On capitulation of S-ideals in $\mathbf{Z}_p$-extensions

Dedicated to the memory of Professor Kenkichi Iwasawa

Hiroki Sumida*

Abstract

Let k be a finite extension of $\mathbf{Q}$ and p a prime number. Let K be a $\mathbf{Z}_p$-extension of k and S the set of all prime ideals in k which are ramified in K. We denote by A'_∞ the p-Sylow subgroup of the S-divisor class group of K. We give a criterion for $A'_\infty = 0$ which can be applied for general $\mathbf{Z}_p$-extensions. Further we especially investigate the criterion for a totally real number field k in which p splits completely.

1 Introduction

Let k be a finite extension of $\mathbf{Q}$ and p a prime number. Let K be a $\mathbf{Z}_p$-extension of k and $k_n \subset K$ the unique cyclic extension of k of degree p^n. Further let S be the set of all prime ideals in k which are ramified in K. By Theorem 1 in [11], all prime ideals in S lie above p. We assume that all prime ideals in S are fully ramified in K. We denote by A_n the p-Sylow subgroup of the ideal class group of k_n. We put $A_\infty = \varinjlim A_n$, where the map : $A_n \to A_m$ is induced by the natural inclusion map $i_{n,m} : k_n \hookrightarrow k_m$ for $m \geq n$. We will denote the induced maps by $i_{n,m}$. Similarly we denote by A'_n the p-Sylow subgroup of the S-ideal class group of k_n and put $A'_\infty = \varinjlim A'_n$.

The main purpose of this paper is to investigate capitulation of S-ideals $H'_n = \mathrm{Ker}(i_{n,\infty} : A'_n \to A'_\infty)$. For totally real fields k and $K = k_\infty$ the cyclotomic $\mathbf{Z}_p$-extension, some criteria for $A'_\infty = 0$, i.e. $A'_n = H'_n$ for all n were given in [2, 4, 5, 6, 20]. We first generalize them to apply for general

*Partly supported by the Grants-in-Aid for Scientific Research, The Ministry of Education, Science and Culture, Japan.
2000 Mathematics Subject Classification. 11R23

number fields k and general $\mathbf{Z}_p$-extensions. Put $S_n = \{\mathfrak{p}_n | \mathfrak{p}_n^{p^n} = i_{0,n}(\mathfrak{p}), \mathfrak{p} \in S\}$. Denote by $k_{n,\mathfrak{p}_n}$ the completion of k_n at $\mathfrak{p}_n$ and by $U_{\mathfrak{p}_n}$ the group of principal units in $k_{n,\mathfrak{p}_n}$. We define the following groups (cf. [19]):

$$U_n = \{(u_{\mathfrak{p}_n}) \in \prod_{\mathfrak{p}_n \in S_n} U_{\mathfrak{p}_n} | \prod_{\mathfrak{p}_n \in S_n} \left(\frac{u_{\mathfrak{p}_n}, k_m/k_n}{\mathfrak{p}_n} \right) = 1 \text{ for all } m \geq n\},$$

$$V_{\mathfrak{p}_n} = \bigcap_{m \geq n} N_{k_{m,\mathfrak{p}_m}/k_{n,\mathfrak{p}_n}} U_{\mathfrak{p}_m}, \quad V_n = \prod_{\mathfrak{p}_n \in S_n} V_{\mathfrak{p}_n},$$

$$W_{\mathfrak{p}_n} = \bigcap_{m \geq n} N_{k_{m,\mathfrak{p}_m}/k_{n,\mathfrak{p}_n}} k_{m,\mathfrak{p}_m}^{\times}, \quad W_n = \prod_{\mathfrak{p}_n \in S_n} W_{\mathfrak{p}_n},$$

where $\left(\frac{u,k'/k}{\mathfrak{p}}\right)$ is the norm residue symbol. Let d_n be the diagonal map $k_n^{\times} \to \prod_{\mathfrak{p}_n \in S_n} k_{n,\mathfrak{p}_n}^{\times}$. Let E_n be the group of units in k_n and E'_n the group of S-units in k_n. Define

$$\overline{E}_n = \overline{U_n \cap d_n(E_n)} \text{ and } \overline{E}'_n = \overline{U_n \cap (d_n(E'_n) W_n)},$$

where $\overline{A}$ is the topological closure of A.

