (see also [6, Lemma 2.1]).

Proposition 6.2. *Let χ be a character of G. Then $(R_q)_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is non-trivial if and only if χ satisfies $\chi(I) = 1$ and $\chi^{-1}\omega(\sigma_0) = 1$. Moreover, if $(R_q)_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is non-trivial, then*

$$(R_q)_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong \Lambda_\chi / f_{q,\chi}(T) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p,$$

and $\mathrm{rank}_{\mathbb{Z}_p}(R_q)_\chi = d_\chi p^m$.

By class field theory, we have the following exact sequence:

$$E_\infty \to R_q \to \mathrm{Gal}(M_q(K_\infty)/L(K_\infty)) \to 0,$$

where $E_\infty = \varprojlim \hat{E}_{K_n}$. Assume that χ is a non-trivial *even* character of G satisfying $\chi(I) = 1$ and $\chi^{-1}\omega(\sigma_0) = 1$. By taking the χ-quotient (it is right exact), we see

$$(E_\infty)_\chi \to (R_q)_\chi \to \mathrm{Gal}(M_q(K_\infty)/L(K_\infty))_\chi \to 0$$

is exact. Since $(R_q)_\chi$ is annihilated by $f_{q,\chi}(T)$, we obtain the exact sequence:

$$(E_\infty)_\chi / f_{q,\chi}(T) \to (R_q)_\chi \to \mathrm{Gal}(M_q(K_\infty)/L(K_\infty))_\chi \to 0.$$

By tensoring with $\mathbb{Q}_p$, we also obtain the exact sequence:

$$(E_\infty)_\chi / f_{q,\chi}(T) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \to (R_q)_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \to \mathrm{Gal}(M_q(K_\infty)/L(K_\infty))_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \to 0.$$

We shall show the following result (see also [6]).

Proposition 6.3. *For every non-trivial even character χ of G satisfying $\chi(I) = 1$ and $\chi^{-1}\omega(\sigma_0) = 1$, the mapping*

$$(E_\infty)_\chi / f_{q,\chi}(T) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \to (R_q)_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

appeared above is an isomorphism.

Proof. As we noted before, we have a decomposition

$$\mathrm{Gal}(M_q(K_\infty)/L(K_\infty))_\chi \cong \mathrm{Gal}(M_q(K_\infty)/L(K_\infty))^+_\chi \oplus \mathrm{Gal}(M_q(K_\infty)/L(K_\infty))^-_\chi.$$

Moreover, we already know that $\mathrm{Gal}(M_q(K_\infty)/L(K_\infty))^-_\chi$ is trivial for every even character χ. Let K^+ be the maximal real subfield of K. Since p is odd, we see that $\mathrm{Gal}(M_q(K_\infty)/L(K_\infty))^+$ is isomorphic to $\mathrm{Gal}(M_q(K^+_\infty)/L(K^+_\infty))$. Hence we obtain

$$\mathrm{Gal}(M_q(K_\infty)/L(K_\infty))_\chi \cong \mathrm{Gal}(M_q(K^+_\infty)/L(K^+_\infty))_\chi$$

for every χ satisfying the assumption. (We note that χ can be viewed as a character of $\mathrm{Gal}(K^+_\infty/\mathbb{Q}_\infty)$.)

By Theorem 1.1, we see that $\mathrm{Gal}(M_q(K^+_\infty)/L(K^+_\infty))$ is finite, and hence we see that $\mathrm{Gal}(M_q(K_\infty)/L(K_\infty))_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is trivial. From this, we have a surjection

$$(E_\infty)_\chi / f_{q,\chi}(T) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \to (R_q)_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

By Proposition 6.2, $\dim_{\mathbb{Q}_p}(R_q)_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = d_\chi p^m$. We shall calculate the dimension of $(E_\infty)_\chi / f_{q,\chi}(T) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

Let $\mathcal{U}$ be the projective limit of semi local units in K_∞/K for the primes lying above p, and $\mathcal{E}$ the closure of the diagonal image of global units. (For the precise definition, see Section 4.) Since Leopoldt's conjecture is valid for all K_n (see [1], [15]), we see that $\mathcal{E}$ is isomorphic to E_∞. It is known that $\mathcal{E}_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is a free cyclic $\Lambda_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$-module. (See [14, Lemma 3.5], [5].) Then we see

$$\begin{aligned}(\mathcal{E}_\chi / f_{q,\chi}(T)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p &\cong (\mathcal{E}_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)/(f_{q,\chi}(T) \otimes 1)\\ &\cong (\Lambda_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)/(f_{q,\chi}(T) \otimes 1)\\ &\cong (\Lambda_\chi / f_{q,\chi}(T)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.\end{aligned}$$

