GREENBERG’S CONJECTURE AND RELATIVE UNIT GROUPS FOR REAL QUADRATIC FIELDS

TAKASHI FUKUDA (福田隆・日大産工)

ABSTRACT. For an odd prime number $p$ and a real quadratic field $k$, we consider relative unit groups for intermediate fields of the cyclotomic $\mathbb{Z}_p$-extension of $k$ and discuss the relation to Greenberg’s conjecture.

1. INTRODUCTION

Greenberg’s conjecture claims that $\mu_p(k)$ and $\lambda_p(k)$ both vanish for any prime number $p$ and any totally real number field $k$ (cf. [9]). Here $\mu_p(k)$ and $\lambda_p(k)$ denote the Iwasawa invariants for the cyclotomic $\mathbb{Z}_p$-extension of $k$. A Galois extension $K/k$ is called a $\mathbb{Z}_p$-extension if the Galois group $G(K/k)$ is topologically isomorphic to the additive group of the ring of $p$-adic integers $\mathbb{Z}_p$ and said to be cyclotomic if it is contained in the field obtained by adjoining all $p$-power-th roots of unity to $k$ (cf. [13]). This conjecture is still open in spite of the efforts of many mathematicians (cf. [3], [4], [6], [8], [10], [11], [15], [16], [18], [19]) even in real quadratic case. In [3], we verified numerically the conjecture for $p=3$ and some real quadratic fields $k$ in which 3 splits, using the invariants $n_0^{(2)}$ and $n_2^{(2)}$ which were defined generally in [20]. In order to calculate $n_0^{(2)}$ and $n_2^{(2)}$, we introduced the notion of relative unit group in [3]. In this paper, we study the structure of the relative unit groups for all intermediate fields of the cyclotomic $\mathbb{Z}_p$-extension of $k$, and see that the relative unit group is closely related to Greenberg’s conjecture.

2. RELATIVE UNIT GROUP

Let $p$ be an odd prime number and $k$ a real quadratic field. Let $Q = Q_0 \subset Q_1 \subset \cdots \subset Q_\infty$ and $k = k_0 \subset k_1 \subset \cdots \subset k_\infty$ be the cyclotomic $\mathbb{Z}_p$-extensions. Note that $Q_n$ is a cyclic extension of degree $p^n$ over $Q$, $k_n = kQ_n$ is a cyclic extension of degree $2p^n$ over $Q$ and $k \cap Q_n = Q$. We denote by $E(F)$ the unit group of an algebraic number field $F$ and by $N_{L/F}$ the norm map for a finite
Galois extension $L/F$. We define the relative unit group $E_{n,R}$ for $k_n$ by

$$E_{n,R} = \{ \epsilon \in E(k_n) \mid N_{k_n/Q_n}(\epsilon) = \pm 1, \ N_{k_n/k}(\epsilon) = \pm 1 \}.$$ 

Note that this definition is slightly different from the original one of Leopoldt (cf. [17]).

**Lemma 2.1.** The free rank of $E_{n,R}$ is $p^n - 1$.

**Proof.** Let $\epsilon$ be any element of $E(k_n)$. Then,

$$\epsilon^{2p^n} N_{k_n/Q_n}(\epsilon)^{-p^n} N_{k_n/k}(\epsilon)^{-2} \in E_{n,R},$$

and hence

$$E(k_n)^{2p^n} \subset E(Q_n)E(k)E_{n,R} \subset E(k_n).$$

Since $E(Q_n)E(k) \cap E_{n,R} = \{ \pm 1 \}$, we see that

$$\text{rank}_\mathbb{Z}(E_{n,R}) = \text{rank}_\mathbb{Z}(E(k_n)) - \text{rank}_\mathbb{Z}(E(Q_n)) - \text{rank}_\mathbb{Z}(E(k)) = 2p^n - 1 - (p^n - 1) - 1 = p^n - 1.$$ 

The Galois group $G(k_n/Q)$ acts on $E(k_n)$ and $E_{n,R}$. We investigate the Galois module structure of $E_{n,R}$. It is well known that there exists so called Minkowski unit in $E(k_n)$. We see that $E_{n,R}$ also has such a unit.

**Lemma 2.2.** Let $K_1$ and $K_2$ be finite Galois extensions over $\mathbb{Q}$ satisfying $K_1 \cap K_2 = \mathbb{Q}$ and let $L = K_1 K_2$. Let

$$E_R = \{ \epsilon \in E(L) \mid N_{L/K_i}(\epsilon) = \pm 1 \text{ for } i = 1, 2 \}.$$ 

Then there exists $\eta \in E_R$ such that

$$(E_R : \langle \eta^\sigma \mid \sigma \in G(L/\mathbb{Q}) \rangle) < \infty.$$ 

**Proof.** Let $G = G(L/Q)$ and let $H_i = G(L/K_i)$, $h_i = |H_i|$ for $i = 1, 2$. For $\epsilon \in E(L)$ and $\sigma \in G$, we see that

$$N_{L/K_i}(\epsilon)^\sigma = \prod_{\tau \in H_i} \epsilon^{\tau H_i} = \prod_{\tau \in H_i} \epsilon^{\sigma^{-1} \tau \sigma} = N_{L/K_i}(\epsilon^\sigma).$$

Therefore $E_R$ is stable under the action of $G$. Let $\epsilon$ be a Minkowski unit of $L$. Then $m = (E(L) : \langle \epsilon^\sigma \mid \sigma \in G \rangle)$ is finite and

$$\eta = \epsilon^{h_1 h_2} N_{L/K_1}(\epsilon)^{-h_2} N_{L/K_2}(\epsilon)^{-h_1} \in E_R.$$ 

Let $\xi$ be any element of $E_{n,R}$. We can write

$$\xi^m = \prod_{\sigma \in G} \epsilon^{a_{\sigma, \sigma}}.$$
with suitable integers $a_{\sigma}$. Then,

$$\prod_{\sigma \in G} \eta^{a_{\sigma} \sigma} = \xi^{m_{h_{1}h_{2}}}N_{L/K_{1}}(\xi)^{-m_{h_{2}}}N_{L/K_{2}}(\xi)^{-m_{h_{1}}} = \pm \xi^{m_{h_{1}h_{2}}}.$$ 

Hence we have $E_{R}^{m_{h_{1}h_{2}}} \subset <-1, \eta^{\sigma} | \sigma \in G> \subset E_{R}$. □

We fix a topological generator $\sigma$ of $G(k_{\infty}/Q)$ and write $\epsilon_{i} = \epsilon^{\sigma^{i}}$ for $\epsilon \in E(k_{\infty})$ and $i \in \mathbb{Z}$.

