ON THE IDEAL CLASS GROUPS OF
$\mathbb{Z}_p$-EXTENSIONS OVER REAL ABELIAN FIELDS

JAE MOON KIM, JA DO RYU

Abstract. Let $k$ be a real abelian field and $k_\infty = \bigcup_{n \geq 0} k_n$ be its $\mathbb{Z}_p$-extension for an odd prime $p$. For each $n \geq 0$, we denote the class number of $k_n$ by $h_n$. The following is a well known theorem:

**Theorem.** Suppose $p$ remains inert in $k$ and the prime ideal of $k$ above $p$ totally ramifies in $k_\infty$. Then $p \nmid h_0$ if and only if $p \nmid h_n$ for all $n \geq 0$.

The aim of this paper is to generalize above theorem:

**Theorem 1.** Suppose $H^1(G_n, E_n) \cong (\mathbb{Z}/p^n\mathbb{Z})^l$, where $l$ is the number of prime ideals of $k$ above $p$. Then $p \nmid h_0$ if and only if $p \nmid h_n$.

**Theorem 2.** Let $k$ be a real quadratic field. Suppose that $H^1(G_1, E_1) \cong (\mathbb{Z}/p\mathbb{Z})^l$. Then $p \nmid h_0$ if and only if $p \nmid h_n$ for all $n \geq 0$.

1. Introduction

Let $k$ be a number field. For each prime $p$, let $k_\infty$ be a $\mathbb{Z}_p$-extension of $k$. Namely, $k_\infty$ is an extension of $k$ whose Galois group over $k$ is isomorphic to the additive group of the $p$-adic integers $\mathbb{Z}_p$.

By infinite Galois theory, to each closed subgroup $p^n\mathbb{Z}_p$ of $\mathbb{Z}_p$, there corresponds a unique intermediate field $k_n$ such that $\text{Gal}(k_n/k) \cong \mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$ and that $k_\infty = \bigcup_{n \geq 0} k_n$.

For example, $\mathbb{Q}(\zeta_{p^n}) = \bigcup_{n \geq 1} \mathbb{Q}(\zeta_{p^n})$ is a $\mathbb{Z}_p$-extension of $\mathbb{Q}(\zeta_p)$, where $\zeta_{p^n}$ is a primitive $p^n$th root of 1. Let $\mathbb{Q}_n$ be the unique subfield of $\mathbb{Q}(\zeta_{p^{n+1}})$ whose degree over $\mathbb{Q}$ is $p^n$. Then $\mathbb{Q}_\infty = \bigcup_{n \geq 0} \mathbb{Q}_n$ is a

Received June 12, 1999.
Key words and phrases: $\mathbb{Z}_p$-extension, class number, circular units.
This paper was supported by research fund of Inha University, 1998.
\( \mathbb{Z}_p \)-extension of \( \mathbb{Q} \). In general, for any number field \( k \), \( k_{\infty} = k \mathbb{Q}_\infty \) is a \( \mathbb{Z}_p \)-extension of \( k \) and such a \( \mathbb{Z}_p \)-extension is called the basic (or cyclotomic) \( \mathbb{Z}_p \)-extension of \( k \). Thus every number field has at least one \( \mathbb{Z}_p \)-extension. When \( k \) is a totally real field, Leopoldt conjecture asserts that \( k \) admits only one \( \mathbb{Z}_p \)-extension, namely the basic \( \mathbb{Z}_p \)-extension. And Leopoldt conjecture is valid when \( k \) is a real abelian field ([11]).

Let \( k_{\infty} = \bigcup_{n \geq 0} k_n \) be a \( \mathbb{Z}_p \)-extension of \( k \). Let \( h_n \) be the class number of \( k_n \), and \( e_n \) the exact power of \( p \) in \( h_n \), i.e., \( p^{e_n} \mid h_n \). Then, by Iwasawa theory, there are integers \( \mu, \lambda \geq 0 \) and \( \nu \) such that \( e_n = \mu p^n + \lambda n + \nu \) for \( n \gg 0 \) ([3]). These constants are called the Iwasawa invariants of \( k_{\infty} \) over \( k \). In 1979, Ferrero and Washington ([1]) proved that \( \mu = 0 \) when \( k \) is an abelian field and \( k_{\infty} \) is the basic \( \mathbb{Z}_p \)-extension of \( k \). Around at the same time, Greenberg conjectured that \( \lambda = 0 \) if \( k \) is a totally real field and gave a number of examples supporting the conjecture ([2]). Therefore, if Greenberg conjecture holds for a real abelian field \( k \), then \( \mu = \lambda = 0 \) and thus \( e_n = \nu \) is a constant for \( n \gg 0 \), which is independent of \( n \).