Theorem 1. *The following statements are equivalent.*
(1) $A'_{\infty} = 0$.
(2) $A'_0 \cong H^1(k_n/k, E'_n)$ *and* $U_n = V_n \overline{E}'_n$ *for some* n.

For every totally real number field k and the cyclotomic $\mathbf{Z}_p$-extension k_{∞}, it is conjectured that $\sharp A_n$ is bounded as $n \to \infty$, which is equivalent to $A_{\infty} = 0$ (see [5, 11]). If Leopoldt's conjecture is valid for k and p, i.e. ($\mathbf{Z}$-rank of E_0) = ($\mathbf{Z}_p$-rank of $\overline{E}_0$), the conjecture is equivalent to $A'_{\infty} = 0$. Several authors gave sufficient conditions for the conjecture and verified them for $p = 3$ and quadratic fields with small discriminants (see [2, 4, 7, 8, 13]). However the conjecture is not proved in general. Following [5], we study two typical cases. (A) Only one prime ideal in k ramifies in K. (B) k is a totally real number field in which p splits completely, and Leopoldt's conjecture is valid for k and p. By studying inflation maps $H^2(k_n/k, E'_n) \to H^2(k_m/k, E'_m)$, we can show a difference between (A) and (B). The following corollary and theorem are reformulations of Theorem 1 and Theorem 2 in [5].

Corollary 1. *Assume* (A). *The following statements are equivalent.*
(1) $A'_{\infty} = 0$.
(2) $A'_0 \cong H^1(k_n/k, E'_n)$ *for some* n.

This corollary is immediately obtained from Theorem 1. In contrast to the former result, Theorem 1 in [5], we do not have to assume that k is totally real. For an extension M/L and a subgroup A of $M^\times$, we define

$$R(M/L, A) = \mathrm{Ker}(H^2(M/L, A) \to H^2(M/L, M^\times)).$$

Let j_n be the natural map $R(k_n/k, E_n) \to R(k_n/k, E'_n)$. For a $\mathbf{Z}$-module A, put $\mathrm{rk}_p A = \dim_{\mathbf{F}_p}(A/pA)$. We denote by $m \gg n$ that $m - n$ is sufficiently large.

Theorem 2. *Assume* (B). *The following statements are equivalent.*
(1) $A'_\infty = 0$.
(2) $A'_0 \cong H^1(k_n/k, E'_n)$ *for some* n *and*
$\mathrm{rk}_p R(k_m/k, E'_m) = \mathrm{rk}_p(R(k_m/k, E'_m)/j_m(R(k_m/k, E_m)))$ *for all* $m \gg 0$.

If (1) holds, the last statement can be verified by finite steps. We will give an example which explains how to apply (2) for verification of (1).

For a general number field k, let $\tilde{k}$ be the composite of all $\mathbf{Z}_p$-extensions of k and $L_{\tilde{k}}$ the maximal unramified abelian p-extension of $\tilde{k}$. Greenberg conjectured that $\mathrm{Gal}(L_{\tilde{k}}/\tilde{k})$ is pseudo-null as a $\mathbf{Z}_p[[\mathrm{Gal}(\tilde{k}/k)]]$-module. When k is totally real and Leopoldt's conjecture is valid for k and p, this is equivalent to the above conjecture. For this generalized conjecture, capitulation of S-ideal classes in $\mathbf{Z}_p$-extensions is also important (cf. [15, 17]). We hope our criterion will play some role for study of multiple $\mathbf{Z}_p$-extensions.

2 General case

We use the same notation as in introduction. Put $\Gamma = \mathrm{Gal}(K/k)$ and $\Gamma_n = \mathrm{Gal}(K/k_n)$. Fix a topological generator γ of Γ and put $\gamma_n = \gamma^{p^n}$. We denote by $N_{m,n}$ the norm map $k_m \to k_n$ for $m \geq n$. We will denote induced maps by $N_{m,n}$. Put $s = \sharp S = \sharp S_n$ and $H_n = \mathrm{Ker}(i_{n,\infty} : A_n \to A_\infty)$. For a G-module A, we denote by A^G the fixed subgroup by all elements in G.