**Lemma 2.3.** We have $\epsilon_{r} = \pm (\epsilon_{0} \cdots \epsilon_{r-2})/(\epsilon_{1} \cdots \epsilon_{r-1})$ for $\epsilon \in E_{n,R}$.

**Proof.** Since $N_{k_{n}/Q}(\epsilon) = \epsilon_{0} \epsilon_{r+1} = \pm 1$, we have $\epsilon_{r+1} = \pm \epsilon_{0}^{-1}$. Then,

$$N_{k_{n}/k}(\epsilon) = \epsilon_{0} \epsilon_{2} \cdots \epsilon_{r-2} \epsilon_{r} \epsilon_{r+2} \cdots \epsilon_{2r} = \epsilon_{0} \epsilon_{2} \cdots \epsilon_{r-2} \epsilon_{r} (\epsilon_{1} \cdots \epsilon_{r-1})^{-1} = \pm 1.$$

From this we have the desired relation. □

The next corollary follows from Lemmas 2.2 and 2.3, and this leads us to the following definition.

**Corollary 2.4.** There exists $\epsilon \in E_{n,R}$ such that

$$(E_{R} : <-1, \epsilon_{0}, \epsilon_{1}, \cdots, \epsilon_{r-1}>) < \infty.$$ 

**Definition 2.5.** We say that $E_{n,R}$ has a $p$-normal basis if there exists $\epsilon \in E_{n,R}$ such that $<-1, \epsilon_{0}, \epsilon_{1}, \cdots, \epsilon_{r-1}>$ has a finite index prime to $p$ in $E_{n,R}$.

We put

$$E_{n,R,p^{n}} = \{ \epsilon \in E_{n,R} | \epsilon^{1+\sigma} \in E_{n,R}^{p^{n}} \}.$$ 

We see that $E_{n,R,p^{n}}$ is a fairly small subgroup of $E_{n,R}$. Indeed, if we put

$$V_{n} = E_{n,R,p^{n}}/E_{n,R}^{p^{n}},$$

then $V_{n}$ is a finite group.

**Proposition 2.6.** The order of $V_{n}$ is $p^{n}$.

Now, we define the $p$-rank $r(V_{n})$ of $V_{n}$ to be $\dim_{F_{p}}(V_{n}/V_{n}^{p})$. Since the map $V_{n} \ni \Phi E_{n,R}^{p^{n}} \mapsto \Phi^{p} E_{n+1,R}^{p^{n+1}} \in V_{n+1}$ is injective, we obtain the following lemma.

**Lemma 2.7.** $r(V_{n}) \leq r(V_{n+1})$ for all $n \geq 1$. 


On the other hand, as we shall see in the following sections, $r(V_n)$ is bounded. The following proposition states a relation between the group structure of $V_n$ and the Galois module structure of $E_{n,R}$.

**Proposition 2.8.** $V_n$ is cyclic if and only if $E_{n,R}$ has a $p$-normal basis.

In order to prove Propositions 2.6 and 2.8, we have to prepare some lemmas. For a subgroup $E$ of $E(k_n)$, we put $\bar{E} = E / \text{tor}(E)$ and denote by $\bar{e}$ the image of $e$ under the homomorphism $E \rightarrow \bar{E}$.

**Lemma 2.9.** The endomorphism $1 + \sigma$ of $\bar{E}_{n,R}$ is injective.

*Proof.* Let $e$ be an element of $E_{n,R}$ satisfying $e^{1+\sigma} = \pm 1$. Then we have $e_1 = \pm e_0^{-1}$ and $e_2 = e_0$. Since $r$ is even, we have $e_0 = e_r = \pm e_0^{r}$ from Lemma 2.3. Hence $e^{r+1} = \pm 1$. Since $k_n$ is real, we have $e = \pm 1$. $\square$

**Lemma 2.10.** Let $e \in E_{n,R}$ and $N = \langle -1, e_0, e_1, \ldots, e_{r-1} \rangle$. If $(E_{n,R} : N)$ is finite, then $\bar{N}/\bar{N}^{1+\sigma} \simeq \mathbb{Z}/p^n\mathbb{Z}$.

*Proof.* It is clear from Lemma 2.9 that $\{ \bar{e}_0, \bar{e}_1, \ldots, \bar{e}_{r-1} \}$ forms a free basis of $\bar{N}$ over $\mathbb{Z}$ and $\{ \bar{e}_0^{1+\sigma}, \bar{e}_1^{1+\sigma}, \ldots, \bar{e}_{r-1}^{1+\sigma} \}$ forms a free basis of $\bar{N}^{1+\sigma}$ over $\mathbb{Z}$. From Lemma 2.3, we have $\bar{e}_r^{1+\sigma} = (\bar{e}_0 \bar{e}_2 \cdots \bar{e}_{r-2})^{-1} \bar{e}_1 \bar{e}_3 \cdots \bar{e}_{r-3}^{2} \bar{e}_{r-1}$. It is easy to see that the invariant of $r \times r$ matrix

$$
\begin{pmatrix}
1 & 1 & 0 & \cdots & 0 & 0 \\
0 & 1 & 1 & \cdots & 0 & 0 \\
\vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & 1 & 1 & 0 \\
0 & 0 & \cdots & 0 & 1 & 1 \\
-1 & -1 & \cdots & -1 & 2
\end{pmatrix}
$$

is $(1, 1, \cdots, 1, p^n)$. The desired isomorphism immediately follows from this. $\square$

**Lemma 2.11.** Let $M$ be a finitely generated free $\mathbb{Z}$-module and $f$ an injective endomorphism of $M$. If $N$ is a submodule of $M$ such that $(M : N) < \infty$ and $f(N) \subset N$, then $(M : f(M)) = (N : f(N))$.

*Proof.* Let $\text{rank}_\mathbb{Z}(M) = n$. There exist $v_i \in M$, $x_i \in \mathbb{Z}$ ($1 \leq i \leq n$) such that $M = \bigoplus_{1 \leq i \leq n} \mathbb{Z}v_i$, $N = \bigoplus_{1 \leq i \leq n} \mathbb{Z}x_i v_i$.