It might happen that \( p \nmid h_n \) for all \( n \geq 0 \), i.e., \( \mu = \lambda = \nu = 0 \). The aim of this paper is to study when this happens. In certain cases, \( p \nmid h_0 \) is necessary and sufficient for \( p \nmid h_n \) for all \( n \geq 0 \). For instance, we have the following theorem ([11]):

**Theorem.** Suppose \( p \) remains inert in \( k \) and the prime ideal of \( k \) above \( p \) totally ramifies in \( k_{\infty} \). Then \( p \nmid h_0 \) if and only if \( p \nmid h_n \) for all \( n \geq 0 \).

In this paper we study generalizations of above theorem. Namely, we will find conditions under which the statement “\( p \nmid h_0 \) if and only if \( p \nmid h_n \)” is true.

### 2. Units and circular units

Let \( k \) be a real abelian field such that \( k \cap \mathbb{Q}_\infty = \mathbb{Q} \) and consider its basic \( \mathbb{Z}_p \)-extension \( k_{\infty} = \bigcup_{n \geq 0} k_n \) for an odd prime \( p \) such that \( p \nmid h_0 \) and \( p \nmid f \varphi(f) \), where \( f \) is the conductor of \( k \). Let \( E_n \) be the unit group of \( k_n \) and \( C_n \) the subgroup of \( E_n \) consisting of circular units defined by Sinnott ([10]). Let \( B_n \) be the Sylow \( p \)-subgroup of \( E_n/C_n \), and \( A_n \) that of the ideal class group of \( k_n \). Then the index theorem of Sinnott
On the ideal class groups of $\mathbb{Z}_p$-extensions over real abelian fields

says that $\#A_n = \#B_n$ if $p$ is an odd prime ([10]).

In this section, we introduce two exact sequences involving cohomology groups of units and circular units. The first one is well known and we omit its proof. For details, refer to [7].

Let $I_n$ be the ideal group of $k_n$ and $P_n$ its subgroup generated by principal ideals. Then we have the following exact sequence ([7]):

$$0 \to H^1(G_n, E_n) \to I_n^{G_n}/P_0 \to (I_n/P_n)^{G_n} \to \text{Ker}(\hat{H}^0(G_n, E_n) \to \hat{H}^0(G_n, k_n^\times)) \to 0,$$

where $G_n$ is the Galois group $\text{Gal}(k_n/k)$.

Since we are assuming $p \nmid h_0$, $I_0/P_0 = \{0\}$. Thus we get

$$(1) \quad 0 \to H^1(G_n, E_n) \to I_n^{G_n}/I_0 \to A_n^{G_n} \to \text{Ker}(\hat{H}^0(G_n, E_n) \to \hat{H}^0(G_n, k_n^\times)) \to 0.$$ 

For the second exact sequence, we need a lemma.

**Lemma 1.** Let $G_{m,n} = \text{Gal}(k_m/k_n)$ for $m > n \geq 0$. Then we have $C_{G_{m,n}} = C_n$.

**Proof.** Let $K_m = \mathbb{Q}(\zeta_{p^{m+1}})$ and $K_n = \mathbb{Q}(\zeta_{p^{n+1}})$. Then it is known that $C_{G_{m,n}} = C_n$, where $C_m$ (resp. $C_n$) is the group of cyclotomic units of $K_m$ (resp. $K_n$) ([5]). Obviously, $C_n \subset C_{G_{m,n}}$. To prove $C_{G_{m,n}} \subset C_n$, take $u \in C_{G_{m,n}}$. We will show that $u^d \in C_n$ and $u^{p^{m-n}} \in C_n$, where $d = [\mathbb{Q}(\zeta_{p^d}) : k]$. Then, since $(d, p^{m-n}) = 1$, we have $u \in C_n$.

First, we view $u$ as an element in $C_{G_{m,n}}$. Since $C_{G_{m,n}} = C_n$, $u \in C_n \cap k_m \subset k_n$. Therefore $N_{K_n/k_m}(u) = u^d \in C_n$. Next, note that $u^{p^{m-n}} = N_{k_m/k_n}(u)$ since $u$ is fixed under $G_{m,n}$. Thus $u^{p^{m-n}} \in C_n$. This proves the lemma. 