The following proposition was proved by Greenberg (see Proposition 2 and the proof of Theorem 1 in [5]).

Proposition 1. *The following statements are equivalent.*
(1) $\sharp A_n$ *is bounded as* $n \to \infty$.
(2) $A_n = H_n$ *for all* $n \geq 0$.
(3) $A_n^\Gamma \subseteq H_n$ *for all* $n \geq 0$.
(4) $A_\infty = 0$.

In a similar way, we can prove the following proposition.

Proposition 2. *The following statements are equivalent.*
(1) $\sharp A'_n$ *is bounded as* $n \to \infty$.
(2) $A'_n = H'_n$ *for all* $n \geq 0$.
(3) ${A'_n}^{\Gamma} \subseteq H'_n$ *for all* $n \geq 0$.
(4) $A'_\infty = 0$.

Let D_n be the subgroup of A_n consisting of classes which contain ideals whose prime divisors lie above S. Then we have $A'_n = A_n/D_n$. Let I_n be the ideal group of k_n, P_n the principal ideal group of k_n and $Q_n = \{\mathfrak{a} \in I_n |$ all prime divisors of $\mathfrak{a}$ lie above $S\}$. Put $D_{m,n} = ((Q_m i_{n,m}(P_n))/i_{n,m}(P_n))[p]$ and identify A_n with $(i_{n,m}(I_n)/i_{n,m}(P_n))[p]$, where $A[p]$ is the p-Sylow subgroup of A.

Lemma 1. *There are exact sequences:*

$$0 \to H^1(k_m/k_n, E_m) \to D_{m,n}A_n \to A_m^{\Gamma_n} \to R(k_m/k_n, E_m) \to 0,$$

$$0 \to H^1(k_m/k_n, E'_m) \to A'_n \to {A'_m}^{\Gamma_n} \to R(k_m/k_n, E'_m) \to 0.$$

Further

$$H^1(k_m/k_n, E_m) \cong E_m[N_{m,n}]/E_m^{\gamma_n - 1},$$

$$R(k_m/k_n, E_m) \cong (E_0 \cap N_{m,n}k_m^\times)/N_{m,n}E_m,$$

$$H^1(k_m/k_n, E'_m) \cong E'_m[N_{m,n}]/{E'_m}^{\gamma_n - 1},$$

$$R(k_m/k_n, E'_m) \cong (E'_0 \cap N_{m,n}k_m^\times)/N_{m,n}E'_m,$$

where $A[N_{m,n}] = \mathrm{Ker}(A \to A\ (a \mapsto N_{m,n}a))$.

Proof. We obtain the above exact sequences from the p-part of seven term exact sequences independently found by Auslander-Brumer and Chase-Harrison-Rosenberg (see [1, 12]). For a $\mathrm{Gal}(k_m/k_n)$-module A, since $\mathrm{Gal}(k_m/k_n)$ is cyclic, we have

$$H^1(k_m/k_n, A) \cong A[\nu_{n,m}]/A^{\gamma_n - 1} \text{ and } H^1(k_m/k_n, A) \cong A[\gamma_n - 1]/A^{\nu_{n,m}},$$

where $\nu_{n,m} = \sum_{i=0}^{p^{m-n}-1} \gamma_n^i$, $A[\nu_{n,m}] = \mathrm{Ker}(A \to A\ (a \mapsto a^{\nu_{n,m}}))$ and $A[\gamma_n - 1] = \mathrm{Ker}(A \to A\ (a \mapsto a^{\gamma_n - 1}))$. Since $N_{m,n}a = a^{\nu_{n,m}}$ and $A^{\Gamma_n} = A[\gamma_n - 1]$, the lemma follows. $\square$

Lemma 2. *For* $\varepsilon \in E'_n$, $\varepsilon \in N_{m,n}k_m^\times$ *if and only if* $d_n(\varepsilon) \in W_n U_n^{p^{m-n}}$.