We write $f(v_i) = \sum_{1 \leq j \leq n} a_{ij} v_j$.
with suitable integers $a_{ij}$. Then,

$$(M : N)(N : f(N)) = (M : f(N))
= |\det(x_{i}a_{ij})|
= |\prod x_{i}| \cdot |\det(a_{ij})|
= (M : N)(M : f(M)).$$

From the finiteness of this expression, we have $(M : f(M)) = (N : f(N))$. □

**Proof of Proposition 2.6.** From Corollary 2.4, we can choose $\eta \in E_{n,R}$ such that $N = <-1, \eta_{0}, \eta_{1}, \cdots, \eta_{r-1}>$ has a finite index in $E_{n,R}$. Then we have

(1) 
$$(\overline{E}_{n,R} : \overline{E}_{n,R}^{1+\sigma}) = (\overline{N} : \overline{N}^{1+\sigma}) = p^{n}$$

from Lemmas 2.9, 2.11 and 2.10. We claim that

$$\overline{E}_{n,R}^{1+\sigma} = \overline{E}_{n,R}^{p^{n}}.$$ 

Indeed, $\overline{E}_{n,R}^{1+\sigma} \subset \overline{E}_{n,R}^{p^{n}}$ is clear from definition. Conversely, take $\varepsilon \in E_{n,R}$. Then $\varepsilon^{p^{n}} \in \overline{E}_{n,R}^{1+\sigma}$ from (1) and hence $\varepsilon^{p^{n}} = \gamma^{1+\sigma}$ for some $\gamma \in E_{n,R}$. It is clear that $\gamma \in E_{n,R,p^{n}}$ and so $\varepsilon^{p^{n}} \in \overline{E}_{n,R}^{1+\sigma}$. Then we have

(2) 
$$V_{n} \simeq \overline{E}_{n,R,p^{n}} / \overline{E}_{n,R}^{p^{n}} \simeq \overline{E}_{n,R}^{1+\sigma} / \overline{E}_{n,R}^{p^{n}(1+\sigma)} = \overline{E}_{n,R}^{p^{n}} / \overline{E}_{n,R}^{p^{n}(1+\sigma)} \simeq \overline{E}_{n,R} / \overline{E}_{n,R}^{1+\sigma}$$

from Lemma 2.9. Therefore (1) implies that $|V_{n}| = p^{n}$. □

**Lemma 2.12.** Let $M$ be a finitely generated $\mathbb{Z}$-module, $N$ a submodule of $M$ and $p$ a prime number. If $M = pM + N$, then $(M : N)$ is finite and prime to $p$.

**Proof.** The assertion follows from $p(M/N) = (pM + N)/N = M/N$. □

**Proof of Proposition 2.8.** First assume that $V_{n}$ is cyclic. Then there exists $\Phi \in E_{n,R}$ such that $V_{n} = <\Phi E_{n,R}^{p^{n}} >$. We choose $\varphi \in E_{n,R}$ such that $\Phi^{1+\sigma} = \varphi^{p^{n}}$. The isomorphism (2) implies that $\overline{E}_{n,R} = < \varphi > \overline{E}_{n,R}^{1+\sigma}$. Then, we have

$$\overline{E}_{n,R} = < \varphi > \overline{E}_{n,R}^{1+\sigma}
= < \varphi, \varphi^{1+\sigma} > \overline{E}_{n,R}^{(1+\sigma)^{2}}
= < \varphi, \varphi^{1+\sigma}, \cdots, \varphi^{(1+\sigma)^{r}} > \overline{E}_{n,R}^{(1+\sigma)^{r+1}}
= < \varphi_{0}, \varphi_{1}, \cdots, \varphi_{r-1} > \overline{E}_{n,R}^{p}$$
because \( \bar{E}_{n,R} \supset \bar{E}_{n,R}^{p} \supset \bar{E}_{n,R}^{(1+\sigma)p^{n}} \). Hence, Lemma 2.12 immediately shows that \( E_{n,R} \) has a \( p \)-normal basis. Conversely assume that there exists \( \varphi \in E_{n,R} \) such that \( N = \langle -1, \varphi_0, \varphi_1, \ldots, \varphi_{r-1} \rangle \) has a finite index \( p \)-prime to \( p \) in \( E_{n,R} \). Put

\[
\Phi = \varphi_0 \varphi_1^{-2} \varphi_2 \cdots \varphi_{r-1}^{-1}.
\]

We see from Lemma 2.3 that \( \Phi^{1+\sigma} = \pm (\varphi_0 \varphi_1^{-1} \varphi_2 \cdots \varphi_{r-1}^{-1}) p^n \) and hence \( \Phi \in E_{n,R,p^n} \). If the order of \( \Phi \bar{E}_{n,R}^{p^n} \) in \( V_n \) is less than \( p^n \), then \( \Phi^{p^{n-1}} \in E_{n,R}^{p^n} \) and so \( \Phi^{1/p} \in E_{n,R} \). Then

\[
\langle -1, \varphi_0, \varphi_1, \ldots, \varphi_{r-1} \rangle = \langle -1, \Phi, \varphi_1, \ldots, \varphi_{r-1} \rangle
\]

\[
\subset \Phi^{1/p}, \varphi_1, \ldots, \varphi_{r-1} \rangle \subset E_{n,R}
\]

shows that \( (E_{n,R} : N) \) is divisible by \( p \). This is a contradiction. Hence, the order of \( \Phi \bar{E}_{n,R}^{p^n} \) is not less than \( p^n \) and \( V_n = \langle \Phi \bar{E}_{n,R}^{p^n} \rangle \) from Proposition 2.6. \( \square \)

We give two more lemmas to use in the following sections. Throughout the following, we abbreviate \( E_n = E(k_n) \).

**Lemma 2.13.** Let \( \phi \) be the fundamental unit of \( k \) and \( s \) an integer such that \( 0 \leq s \leq n \). Then \( N_{k_n/k}(E_n) \supset E_0^{p^s} \) if and only if \( \phi^{p^s} \eta \in E_0^{p^n} \) for some \( \eta \in E_{n,R,p^n} \).

**Proof.** First assume that \( N_{k_n/k}(E_n) \supset E_0^{p^s} \) and take \( \epsilon \in E_n \) such that \( N_{k_n/k}(\epsilon) = \phi^{p^s} \). Then

\[ \eta = \epsilon^{2p^{n-s}}N_{k_n/k}(\epsilon)^{-p^{n-s}} \phi^{-2} \in E_{n,R} \]

and moreover \( \eta^{p^s} \in E_{n,R,p^n} \). We see that \( \phi^{p^s} \eta^{p^s} \in E_0^{p^n} \). Conversely, if \( \phi^{p^s} \eta = \epsilon^{p^n} \) for some \( \eta \in E_{n,R,p^n} \) and \( \epsilon \in E_n \), then \( N_{k_n/k}(\epsilon)^{p^n} = \pm \phi^{p^{n+s}} \) and hence \( N_{k_n/k}(\epsilon) = \pm \phi^{p^{s}} \) because \( k \) is real. \( \square \)

**Lemma 2.14.** Assume further that \( V_n = \langle \Phi \bar{E}_{n,R}^{p^n} \rangle \) is cyclic under the same conditions in Lemma 2.13. Then \( N_{k_n/k}(E_n) = E_0^{p^s} \) if and only if \( \phi^i \Phi \in E_{n}^{p^{n-s}} \) for some integer \( i \) and \( \phi_j \Phi \notin E_{n}^{p^{n-s+1}} \) for any integer \( j \).