From the short exact sequence

$$0 \to C_n \to E_n \to B_n \to 0,$$


we have a long exact sequence
\[ 0 \to C_n^G \to E_n^G \to B_n^G \to H^1(G_n, C_n) \to H^1(G_n, E_n) \to H^1(G_n, B_n) \to \cdots. \]

Since \( C_n^G = C_0 \) and \( E_n^G = E_0 \), the first four terms of above sequence read:
\[ 0 \to C_0 \to E_0 \to B_0^G \to H^1(G_n, C_n) \to \cdots. \]

Thus we have
\[ 0 \to B_n^G / B_0 \to H^1(G_n, C_n) \to \cdots. \]

By the index theorem of Sinnott ([10]), \( B_0 = A_0 = \{0\} \). Therefore we obtain
\[(2) \quad 0 \to B_n^G \to H^1(G_n, C_n) \to H^1(G_n, E_n) \to H^1(G_n, B_n) \to \cdots. \]

3. Main theorems

Let \( k \) be a real abelian field and \( l \) the number of prime ideals of \( k \) above \( p \).

THEOREM 1. Suppose that \( H^1(G_n, E_n) \simeq (\mathbb{Z}/p^n\mathbb{Z})^l \). Then \( p \nmid h_0 \) if and only if \( p \nmid h_n \).

REMARKS.

1. It is known that \( \lim H^1(G_n, E_n) \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^l \), where the limit is taken under the inflation maps ([4]). Also, from the exact sequence (1) in Section 2, \( H^1(G_n, E_n) \leftarrow I_n^G / I_0 \simeq (\mathbb{Z}/p^n\mathbb{Z})^l \).

Thus it is plausible that \( H^1(G_n, E_n) \simeq (\mathbb{Z}/p^n\mathbb{Z})^l \). But this is not always the case. For instance, when \( k = \mathbb{Q}(\sqrt{85}) \) and \( p = 3 \), \( 3 \nmid h_0 \) but \( 3 \nmid h_1 \). Thus \( H^1(G_1, E_1) \neq (\mathbb{Z}/p\mathbb{Z})^2 \).

2. Suppose that \( l = 1 \), i.e., \( p \) remains inert in \( k \). Let \( \pi_n \) be a prime element of \( \mathbb{Q}_n \). Then \( \pi_n^{p-1} \) is an element of \( H^1(G_n, E_n) \) of order \( p^n \). Thus \( \mathbb{Z}/p^n\mathbb{Z} \) is a subgroup of \( H^1(G_n, E_n) \). On the other hand, by (1) of Section 2, \( H^1(G_n, E_n) \) is a subgroup
of $I_n^G/I_0 \simeq \mathbb{Z}/p^n\mathbb{Z}$. Therefore $H^1(G_n, E_n) \simeq \mathbb{Z}/p^n\mathbb{Z}$ when $p$ remains inert. Thus the hypothesis of Theorem 1 is satisfied in this case. Hence $p \nmid h_0$ if and only if $p \nmid h_n$. But this is nothing but the theorem in the introduction. Therefore Theorem 1 can be thought of as a generalization of the theorem in the introduction.

**Proof of theorem.** By class field theory, $p \nmid h_n$ implies $p \nmid h_0$. We will prove the converse.

First, we claim that the map $H^1(G_n, C_n) \to H^1(G_n, E_n)$ in (2) is surjective. Let $C_\infty = \bigcup_{n \geq 0} C_n$, $E_\infty = \bigcup_{n \geq 0} E_n$ and $B_\infty = \bigcup_{n \geq 0} B_n$. By taking direct limits under the inflation maps of the exact sequence (2), we obtain

$$0 \to B^\Gamma G_n \to H^1(G_n, C_n) \to H^1(G_n, E_n) \to H^1(G_n, B_n) \to H^1(G_n, B_n) \to \cdots,$$

where $\Gamma = Gal(k_\infty/k)$. Note that $B^\Gamma G_n$ is finite, and that $H^1(\Gamma, C_\infty) \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^l ([8])$. Since $H^1(G_n, E_n) \simeq (\mathbb{Z}/p^n\mathbb{Z})^l$, $H^1(\Gamma, E_\infty) = (\mathbb{Q}_p/\mathbb{Z}_p)^l$ by taking limits. Thus $H^1(\Gamma, C_\infty) \to H^1(\Gamma, E_\infty)$ is surjective since $(\mathbb{Q}_p/\mathbb{Z}_p)^l$ has no finite nontrivial cokernel. Now consider the following commutative diagram:

$$
\begin{array}{cccccc}
0 & \rightarrow & B_G^G & \rightarrow & H^1(G_n, C_n) & \rightarrow & H^1(G_n, E_n) \rightarrow 0 \\
0 & \rightarrow & B^\Gamma G_n & \rightarrow & H^1(\Gamma, C_\infty) & \rightarrow & H^1(\Gamma, E_\infty) & \rightarrow & 0
\end{array}
$$

where vertical maps are inflation maps. From the injectivity of the inflation map $H^1(G_n, E_n) \to H^1(\Gamma, E_\infty)$, we see that $H^1(G_n, E_n) \to H^1(G_n, B_n)$ is the zero map. Thus $H^1(G_n, C_n) \to H^1(G_n, E_n)$ is surjective.

Then the sequence (2) in Section 2 reads:

$$0 \to B_G^G \to H^1(G_n, C_n) \to H^1(G_n, E_n) \to 0.$$

Since $H^1(G_n, C_n) \simeq (\mathbb{Z}/p^n\mathbb{Z})^l \simeq H^1(G_n, E_n)([8])$, $B_G^G$ must be trivial. Therefore $B_n = \{0\}$. Hence $A_n = \{0\}$ by the index theorem. This finishes the proof. \qed
Corollary 1. Suppose $p \nmid h_0$. If $H^1(G_n, E_n) \simeq (\mathbb{Z}/p^n\mathbb{Z})^l$, then $E_0 \cap N_{k_n/k}(k_n^\times) = N_{k_n/k}(E_n)$.

Proof. By Theorem 1, $A_n = \{0\}$. So $A_n^{G_n} = \{0\}$. Then by the sequence (1) in Section 2, $\text{Ker}((\hat{H}^0(G_n, E_n) \to \hat{H}^0(G_n, k_n^\times)) = 0$. Thus $\hat{H}^0(G_n, E_n) \to \hat{H}^0(G_n, k_n^\times)$ is injective, i.e., $E_0 / N_{k_n/k}(E_n) \to k^\times / N_{k_n/k}(k_n^\times)$ is injective. Therefore $E_0 \cap N_{k_n/k}(k_n^\times) = N_{k_n/k}(E_n)$. □

When $k$ is a real quadratic field, one can say a little more.

Corollary 2. Let $k$ be a real quadratic field, and suppose that $H^1(G_1, E_1) \simeq (\mathbb{Z}/p\mathbb{Z})^l$. Then $p \nmid h_0$ if and only if $p \nmid h_n$ for all $n \geq 0$.

Proof. If $p \nmid h_0$, then $p \nmid h_1$ by theorem 1. Then this implies $p \nmid h_n$ for all $n \geq 0$ ([6]). □

Theorem 2. Let $k$ be a real quadratic field. Suppose that the fundamental unit of $k$ is not a norm of a unit of $k_1$. Then $p \nmid h_0$ if and only if $p \nmid h_n$ for all $n \geq 0$.

Proof. By Corollary 2, it is enough to show that $H^1(G_1, E_1) \simeq (\mathbb{Z}/p\mathbb{Z})^l$. Since $[k : \mathbb{Q}] = 2$, $l = 1$ or 2. If $l = 1$, there is nothing to prove by the theorem in the introduction or by the remark after Theorem 1. So we may assume $l = 2$ and we will show that $H^1(G_1, E_1) \simeq (\mathbb{Z}/p\mathbb{Z})^2$. Then the theorem follows from Corollary 2. □

The condition of Theorem 2 says that $\hat{H}^0(G_1, E_1)$ is nontrivial. Hence $\hat{H}^0(G_1, E_1)$ has $\mathbb{Z}/p\mathbb{Z}$ as its subgroup. Since the Herbrand quotient for $E_1$ is $p$ ([9]), $\#H^1(G_1, E_1) = p^2 \#\hat{H}^0(G_1, E_1)$. Thus $p^2 \mid \#H^1(G_1, E_1)$. But $H^1(G_1, E_1)$ injects into $(\mathbb{Z}/p\mathbb{Z})^2$ by the sequence (1). Therefore $H^1(G_1, E_1) \simeq (\mathbb{Z}/p\mathbb{Z})^2$ and this completes the proof.

References

On the ideal class groups of $\mathbb{Z}_p$-extensions over real abelian fields


Department of Mathematics
Inha University
Incheon, 402-751, Korea