Hence we showed that $\dim_{\mathbb{Q}_p}(E_\infty)_\chi / f_{q,\chi}(T) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = d_\chi p^m$. This implies the assertion. □

Here we shall state our main result. Let χ be an arbitrary character of G. Let S be a finite set of rational primes which does not include p. We put $X_S(K_\infty) = \mathrm{Gal}(M_S(K_\infty)/K_\infty)$, where $M_S(K_\infty)/K_\infty$ is the maximal abelian pro-p extension unramified outside S. In this case, G acts on $X_S(K_\infty)$ and hence its χ-quotient can be considered. We shall give a formula of $\mathrm{rank}_{\mathbb{Z}_p} X_S(K_\infty)_\chi$. For a prime $q \in S$, let I_q be the inertia subgroup of G for q. We also write $\sigma_{p,q}, \sigma_{0,q}, m_q$ as σ_p, σ_0, m for q (defined before), respectively. (Recall that $\sigma_{p,q}$ and $\sigma_{0,q}$ are determined modulo I_q.) We also recall that $\kappa_0 = \kappa(\gamma)$.

Theorem 6.4. *We put*

$$S_\chi = \{q \in S \mid \chi(I_q) = 1,\ \chi^{-1}\omega(\sigma_{0,q}) = 1\}$$

and

$$f_{q,\chi}(T) = (1+T)^{p^{m_q}} - \chi^{-1}(\sigma_{p,q})\kappa_0^{p^{m_q}} \in O_\chi[[T]].$$

If S_χ is not empty, then

$$\operatorname{rank}_{\mathbb{Z}_p} X_S(K_\infty)_\chi = \operatorname{rank}_{\mathbb{Z}_p} X(K_\infty)_\chi + \sum_{q\in S_\chi} d_\chi p^{m_q} - P_\chi,$$

where

$$P_\chi = \begin{cases} 1 & (\chi = \omega), \\ 0 & (\chi\colon \textit{odd},\ \chi \neq \omega), \\ d_\chi \deg F(T) & (\chi\colon \textit{even}). \end{cases}$$

and $F(T) = \operatorname{lcm}_{q\in S_\chi} f_{q,\chi}(T)$. If S_χ is empty, then $\operatorname{rank}_{\mathbb{Z}_p} X_S(K_\infty)_\chi = \operatorname{rank}_{\mathbb{Z}_p} X(K_\infty)_\chi$.

Proof. We may assume that S is not empty. Recall the following exact sequence:

$$E_\infty \to \bigoplus_{q\in S} R_q \to \operatorname{Gal}(M_S(K_\infty)/L(K_\infty)) \to 0$$

which is stated in Section 2. By Proposition 6.2, we see that $(R_q)_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is non-trivial if and only if $q \in S_\chi$. Hence, if S_χ is empty, then $\operatorname{Gal}(M_S(K_\infty)/L(K_\infty))_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is trivial, and $\operatorname{rank}_{\mathbb{Z}_p} X_S(K_\infty)_\chi = \operatorname{rank}_{\mathbb{Z}_p} X(K_\infty)_\chi$. In the following, we assume that S_χ is not empty. By taking the χ-quotient and tensoring with $\mathbb{Q}_p$, we have the exact sequence:

$$(E_\infty)_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \xrightarrow{\eta_\chi} \bigoplus_{q\in S_\chi} (R_q)_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \to \operatorname{Gal}(M_S(K_\infty)/L(K_\infty))_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \to 0.$$

It is sufficient to determine the cokernel of η_χ.

Since p is odd, we have a decomposition $E_\infty \cong E_\infty^+ \oplus E_\infty^-$, and we can see $E_\infty^- \cong \varprojlim \mu_{p^n}$. We also note that $(E_\infty)_\chi \cong (E_\infty^+)_\chi \oplus (E_\infty^-)_\chi$ for a character χ of G. It was already shown that if χ is an odd character, then $(E_\infty^+)_\chi$ is trivial, and hence $(E_\infty)_\chi \cong (\varprojlim \mu_{p^n})_\chi$.