**Proof.** First we give a notice when \( s = 0 \). Namely, we have \( \phi^i \Phi \notin E_{n}^{p^{n+1}} \) for any integer \( j \). Indeed, if \( \phi^i \Phi \in E_{n}^{p^{n+1}} \) for some \( j \), then \( \phi^j \Phi = \alpha^{p^{n+1}} \) for some \( \alpha \in E_n \). It easily follows that \( j \) is prime to \( p \) and that \( \Phi \in E_0^{p^s} \) by applying \( N_{k_n/k} \), which is a contradiction. Now assume that \( N_{k_n/k}(E_n) \supset E_0^{p^s} \). Then, from the above lemma, \( \phi^{p^n} \eta \in E_{n}^{p^n} \) for some \( \eta \in E_{n,R,p^n} \). Since \( V_n = \langle \Phi \bar{E}_{n,R}^{p^n} \rangle \), we can write \( \eta = \Phi^j \alpha^{p^n} \) for some \( j \in \mathbb{Z} \) and \( \alpha \in E_{n,R} \). We see that \( \phi^{p^n} \Phi^j \in E_{n}^{p^n} \) and hence \( j = p^s j' \) with \( (j', p) = 1 \). Hence, \( \phi^{p^n} \Phi^j \in E_{n}^{p^{n-s}} \). Since \( j' \) is prime to \( p \), there exists
an integer \( i \) such that \( \phi^i \Phi \in E_n^{p^{-s}} \). Conversely, if \( \phi^i \Phi \in E_n^{p^{-s}} \) for some integer \( i \), then we easily see that \( N_{k_n/k}(E_n) \supset E_0^p \). Hence we have

\[
N_{k_n/k}(E_n) \supset E_0^p \iff \phi^i \Phi \in E_n^{p^{-s}} \text{ for some } i.
\]

This completes the proof because \( N_{k_n/k}(E_n) = E_0^p \) is equivalent to \( N_{k_n/k}(E_n) \supset E_0^p \) and \( N_{k_n/k}(E_n) \not\supset E_0^{p^{-s}-1} \).

3. Application to Greenberg's Conjecture (Non-split case)

Throughout this section, we assume that \( p \) does not split in \( k \). We discuss a relation between \( V_n \) and Greenberg's conjecture of this case. Let \( A_n \) be the \( p \)-Sylow subgroup of the \( n \)-th layer \( k_n \) of the cyclotomic \( \mathbb{Z}_p \)-extension of \( k \). Let \( \iota_{n,m} : k_n \rightarrow k_m \) be the inclusion map for \( 0 \leq n \leq m \).

The equality

\[
(E_0 : N_{k_n/k}(E_n)) = |\ker(A_0 \rightarrow A_n)|
\]

which was proved in [12] is fundamental in this case. The following theorem gives an necessary and sufficient condition for the conjecture in this case.

**Theorem 3.1 (Theorem 1 in [9]).** \( \mu_p(k) = \lambda_p(k) = 0 \) if and only if \( \iota_{0,n} : A_0 \rightarrow A_n \) is zero map for some \( n \geq 1 \).

The capitantual affair of \( A_0 \rightarrow A_n \) is related to the property of \( V_n \) through Lemmas 2.13 and 2.14. We first state the boundedness of \( r(V_n) \).

**Lemma 3.2.** If \( |\ker(A_0 \rightarrow A_n)| \leq p^s \), then \( r(V_n) \leq s + 1 \).

**Proof.** Since \( |\ker(A_0 \rightarrow A_n)| \leq p^n \) from (3), we may assume that \( s \leq n \). Furthermore, if \( n - 1 \leq s \leq n \), then the claim is clear from proposition 2.6. So we assume that \( s < n - 1 \). We have \( (E_0 : N_{k_n/k}(E_n)) \leq p^s \) again from (3). Therefore \( N_{k_n/k}(E_n) \supset E_0^{p^s} \) and \( \phi^{p^s} \eta \in E_0^{p^s} \) for some \( \eta \in E_{n,R,p^n} \) from Lemma 2.13. If \( r(V_n) \geq s + 2 \), then the exponent of \( V_n \) is less than \( p^{n-s} \) from Proposition 2.6. Therefore \( \eta^{p^{n-s}} \in E_{n,R}^{p^n} \) and so \( \eta \in E_{n,R}^{p^{n+1}} \). It follows that \( \phi \in E_n^p \), which is a contradiction. Hence, \( r(V_n) \leq s + 1 \).

**Corollary 3.3.** If \( |A_0| = p^s \), then \( r(V_n) \leq s + 1 \) for all \( n \geq 1 \).

**Corollary 3.4.** If \( \iota_{0,n} : A_0 \rightarrow A_n \) is injective, then \( V_n \) is cyclic.

As we shall see later, the converse of Corollary 3.4 is not always true. But we have the following theorem.

**Theorem 3.5.** \( \iota_{0,n} : A_0 \rightarrow A_n \) is injective for all \( n \geq 1 \) if and only if \( V_n \) is cyclic for all \( n \geq 1 \).
Proof. Assume that $i_{0,m} : A_0 \rightarrow A_m$ is not injective for some $m \geq 1$. Since $|\text{Ker}(A_0 \rightarrow A_n)|$ is bounded, there exists $n \geq 1$ such that

$$|\text{Ker}(A_0 \rightarrow A_n)| = |\text{Ker}(A_0 \rightarrow A_{n+1})| = p^s > 1.$$ 

If $V_{n+1}$ is cyclic, then $V_n$ is also cyclic from Lemma 2.7. Let $V_{n+1} = \langle \Psi E_{n+1,R}^{p^{n+1}} \rangle$ and $V_n = \langle \Phi E_{n,R}^{p^n} \rangle$. Let $\Phi^p = \Psi^j \alpha^{p^n}$ for some $j \in \mathbb{Z}$ and $\alpha \in E_{n+1,R}$. Since $\Psi$ is not $p$-th power in $E_{n+1,R}$ and $\Phi$ is not $p$-th power in $E_{n,R}$, $j$ is divisible by $p$ but not divisible by $p^2$. Hence $\Psi = \Phi^i \beta^{p^n}$ for some $\beta \in E_{n+1,R}$ and integer $i$ prime to $p$. Now, $N_{k_{n+1}/k}(E_{n+1}) = E_{n+1}^{p^s}$ and Lemma 2.14 imply that $\phi^j \Psi = \phi^j \Phi^i \beta^{p^n} \in E_{n+1}^{p^{n+1}}$ for some integer $j$. It follows that $\phi^j \Phi^i \in E_{n+1}^{p^{n+1}}$ because $s \geq 1$ and that $\phi^j \Phi^i \in E_{n+1}^{p^{n+1}}$ because $k_{n+1}/k_n$ is a cyclic extension of degree $p$ of real fields. Hence $\phi^j \Phi^i \in E_{n+1}^{p^{n+1}}$ for some integer $j'$ because $i$ is prime to $p$. This is a contradiction in view of $N_{k_n/k}(E_n) = E_0^{p^s}$ and Lemma 2.14. This completes the proof. $\square$

We give a few examples when $p = 3$. Let $H_n = \text{Ker}(A_0 \rightarrow A_n)$. The calculations have been done with a computer.