Proof. For a prime ideal $\mathfrak{q}_n$ of k_n which is not contained in S_n, $\mathfrak{q}_n$ does not ramify in k_m. Hence by local class field theory, ε is a local norm from the completion of k_m at any prime ideals lying above $\mathfrak{q}_n$. For $\mathfrak{p}_n \in S_n$, ε is a local norm from $k_{m,\mathfrak{p}_m}$ if and only if $\varepsilon \in W_{\mathfrak{p}_n} U_{\mathfrak{p}_n}^{p^{m-n}}$ by local class field theory. By the Hasse norm principle, the assertion follows. □

Let p^{t_n} (resp. $p^{t'_n}$) be the minimum annihilator of the group $U_n/(V_n\overline{E}_n)$ (resp. $U_n/(V_n\overline{E}'_n)$). If $U_n/(V_n\overline{E}_n)$ (resp. $U_n/(V_n\overline{E}'_n)$) is not finite, we define $t_n = \infty$ (resp. $t'_n = \infty$).

Proposition 3. *For $m \geq n \geq 0$,*

$$\sharp A_m^{\Gamma_n} = \frac{\sharp A_n \cdot p^{(m-n)(s-1)}}{[E_n : E_n \cap N_{m,n}k_m^{\times}]} \leq \sharp A_n \cdot \sharp(U_n/(V_n\overline{E}_n)),$$
$$\sharp {A'_m}^{\Gamma_n} = \frac{\sharp A'_n \cdot p^{(m-n)(s-1)}}{[E'_n : E'_n \cap N_{m,n}k_m^{\times}]} \leq \sharp A'_n \cdot \sharp(U_n/(V_n\overline{E}'_n)).$$

If $\sharp(U_n/(V_n\overline{E}_n)) < \infty$ (resp. $\sharp(U_n/(V_n\overline{E}'_n)) < \infty$) and $m \geq n+t_n$ (resp. $m \geq n+t'_n$), inequality can be replaced with equality.

Proof. By Lemma 4.1 in Chapter 13 in [14], we obtain the first equality. If $U_n/(V_n\overline{E}_n)$ is not finite, the above inequality automatically holds. So assume that $U_n/(V_n\overline{E}_n)$ is finite. Since $S_n = s$, $U_n/V_n \cong \mathbf{Z}_p{}^{s-1}$. By Lemma 2, $\varepsilon \in E_n \cap N_{m,n}k_m^{\times}$ if and only if $d_n(\varepsilon^{q-1}) \in V_n U_n^{p^{m-n}}$, where q is a large power of p. So $U_n/(V_n\overline{U_n \cap d_n(E_n \cap N_{m,n}k_m^{\times})}) = U_n/(V_n U_n^{p^{m-n}}) \cong (\mathbf{Z}/p^{(m-n)}\mathbf{Z})^{s-1}$ for $m \geq n+t_n$. Since

$$E_n/(E_n \cap N_{m,n}k_m^{\times}) \to (V_n\overline{E}_n)/(V_n\overline{U_n \cap d_n(E_n \cap N_{m,n}k_m^{\times})}) \quad ([\varepsilon] \mapsto [d_n(\varepsilon)^{q-1}])$$

is an isomorphism, the first assertion follows. The other assertion can be proved in the same way. □

Theorem 1. *The following statements are equivalent.*
(1) $A'_\infty = 0$.
(2) $A'_0 \cong H^1(k_n/k, E'_n)$ *and* $U_n = V_n\overline{E}'_n$ *for some* n.

Proof. Using Lemma 1, we obtain the following commutative diagram with exact columns:

$$\begin{array}{ccccccccc}
0 & \to & H^1(k_m/k, E'_m) & \to & A'_0 & \to & {A'_m}^{\Gamma} & \to & R(k_m/k, E'_m) & \to & 0 \\
 & & \uparrow \mathrm{Inf}^1_{n,m} & & \| & & \uparrow i_{n,m} & & \uparrow \mathrm{Inf}^2_{n,m} & & \\
0 & \to & H^1(k_n/k, E'_n) & \to & A'_0 & \to & {A'_n}^{\Gamma} & \to & R(k_n/k, E'_n) & \to & 0,
\end{array}$$

where $\mathrm{Inf}^1_{n,m}$ maps $[\varepsilon_n]_n$ to $[\varepsilon_n]_m$ and $\mathrm{Inf}^2_{n,m}$ maps $[\varepsilon]_n$ to $[\varepsilon^{p^{m-n}}]_m$.