Assume that $\chi = \omega$. Then $(E_\infty)_\omega \cong \varprojlim \mu_{p^n}$, and the natural mapping $\varprojlim \mu_{p^n} \to \bigoplus_{q\in S_\omega} R_q$ is injective. We also note that $d_\omega = 1$. From these facts, we see that

$$\begin{aligned} \operatorname{rank}_{\mathbb{Z}_p} X_S(K_\infty)_\omega &= \operatorname{rank}_{\mathbb{Z}_p} X(K_\infty)_\omega + \sum_{q\in S_\omega} \operatorname{rank}_{\mathbb{Z}_p}(R_q)_\omega - 1 \\ &= \operatorname{rank}_{\mathbb{Z}_p} X(K_\infty)_\omega + \sum_{q\in S_\omega} p^{m_q} - 1. \end{aligned}$$

Assume that χ is odd and $\chi \neq \omega$. Then $(E_\infty)_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is trivial. Hence we see

$$\mathrm{rank}_{\mathbb{Z}_p} X_S(K_\infty)_\chi = \mathrm{rank}_{\mathbb{Z}_p} X(K_\infty)_\chi + \sum_{q \in S_\chi} d_\chi p^{m_q}.$$

Let ε be the trivial character. Then we can see that

$$X_S(K_\infty)_\varepsilon \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong X_S(\mathbb{Q}_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p, \quad X(K_\infty)_\varepsilon \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong X(\mathbb{Q}_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

Hence $\mathrm{rank}_{\mathbb{Z}_p} X(K_\infty)_\varepsilon = 0$. We also note that

$$S_\varepsilon = \{q \in S \mid \omega(\sigma_{0,q}) = 1\} = \{q \in S \mid q \equiv 1 \pmod{p}\}.$$

By the results for $\mathbb{Q}_\infty$ (see [6]), we see that $X_S(\mathbb{Q}_\infty) = X_{S_\varepsilon}(\mathbb{Q}_\infty)$, and

$$\mathrm{rank}_{\mathbb{Z}_p} X_S(K_\infty)_\varepsilon = \sum_{q \in S_\varepsilon} p^{m_q} - \max\{p^{m_q} \mid q \in S_\varepsilon\}.$$

Since $d_\varepsilon = 1$ and $f_{q,\varepsilon}(T) = (1+T)^{p^{m_q}} - \kappa_0^{p^{m_q}}$, we see that

$$\max\{p^{m_q} \mid q \in S_\varepsilon\} = d_\varepsilon \deg F(T).$$

From these facts, the formula

$$\mathrm{rank}_{\mathbb{Z}_p} X_S(K_\infty)_\varepsilon = \mathrm{rank}_{\mathbb{Z}_p} X(K_\infty)_\varepsilon + \sum_{q \in S_\varepsilon} d_\varepsilon p^{m_q} - d_\varepsilon \deg F(T)$$

is certainly satisfied.

Finally, assume that χ is non-trivial and even. By Proposition 6.3, we see that

$$(E_\infty)_\chi / f_{q,\chi}(T) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \to (R_q)_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

is an isomorphism. This isomorphism implies that

$$(E_\infty)_\chi / F(T) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \to \bigoplus_{q \in S_\chi} (R_q)_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

is injective (see also [6]). By using the same argument stated in the proof of Proposition 6.3, we obtain that $\dim_{\mathbb{Q}_p}((E_\infty)_\chi / F(T)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = d_\chi \deg F(T)$. Hence we see that

$$\mathrm{rank}_{\mathbb{Z}_p} X_S(K_\infty)_\chi = \mathrm{rank}_{\mathbb{Z}_p} X(K_\infty)_\chi + \sum_{q \in S_\chi} d_\chi p^{m_q} - d_\chi \deg F(T).$$

We have shown the formula for all cases. $\square$

REMARK. Assume that p does not divide $|G|$. Then $f_{q,\chi}(T) = (1+T)^{p^{m_q}} - \kappa_0^{p^{m_q}}$, and hence $\deg F(T) = \max\{p^{m_q} \mid q \in S_\chi\}$. Moreover, we can see that p^{m_q} is equal to the number of primes of $\mathbb{Q}_\infty$ lying above q.