Example 3.6. Let $k = \mathbb{Q}(\sqrt{257})$. Then $|H_1| = |A_0| = 3$ (cf. [6]) and $V_1 \simeq \mathbb{Z}/3\mathbb{Z}$. This is a trivial counter example for the converse of Corollary 3.4. Next let $k = \mathbb{Q}(\sqrt{443})$. Then $|H_1| = 1$, $|H_2| = |A_0| = 3$ (cf. [6]) and $V_2 \simeq \mathbb{Z}/9\mathbb{Z}$. This is a non-trivial counter example.

Example 3.7. Let $k = \mathbb{Q}(\sqrt{1937})$. In Table 1 of [6], the value of $\lambda_3(k)$ was not known. But we see that $V_2 \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and that $A_0 \rightarrow A_2$ is zero map from Corollary 3.4. Hence $\lambda_3(k) = 0$ from Theorem 3.1. The same argument can be applied for $\mathbb{Q}(\sqrt{3305})$, $\mathbb{Q}(\sqrt{5063})$ and $\mathbb{Q}(\sqrt{6995})$.

Example 3.8. There are 31 $k$'s in Table 1 of [6] for which the value of $|H_2|$ is not known. For four $k$'s in Example 3.7, we have $|H_2| = 3$ because $A_0 \rightarrow A_2$ is zero map. For the rest 27 $k$'s, we verified that $V_2$ is cyclic and $|H_2| = 1$ by constructing numerically a unit $\varepsilon$ of $k_2$ such that $N_{k_2/k}(\varepsilon) = \phi$ using Lemma 2.14.

Example 3.9. Let $k = \mathbb{Q}(\sqrt{254})$. Then $|A_0| = 3$. We could verify that $A_0 \rightarrow A_3$ is injective by constructing a unit $\varepsilon$ of $k_3$ such that $N_{k_3/k}(\varepsilon) = \phi$ using Lemma 2.14. It seems that $A_0 \rightarrow A_4$ is also injective. But the calculation exceeded the capacity of computer.

Remark. In recent papers [10], [15] and [16], it was proved independently that $\lambda_3(\mathbb{Q}(\sqrt{254})) = 0$. Their arguments show that $A_0 \rightarrow A_5$ is zero map.

We discuss a relation about a normal integral basis. We say that a $\mathbb{Z}_p$-extension $K/F$ has a normal $p$-integral basis if $\mathcal{O}_{F_n}[1/p]$ is a free $\mathcal{O}_F[1/p][G(F_n/F)]$-module for each intermediate field $F_n$ of $K/F$. Here $\mathcal{O}_F$ denotes the ring of integers of $F$.  


$F_n$. We restrict our argument to the case $p = 3$ because a connection to a normal integral basis becomes clear in this case. Let $k = \mathbb{Q}(\sqrt{d})$ for a positive square-free integer $d$ which is congruent to 2 modulo 3 and $k^- = \mathbb{Q}(\sqrt{-3d})$. It is known that $k^-$ has the $\mathbb{Z}_3$-extension $k^-_\infty$ such that $k^-_\infty$ is a Galois extension over $\mathbb{Q}$ and $G(k^-_\infty/\mathbb{Q})$ is isomorphic to the semi direct product of $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}_3$. It is called the anti-cyclotomic $\mathbb{Z}_3$-extension of $k^-$. Then the next result is known (cf. Corollary 3.9 of [1]). See also Theorem 2.3 of [14] and Theorem of [5].

**Theorem 3.10.** $k^-_\infty/k^-$ has a normal 3-integral basis if and only if $A_0 \longrightarrow A_n$ is injective for all $n \geq 1$.

Using Proposition 2.8 and Theorem 3.5, we can give equivalent conditions in terms of relative unit groups.

**Theorem 3.11.** The following three conditions are equivalent.

1. $k^-_\infty/k^-$ has a normal 3-integral basis.
2. $E_{n,R}$ has a 3-normal basis for all $n \geq 1$.
3. $V_n$ is cyclic for all $n \geq 1$.

Viewing Theorems 3.1 and 3.10, we are led to the next conjecture which is weaker than Greenberg’s conjecture.

**Conjecture 3.12.** Let $k$ be a real quadratic field in which 3 remains prime. If the class number of $k$ is divisible by 3, then $k^-_\infty/k^-$ does not have a normal 3-integral basis.

Professor K. Komatsu first told the author the importance of studying this conjecture in connection with Greenberg’s one. Concerning this conjecture, we give two examples.

**Example 3.13.** Let $k = \mathbb{Q}(\sqrt{32009})$. Then $A_0 \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and $|H_1| = 3$. Hence, $k^-_\infty/k^-$ does not have a normal 3-integral basis from Theorem 3.10. Furthermore, we can see that $V_2 \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and $|H_2| = 9$ using Lemma 2.13. Hence $\lambda_3(k) = 0$ from Theorem 3.1. This example is interesting by reason that $A_0$ is not cyclic. Similar examples in the split case are given in [7].

**Example 3.14.** Let $k = \mathbb{Q}(\sqrt{53678})$. Then $A_0 \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and $|H_1| = 1$. we can see that $V_2$ is cyclic and $|H_2| = 3$ using Lemma 2.14. Hence $k^-_\infty/k^-$ does not have a normal 3-integral basis. We do not know whether $\lambda_3(k) = 0$.

**Remark.** Dr. Sumida kindly informed the author that he verified $\lambda_3(\mathbb{Q}(\sqrt{53678})) = 0$ with the method in [11].
4. Application to Greenberg's Conjecture (split case)

Throughout this section, we assume that $p$ splits in $k$. As in the preceding section, we discuss a relation between $V_n$ and Greenberg's conjecture in this case. Let $(p) = pp'$ be the prime decomposition of $p$ in $k$ and $p_n$ the prime ideal of $k_n$ lying over $p$. Let $D_n = <\mathrm{cl}(p_n)> \cap A_n$ and $B_n$ the subgroup of $A_n$ consisting of elements which are invariant under the action of $G(k_n/k)$. We note that $D_n \subset B_n$. The following theorem is known as a necessary and sufficient condition for the conjecture in this case.

**Theorem 4.1 (Theorem 2 in [9]).** $\mu_p(k) = \lambda_p(k) = 0$ if and only if $B_n = D_n$ for all sufficiently large $n$.