Assume (1). Then we have $i_{0,n}A'_0 = 0$ and $A'_0 \cong H^1(k_n/k, E'_n)$ for $n \gg 0$ by Proposition 2. Since $\sharp A'_n$ is bounded as $n \to \infty$, $\sharp {A'_n}^{\Gamma}$ is bounded as $n \to \infty$. This implies that $U_0/(V_0\overline{E}'_0)$ is finite and that

$$\overline{U_0 \cap d_0(E'_0 \cap N_{n,0}k_n^\times)W_0}V_0 = U_0^{p^n}V_0$$

for $n \geq t'_0$ by Lemma 2. Since $\mathrm{Inf}^2_{n,m}$ is a zero map for $m \gg n$, for all $\varepsilon \in E'_0 \cap N_{n,0}k_n^\times$ there exist some $\varepsilon_m \in E'_m$ with $\varepsilon^{p^{m-n}} = N_{m,0}\varepsilon_m$. Hence we have

$$\overline{U_0 \cap d_0(N_{m,0}E'_m)W_0}V_0 = U_0^{p^m}V_0$$

for $m \gg n$. Since $N_{m,0} : U_m/V_m \to (U_0^{p^m}V_0)/V_0$ is an isomorphism, we obtain $U_m = V_m\overline{E}'_m$.

Assume (2). Let n be an integer which satisfies $U_n = V_n\overline{E}'_n$. Since $i_{n,m} : U_n/V_n \to U_m/V_m$ is an isomorphism (cf. [19]), we have $U_m = V_m\overline{E}'_m$ for $m \geq n$. For all $\varepsilon \in E'_0 \cap N_{n,0}k_n^\times$ there exists $\varepsilon_n \in E'_n$ such that $d_0(\varepsilon(N_{n,0}\varepsilon_n)^{-1}) \in U_0^{p^m}W_0$ for any $m \geq n$. By Lemma 2, $\varepsilon(N_{n,0}\varepsilon_n)^{-1} = \varepsilon' \in E_0 \cap N_{m,0}k_m^\times$. Therefore we have

$$\mathrm{Inf}^2_{n,m}([\varepsilon]_n) = [\varepsilon]_m^{p^{m-n}} = [\varepsilon(N_{n,0}\varepsilon_n)^{-1}]_m^{p^{m-n}} = [\varepsilon']_m^{p^{m-n}}.$$

Since $U_0/(V_0\overline{E}'_0)$ is a quotient of $U_0/(V_0U_0^{p^n})$, $\sharp A_n^\Gamma$ and $\sharp R_n(k_n/k, E'_n)$ are bounded as $n \to \infty$ by Proposition 3. For $m \gg n$, $\mathrm{Inf}^2_{n,m}$ becomes a zero map and ${A'_n}^{\Gamma} \subseteq H'_n$. Therefore, (2) implies (1) by Proposition 2. □

As follows from the proof, if $U_n = V_n\overline{E}'_n$ for some n, then it holds for all $n \gg 0$.

Corollary 1. *Assume* (A) *only one prime ideal in k ramifies in K. The following statements are equivalent.*
(1) $A'_\infty = 0$.
(2) $A'_0 \cong H^1(k_n/k, E'_n)$ *for some n.*

Proof. Since $s = 1$, we have $U_n = V_n$. Therefore by Theorem 1, the assertion follows. □

3 Totally real case

3.1 Theorem

In this section, we assume (B) k is a totally real number field in which p splits completely, and Leopoldt's conjecture is valid for k and p. This conjecture is valid if and only if $\sharp A_n^{\Gamma}$ is bounded as $n \to \infty$ (cf. Proposition 3). Under the assumption (B), since $D_n \subseteq A_n^{\Gamma}$, $\sharp A_n$ is bounded as $n \to \infty$ if and only if $\sharp A'_n$ is bounded as $n \to \infty$. Moreover Leopoldt's conjecture implies that the cyclotomic $\mathbf{Z}_p$-extension k_∞ is the unique $\mathbf{Z}_p$-extension of a totally real number field k, i.e. $K = k_\infty$.