EXAMPLE 6.5. We put $K = \mathbb{Q}(\mu_p)$, the pth cyclotomic field (recall that p is an odd prime). In this case, every character of $G = \mathrm{Gal}(K/\mathbb{Q})$ is written by the form ω^i with $0 \le i \le p-2$. Note also that $q \in S$ is unramified in K. We may identify G with $(\mathbb{Z}/p\mathbb{Z})^\times$, and $\sigma_{0,q}$ with $q \pmod p$. Then we can see

$$S_{\omega^i} = \{q \in S \mid \omega^{1-i}(\sigma_{0,q}) = 1\} = \{q \in S \mid i \equiv 1 \pmod{f_q}\},$$

where f_q is the order of q in $(\mathbb{Z}/p\mathbb{Z})^\times$. Assume that S_{ω^i} is not empty. We put

$$P^{(i)} = \begin{cases} 1 & (i = 1), \\ 0 & (i\colon \text{odd},\ i \neq 1), \\ \max\{p^{m_q} \mid q \in S_{\omega^i}\} & (i\colon \text{even}). \end{cases}$$

By Theorem 6.4, we see

$$\mathrm{rank}_{\mathbb{Z}_p} X_S(K_\infty)_{\omega^i} = \lambda_{\omega^i} + \sum_{q \in S_{\omega^i}} p^{m_q} - P^{(i)},$$

where $\lambda_{\omega^i} = \mathrm{rank}_{\mathbb{Z}_p} X(K_\infty)_{\omega^i}$ is the ω^i-part of the (unramified) Iwasawa λ-invariant of K_∞/K.

EXAMPLE 6.6. Let k be a real quadratic field with conductor d (the case that p divides d is allowed). We put $K = k(\mu_p)$. Let χ be the quadratic character of $G = \mathrm{Gal}(K/\mathbb{Q})$ corresponding to k. We may regard χ (resp. ω) as a Dirichlet character modulo d (resp. modulo p). In this case, we see

$$S_\chi = \{q \in S \mid \chi(q) \neq 0,\ \chi(q) = \omega(q)\}.$$

Hence S_χ consists of the primes in S which satisfy:

- $q \equiv 1 \pmod p$ and q splits in k, or
- $q \equiv -1 \pmod p$ and q is inert in k.

Assume that $S_\chi \neq \emptyset$. We put $P = \max\{p^{m_q} \mid q \in S_\chi\}$, then we obtain the formula

$$\mathrm{rank}_{\mathbb{Z}_p} X_S(K_\infty)_\chi = \mathrm{rank}_{\mathbb{Z}_p} X(K_\infty)_\chi + \sum_{q \in S_\chi} p^{m_q} - P.$$

Note that $\mathrm{rank}_{\mathbb{Z}_p} X(K_\infty)_\chi$ is equal to the (unramified) Iwasawa λ-invariant of k_∞/k. (If Greenberg's conjecture is true for k and p, then $\mathrm{rank}_{\mathbb{Z}_p} X(K_\infty)_\chi = 0$.) Since

$$\mathrm{rank}_{\mathbb{Z}_p} X_S(k_\infty) = \mathrm{rank}_{\mathbb{Z}_p} X_S(K_\infty)_\chi + \mathrm{rank}_{\mathbb{Z}_p} X_{S_e}(\mathbb{Q}_\infty)$$

(where ε is the trivial character), we can obtain a formula of the $\mathbb{Z}_p$-rank of $X_S(k_\infty)$ (including $\mathrm{rank}_{\mathbb{Z}_p} X(K_\infty)_\chi$).

EXAMPLE 6.7. Let $F/\mathbb{Q}$ be a cyclic extension of degree p. Assume that p is unramified in F. We put $K = F(\mu_p)$, and fix a character χ of $G = \mathrm{Gal}(K/\mathbb{Q})$ satisfying $K^{\ker(\chi)} = F$. Let σ be a fixed generator of $\mathrm{Gal}(F_\infty/\mathbb{Q}_\infty) \cong \mathrm{Gal}(F/\mathbb{Q})$, and $F^{(i)}$ the fixed field of F_∞ by $\overline{\langle \gamma\sigma^i \rangle}$ for $0 \le i \le p-1$ (hence $F^{(0)} = F$). For simplicity, we assume that every prime of S is not decomposed in $\mathbb{Q}_\infty$. Hence if $q \in S$ is unramified in F, then the splitting field of $F_\infty/\mathbb{Q}$ for q must be one of $F^{(0)}, \dots,$ or $F^{(p-1)}$. By the definition of χ, we see that $\chi^{-1}(\sigma)$ is defined, and we put $\chi^{-1}(\sigma) = \zeta$ (note that ζ is a primitive pth root of unity). In this case, we obtain that

$$S_\chi = \{q \in S \mid q \equiv 1 \pmod{p},\ q \text{ is not ramified in } F\}.$$