An integer $n_2$ was defined in [4] by

$$(p)^{n_2} \mid (\phi^{p-1} - 1),$$

where $\phi$ denotes the fundamental unit of $k$. Then the behavior of $|B_n|$ is explicitly described as follows.

**Proposition 4.2 (Proposition 1 in [4]).** We have $|B_n| = |A_0|p^{n-1}$ for all $n \geq n_2 - 1$.

Therefore, in order to investigate Greenberg's conjecture, it is important to study the behavior of $|D_n|$. Since $\mathbb{Q}_n$ is contained in $\mathbb{Q}(\zeta_p^{n+1})$, the unique prime ideal of $\mathbb{Q}_n$ lying over $p$ is principal. We fix a generator $\pi_n$ of it and put

$$\Theta_n = (p\pi_n^r - p^{n})^{r/2},$$

where $r = p^n - 1$ as before. Then $\Theta_n$ is a unit of $\mathbb{Q}_n$ and satisfies

(4) $\Theta_n^{1-\sigma} \in E_n^{p^n}$,

(5) $p\Theta_n^2 \in k_n^{p^n}$

and

(6) $\Theta_n/\Theta_{n+1} \in E_{n,R,p^n}^{p^n}$.

We note that $\Theta_n$ can be written explicitly in terms of cyclotomic units in certain cases (cf. Lemma 3.1 of [3]). Then the order of $D_n$ is described using $\Theta_n$ and $V_n$ as follows.

**Lemma 4.3.** Let $\phi$ be the fundamental unit of $k$ and $s$ an integer such that $0 \leq s \leq n$. Let $d$ be the order of $\mathrm{cl}(p)$ and take a generator $\alpha \in k$ of $p^d$. Then $|D_n| \leq p^n|D_0|$ if and only if $\alpha^{p^s}\Theta_n^d\phi^i\eta \in k_n^{p^n}$ for some $i \in \mathbb{Z}$ and $\eta \in E_{n,R,p^n}$.
Proof. Note that \( \alpha^{1+\sigma} = \pm p^d \). Assume that \( |D_n| \leq p^s|D_0| \) and take a generator \( \beta \in k_n \) of \( p_n^{p^d} \). Then \( (\beta^{p^{-s}}) = p_n^{dp^s} = p^d = (\alpha) \). Hence, \( \beta^{p^{-s}} = \alpha \epsilon \) for some \( \epsilon \in E_n \). From this, we see that \( N_{k_n/k}(\epsilon) \in E_p^{p^{-s}} \). Let \( N_{k_n/k}(\epsilon) = \tau \) and \( N_{k_n/k}(\epsilon) = \pm \phi^{d p^{-s}} \). Then, \( \eta = \epsilon^{2 p^s \tau^{-2p^s}} \in E_n \) and \( \alpha^{2 p^s \tau^{-2p^s}} \in k_p^{p^n} \). Taking norm from \( k_n \) to \( \Omega_n \), we see that \( p_n^{2dp^s \tau^{-2p^s}} \in k_p^{p^n} \) and hence \( \tau^p \Theta_{n}^{-\tau dp^s} \in k_p^{p^n} \) from (5). Therefore, \( \alpha^{2 dp^s \Theta_n^{dp^s} \phi^{2i}} \in k_p^{p^n} \). Since \( (\alpha \Theta_n)^{1+\sigma} = \pm \phi \Theta_n^{1+\sigma} \equiv \Theta_n^{-d(1-\sigma)} \mod k_p^{p^n} \), we have \( (\alpha \Theta_n)^{1+\sigma} \in k_p^{p^n} \) from (4). Therefore, we see that \( \eta \in E_{n,R,p^n} \). Since \( p \) is odd, we completed one side of the proof. Conversely, if \( \alpha \Theta_n^{dp^s \phi^i \Phi^j} \in k_p^{p^n} \) with \( \beta \in k_n \), then \( p_n^{dp^s} = p^d = (\alpha)^p = (\beta)^p \) and hence \( p_n^{dp^s} = (\beta) \). \( \square \)

If \( V_n \) is cyclic, then Lemma 4.3 becomes the following form.

Lemma 4.4. Assume further that \( V_n = \Phi E_{n,R}^{p^n} \) is cyclic under the same conditions in Lemma 4.3. Then \( |D_n| = p^n|D_0| \) if and only if \( \alpha \Theta_n^{dp^s \phi^i \Phi^j} \in k_p^{p^n} \) for some integers \( i, j \) and \( \alpha \Theta_n^{dp^s \phi^i \Phi^j} \not\in k_p^{p^n} \) for any integers \( i, j \).

Proof. The proof is straightforward. We only give a remark in the case that \( s = 0 \). Namely it holds that \( \alpha \Theta_n^{dp^s \phi^i \Phi^j} \not\in k_p^{p^n} \) for any integers \( i, j \). Indeed, if \( \alpha \Theta_n^{dp^s \phi^i \Phi^j} = \beta^{p^n+1} \) for some \( i, j \in \mathbb{Z} \) and \( \beta \in k_n \), then \( p^d = (N_{k_n/k}(\beta))^p \). This is a contradiction. \( \square \)

Now, we can describe the boundedness of \( r(V_n) \).

Lemma 4.5. If \( |D_n| \leq p^n|D_0| \), then \( r(V_n) \leq s + 1 \).

Proof. Since \( |D_n| \leq p^n|D_0| \), we may assume that \( s \leq n \). Furthermore, if \( n - 1 \leq s \leq n \), then the claim is clear from Proposition 2.6. So we assume that \( s < n - 1 \). Applying Lemma 4.3 with the same notations, we have \( \alpha \Theta_n^{dp^s \phi^i \eta} \in k_p^{p^n} \) for some \( i \in \mathbb{Z} \) and \( \eta \in E_{n,R,p^n} \). If \( r(V_n) \geq s + 2 \), then the exponent of \( V_n \) is less than \( p^{-s+1} \), so \( \eta^{p_n^{-s+1}} \in E_p^{p^n} \) and \( \eta \in E_p^{p^{s+1}} \). From this, we see that \( i \) is divisible by \( p^n \) and \( \alpha \Theta_n^{dp^s \phi^i} \in k_n^{p^n} \) for some \( j \in \mathbb{Z} \). If we put \( \beta = \alpha \phi^j \), then we see that \( \beta^{1-\sigma} \in k_p^{p^n} \) from (4), and hence \( \beta^{1-\sigma} = \gamma p \) for some \( \gamma \in k \) because \( k \) is real. Then \( (p^d)^{\delta} = (\alpha^{1-\sigma}) = (\beta^{1-\sigma}) = (\gamma)^p \) implies that \( p \) divides \( d \). Thus, from \( p^d = \pm \alpha^{1+\sigma} = \pm \beta^{1+\sigma} = \pm \beta^2 \gamma^{-p} \), we can write \( \beta = \delta p \) for some \( \delta \in k \). Then we have \( p^d = (\alpha) = (\beta) = (\delta)^p \), and hence \( p^{d/p} = (\delta) \), which contradicts the fact that \( d \) is the order of \( \text{cl}(p) \). Hence \( r(V_n) \leq s + 1 \). \( \square \)

Corollary 4.6. If \( |A_0/D_0| = p^s \), then \( r(V_n) \leq n_2 + s \) for all \( n \geq 1 \).

Proof. We have \( |D_n| \leq p^{n_2+s-1}|D_0| \) from Proposition 4.2 for all sufficiently large \( n \) and apply Lemmas 4.5 and 2.7. \( \square \)

Corollary 4.7. If \( |D_n| = |D_0| \), then \( V_n \) is cyclic.
We remark a difference between split case and non-split case. In the split case, if \( A_0 = D_0 \), then the genus formula for \( k_n/k \) yields that

\[
|D_n| = |D_0| \frac{p^n}{(E_0 : N_{k_n/k}(E_n))}.
\]

Hence, we see the following.

**non-split case:**

\[
N_{k_n/k}(E_n) = E_0 \iff |D_n| = |D_0| \iff V_n : \text{cyclic}
\]

**split case with \( A_0 = D_0 \):**

\[
N_{k_n/k}(E_n) = E_0^{p^n} \iff |D_n| = |D_0| \iff V_n : \text{cyclic}
\]

Namely, the opposite properties of the norm map \( N_{k_n/k} : E_n \to E_0 \) both implies the cyclicity of \( V_n \). We notice some relations between the norm map and the order of \( D_n \) that hold without the assumption \( A_0 = D_0 \).

**Lemma 4.8 (cf. Proposition 6.3 of [2]).** If \( N_{k_n/k}(E_n) = E_0 \), then \( |D_n| = p^n|D_0| \).

**Proof.** Let \( B'_n \) denote the subgroup of \( B_n \) consisting of ideal classes which contain an ideal invariant under the action of \( G(k_n/k) \). Then \( B_n = \iota_{0,n}(A_0)D_n \) and the genus formula for \( k_n/k \) yields that

\[
|B'_n| = |A_0| \frac{p^n}{(E_0 : N_{k_n/k}(E_n))} = p^n|A_0|.
\]

Hence, from

\[
p^n|A_0| = \frac{|i_{0,n}(A_0)|}{|i_{0,n}(A_0) \cap D_n|} \leq \frac{|i_{0,n}(A_0)|}{|i_{0,n}(D_0) \cap D_n|} = \frac{|i_{0,n}(A_0)|}{|i_{0,n}(D_0)|} \frac{|D_n|}{|D_n^{p^n}|} \leq p^n |i_{0,n}(A_0)|,
\]

we see that \( |i_{0,n}(A_0)| = |A_0| \) and hence \( i_{0,n} \) is injective. Therefore, we have that

\[
\frac{|D_n|}{|D_0|} = \frac{|D_n|}{|i_{0,n}(D_0)|} = \frac{|D_n|}{|D_n^{p^n}|} = p^n.
\]

\[ \square \]

**Lemma 4.9.** If \( |D_n| = |D_0| \), then \( N_{k_n/k}(E_n) = E_0^{p^n} \).

**Proof.** We see that \( V_n \) is cyclic from Corollary 4.7 and apply Lemma 4.4 with the same notations. Namely we have \( \alpha \Theta^d \phi^i \Phi^j \in k_n^{p^n} \) for some \( i, j \in \mathbb{Z} \). Now assume that \( \phi^j \Phi \in E_n^p \) for some \( j \in \mathbb{Z} \). Then we see that \( \alpha \Theta^d \phi^j \in k_n^p \) for some \( j \in \mathbb{Z} \) and derive a contradiction as in the proof of Lemma 4.5. Hence \( \phi^j \Phi \not\in E_n^p \) for any \( j \in \mathbb{Z} \) and the claim follows from Lemma 2.14. \[ \square \]

Corollary 4.7 indicate a relation between the cyclicity of \( V_n \) and the order of \( D_n \). But the converse of Corollary 4.7 is not always true. Furthermore an analogue to
Theorem 3.5 is also not true. Namely we can not conclude that $|D_n| = |D_0|$ for all $n \geq 1$ even if $V_n$ is cyclic for all $n \geq 1$. However, by numerical calculations, we are led to the following conjecture.

**Conjecture 4.10.** $A_n = D_n$ for all $n \geq 0$ if and only if $V_n$ is cyclic for all $n \geq 1$.

At present, concerning this conjecture, we can only prove that the first condition implies the second one. First we give a remark about the first condition. Remember the integer $n_0$ defined in [20]. Namely, let $d$ be the order of $\text{cl}(p)$ and take a generator $\alpha$ of $p^d$. Then $n_0$ is defined to be the integer satisfying

$$p^{n_0} || (\alpha^{p^n - 1} - 1).$$

The inequality $n_0 \leq n_2$ is needed for the uniqueness of $n_0$. Then we obtain the following lemma.

**Lemma 4.11.** The following three conditions are equivalent:

1. $A_n = D_n$ for all $n \geq 0$.
2. $A_1 = D_1$.
3. $A_0 = D_0$ and $n_0 = 1$.

**Proof.** It is clear that (1) implies (2). Next assume (2). Then it follows that $A_0 = D_0$ because norm maps $A_1 \rightarrow A_0$ and $D_1 \rightarrow D_0$ are both surjective. If $n_0 \geq 2$, then $n_2 \geq 2$ and so $|D_1| = p|D_0|$ from Proposition 4.2. Let $d$ be the order of $\text{cl}(p)$ and take a generator $\alpha$ of $p^d$. Then, by local class field theory, $\alpha$ is a $p'$-adic norm for $k_1/k$ and also $l$-adic norm if $l$ is a prime ideal of $k_1$ prime $p$. Hence, by the product formula of the norm residue symbol and Hasse’s norm theorem, $\alpha$ is a global norm. Let $\alpha = N_{k_1/k}(\alpha_1)$ for some $\alpha_1 \in k_1$ and $a = p_1^d(\alpha_1^{-1})$. Then $N_{k_1/k}(a) = (1)$ and hence $a = b^{p^n - 1}$ for some ideal $b$ of $k_1$, where $\rho$ is a generator of $G(k_1/k)$. Therefore $D_1^d \subset A_1^{\rho - 1}$. Since $|D_1| = p|D_0|$, it follows that $A_1^{\rho - 1} \neq 1$, which contradicts the assumption $A_1 = D_1$. Hence $n_0 = 1$. Therefore (2) implies (3). Finally assume (3). Since $n_0 = n_1$ in the case that $A_0 = D_0$, Theorem 1 in [4] shows that $A_n = D_n$ for all sufficiently large $n$. Noting that norm maps $A_{n+1} \rightarrow A_n$ and $D_{n+1} \rightarrow D_n$ are both surjective for any $n$, we conclude that (1) holds. □

Now we give a partial answer for Conjecture 4.10.