Under the assumption for S, we see $m_q = 0$ for all $q \in S_\chi$. When $q \in S_\chi$ splits in $F^{(i)}$, we see that $\chi^{-1}(\sigma_{p,q}) = \chi^{-1}(\sigma^i) = \zeta^i$, and hence $f_{q,\chi}(T) = (1+T) - \zeta^i\kappa_0$. We note that if $i \ne j$, then $(1+T) - \zeta^i\kappa_0$ and $(1+T) - \zeta^j\kappa_0$ are relatively prime. We put

$$S_{\chi,i} = \{q \in S_\chi \mid q \text{ splits in } F^{(i)}\},$$

for $0 \le i \le p-1$. Assume that $S_\chi \ne \emptyset$. From the above facts, we see that $\deg F(T)$ is equal to the number of non-empty $S_{\chi,i}$'s. That is,

$$\deg F(T) = |\Psi|, \quad \text{where} \quad \Psi = \{i \mid 0 \le i \le p-1,\ S_{\chi,i} \ne \emptyset\}.$$

Since $d_\chi = p-1$, we see

$$\mathrm{rank}_{\mathbb{Z}_p} X_S(K_\infty)_\chi = \mathrm{rank}_{\mathbb{Z}_p} X(K_\infty)_\chi + (p-1)\sum_{i\in\Psi}(|S_{\chi,i}| - 1).$$

ACKNOWLEDGEMENTS. The basic ideas of our proof of the main theorem are due to the previous paper [6]. The author express his thanks to Professors Yasushi Mizusawa and Manabu Ozaki for giving many suggestions during (and after) the collaborative work. The author also express his thanks to Dr. Takae Tsuji for answering a question, and to the referee for his/her useful comments. The author was supported by research grant from the Research Institute, Chiba Institute of Technology.

References

[1] A. Brumer: *On the units of algebraic number fields*, Mathematika **14** (1967), 121–124.

[2] B. Ferrero and L.C. Washington: *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. (2) **109** (1979), 377–395.
[3] R. Greenberg: *On a certain l-adic representation*, Invent. Math. **21** (1973), 117–124.
[4] R. Greenberg: *On p-adic L-functions and cyclotomic fields*. II, Nagoya Math. J. **67** (1977), 139–158.
[5] C. Greither: *Class groups of abelian fields, and the main conjecture*, Ann. Inst. Fourier (Grenoble) **42** (1992), 449–499.
[6] T. Itoh, Y. Mizusawa and M. Ozaki: *On the $\mathbb{Z}_p$-ranks of tamely ramified Iwasawa modules*, Int. J. Number Theory **9** (2013), 1491–1503.
[7] K. Iwasawa: *On $\mathbf{Z}_l$-extensions of algebraic number fields*, Ann. of Math. (2) **98** (1973), 246–326.
[8] K. Iwasawa: *Riemann–Hurwitz formula and p-adic Galois representations for number fields*, Tôhoku Math. J. (2) **33** (1981), 263–288.
[9] C. Khare and J.-P. Wintenberger: *Ramification in Iwasawa modules*, arXiv:`1011.6393`, (2010).
[10] Y. Mizusawa and M. Ozaki: *On tame pro-p Galois groups over basic $\mathbb{Z}_p$-extensions*, Math. Z. **273** (2013), 1161–1173.
[11] J. Neukirch, A. Schmidt and K. Wingberg: Cohomology of Number Fields, second edition, Grundlehren der Mathematischen Wissenschaften **323**, Springer, Berlin, 2008.
[12] L. Salle: *On maximal tamely ramified pro-2-extensions over the cyclotomic $\mathbb{Z}_2$-extension of an imaginary quadratic field*, Osaka J. Math. **47** (2010), 921–942.
[13] T. Tsuji: *Semi-local units modulo cyclotomic units*, J. Number Theory **78** (1999), 1–26.
[14] T. Tsuji: *On the Iwasawa λ-invariants of real abelian fields*, Trans. Amer. Math. Soc. **355** (2003), 3699–3714.
[15] L.C. Washington: Introduction to Cyclotomic Fields, second edition, Graduate Texts in Mathematics **83**, Springer, New York, 1997.

Division of Mathematics
Education Center
Faculty of Social Systems Science
Chiba Institute of Technology
2-1-1 Shibazono, Narashino, Chiba 275-0023
Japan
e-mail: tsuyoshi.itoh@it-chiba.ac.jp