**Theorem 4.12.** If $A_n = D_n$ for all $n \geq 0$, then $V_n$ is cyclic for all $n \geq 1$.

**Proof.** We see that $A_0 = D_0$ and $n_0 = 1$ from Lemma 4.11. Let $n$ be a sufficiently large integer. We have $|D_n| \leq p^{n_2 - 1}|D_0|$ from Proposition 4.2. Let $d$ be the order of $\text{cl}(p)$ and take a generator $\alpha$ of $p^d$ satisfying $p^d || (\alpha^{p^n - 1} - 1)$. From Lemma 4.3, we see that $\alpha^p \Theta_n^{\eta} \phi_i \eta = \beta^{p^n}$ for some $i \in \mathbb{Z}$, $\eta \in E_{n,R,p^n}$ and $\beta \in k_n$. Then $N_{k_n/k}(\beta) = \pm \alpha^{p^{n-1}} \phi_i$. If $p$ divides $i$, then $p^{n_2} || (N_{k_n/k}(\beta)^{p^n - 1} - 1)$, which is a contradiction because $n$ is sufficiently large. Hence $p$ does not divide $i$. Now
assume that $V_n$ is not cyclic. Then $\eta^{n-1} \in E_{n,R}$ and so $\eta \in E_{n,R}$. Therefore $\alpha^{n-1} \Theta_{n}^{d_{n-1}} \phi \in k_{n}^{p}$. If $n_2 = 1$, then we see that $\alpha \Theta_{n}^{d_{n}} \phi \in k_{n}^{p}$, which is a contradiction as we have seen in the proof of Lemma 4.5. Otherwise, if $n_2 > 1$, then we see that $\phi \in k_{n}^{p}$ and so $\phi \in k_{n}^{p}$, which is also a contradiction. Hence $V_n$ is cyclic for all sufficiently large $n$. The claim immediately follows from Lemma 2.7. \( \square \)

If we assume Greenberg's conjecture, then we can prove that the converse of Theorem 4.12 is also true.

**Theorem 4.13.** Assume that Greenberg's conjecture holds for $k$ and $p$. If $V_n$ is cyclic for all $n \geq 1$, then $A_n = D_n$ for all $n \geq 0$.

**Proof.** Let $|A_0/D_0| = p^t$ and $s = n_2 + t - 1$. Let $n$ be sufficiently large. Since Greenberg's conjecture holds, we have

$$|D_n| = |D_{n-1}| = p^s|D_0|$$

from Theorem 4.1 and Proposition 4.2. Let $V_n = \Phi E_{n,R}^{p^n}$ and $V_{n-1} = \Psi E_{n-1,R}^{p^n}$. We may assume that $\Phi = \Psi \gamma^{p^n}$ with suitable $\gamma \in E_n$. Let $d$ be the order of $Cl(p)$ and take a generator $\alpha$ of $P^d$ satisfying $p^{n_0} || (\alpha^{p-1} - 1)$. From Lemma 4.4, we see that $\alpha^{p^s} \Theta_{n}^{d_{n}} \phi \Phi = \beta^{p^n}$ for some integers $i, j$ and $\beta \in k_n$. First assume that $s \geq 1$. If $p$ divides $i$, then $p$ also divides $j$ because $\Phi \notin k_{n}^{p}$. Let $i = pi'$ and $j = pj'$. Using (6), we see that $\alpha^{p^s} \Theta_{n-1}^{d_{n-1}} \phi \Phi' \in k_{n-1}^{p^n}$. Then Lemma 4.4 again shows that $|D_{n-1}| \leq p^{s-1}|D_0|$, which contradicts $|D_n| = |D_{n-1}|$. Therefore $p$ does not divide $i$. Since $N_{k_n/k}(\beta) = \pm \alpha^{p^s} \phi$ is a $p'$-adic $p^{n-1}$-th power in $k$ and $n$ is sufficiently large, we conclude that $n_0 + s = n_2$. This means that $n_0 = 1$ and $t = 0$. Next assume that $s = 0$. Then $n_2 + t = 0$ implies that $n_2 = 1$ and $t = 0$. This completes the proof. \( \square \)

Finally we give a few examples when $p = 3$ based on calculations with a computer.

**Example 4.14.** Let $k = \mathbb{Q}(\sqrt{727})$. Then $|D_0| = 1$ and $|D_1| = 3$ (cf. [8]). This is a trivial counter example for the converse of Corollary 4.7. Next let $k = \mathbb{Q}(\sqrt{2713})$. Then $|D_0| = |D_1| = 1$ and $|D_2| = 3$ (cf. [3]). Furthermore we see that $V_2 \simeq \mathbb{Z}/9\mathbb{Z}$. This is a non-trivial counter example.

**Example 4.15.** Let $k = \mathbb{Q}(\sqrt{m})$ where $m = 3469, 5971, 6187$ and 7726. For these $k$'s, we could not calculate the values of $n_0^{(2)}$ and $n_2^{(2)}$ in [3]. Now we see that $V_2 \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ for these $k$'s. Corollary 4.7, Proposition 4.2 and Theorem 4.1 immediately show that $\lambda_3(k) = 0$ for $m = 3469, 5971$ and 6187. It can be also deduced from Theorem 2 in [8]. We calculated $n_0^{(2)}$ and $n_2^{(2)}$ using Lemmas 4.3 and 2.13. We show the results below.
For $m = 7726$, we can not decide the value of $\lambda_3(k)$.

**Remark.** In [11], it is shown that $\lambda_3(\mathbb{Q}(\sqrt{7726})) = 0$.

**References**


| $m$       | $n_0^{(2)}$ | $n_2^{(2)}$ | $|D_2|$ | $\lambda_3(k)$ |
|-----------|-------------|-------------|------|----------------|
| 3469      | 3           | 3           | 3    | 0              |
| 5971      | 3           | 4           | 3    | 0              |
| 6187      | 3           | 3           | 3    | 0              |
| 7726      | 3           | 3           | 3    | ?              |


DEPARTMENT OF MATHEMATICS, COLLEGE OF INDUSTRIAL TECHNOLOGY, NIHON UNIVERSITY, 2-11-1 SHIN-EI, NARASHINO, CHIBA, JAPAN

E-mail: fukuda@math.cit.nihon-u.ac.jp