Lemma 3. *Assume* (B), *then*

$$E_0 \cap N_{n+t_0,0} k_{n+t_0}^{\times} \subseteq \pm E_0^{p^n}$$

for all $n \geq 0$.

Proof. Since p splits completely in k, V_0 is trivial. Leopoldt's conjecture implies that $U_0/(V_0\overline{E}_0) = U_0/\overline{E}_0$ is finite and that $t_0 < \infty$. For $\varepsilon \in E_0$, $\varepsilon \in N_{n+t_0,0}k_{n+t_0}^{\times}$ if and only if $d_0(\varepsilon^{p-1}) \in U_0^{p^{n+t_0}}$ (resp. $d_0(\varepsilon^2) \in U_0^{p^{n+t_0+1}}$) for odd prime p (resp. $p = 2$) by Lemma 2. Since $U_0^{p^{t_0}} \subseteq \overline{E}_0$, Leopoldt's conjecture implies that $\varepsilon \in \pm E_0^{p^n}$. □

In the following lemma, we do not assume (B).

Lemma 4. *Assume that* $K = k_\infty$ *the cyclotomic* $\mathbf{Z}_p$*-extension. For every unit* (*resp. S-unit*) $\varepsilon \in k \cap \mathbf{Q}_\infty$, *we have* $\varepsilon \in N_{n,0}E_n$ (*resp.* $\varepsilon \in N_{n,0}E'_n$).

Proof. Put $\mathbf{Q}_{n'} = k \cap \mathbf{Q}_\infty$. Then we have $k_n \cap \mathbf{Q}_\infty = \mathbf{Q}_{n'+n}$. Let us consider an exact sequence of Lemma 1 for $\mathbf{Q}_n$. By local class field theory and the Hasse norm principle, every unit in $\mathbf{Q}_n$ is a local norm and also a global norm. Since A_n for $\mathbf{Q}$ is trivial for all $n \geq 0$ (cf. [9]), every unit is a norm of some unit. □

Lemma 5. *Assume* (B), *then*

$$\mathrm{Inf}_{n,m}^2 : H^2(k_n/k, E_n) \to H^2(k_m/k, E_m)$$

is injective for $m \geq n \gg 0$.

Proof. For $\varepsilon \in E_0$, if $\varepsilon^{p^{m-n}} \in N_{m,0}E_m$, we have $\varepsilon \in E_0 \cap N_{n,0}k_n^{\times}$ by Lemma 2. Therefore it suffices to show that $\mathrm{Inf}_{n,m}^2 : R_n \to R_m$ is injective. Let $m \geq n \geq t_0$. Suppose $\varepsilon \in E_0 \cap N_{m,0}k_m^{\times}$. Then we have $\varepsilon = \pm\eta^{p^{m-t_0}}$ by Lemma 3. Here we have $\eta^{p^{n-t_0}} \in N_{n,0}k_n^{\times}$ and $-1 \in N_{m,0}E_m$ by Lemma 4. Hence $\mathrm{Inf}_{n,m}^2 : R_n \to R_m$ is surjective. By Leopoldt's conjecture, $\overline{U_0 \cap d_0(E_0 \cap N_{n,0}k_n^{\times})} = U_0^{p^n}$ and $(N_{n,0}E_n)^{p^{m-n}} \subseteq N_{m,0}E_m$ for $m \geq n \geq t_0$. Therefore we have that $\sharp R_n \geq \sharp R_m$ and that $\sharp R_n$ is constant for $n \gg 0$. This implies that $\mathrm{Inf}_{n,m}^2 : R_n \to R_m$ is injective. □

Lemma 6. *Assume* (B)*, then*

$$R(k_n/k, E'_n) \cong \mathrm{Ker}(\mathrm{Inf}^2_{n,\infty}) \oplus R(k_n/k, E_n),$$

$$\mathrm{Ker}(\mathrm{Inf}^2_{n,\infty}) \cong \langle(\varepsilon)|\varepsilon \in E'_0 \cap N_{n,0}k_n^\times\rangle/\langle(\varepsilon)|\varepsilon \in N_{n,0}E'_n\rangle$$

for $n \gg 0$.

Proof. We first show that there exist two subgroups Π_n, $\Pi'_n \subseteq E'_0 \cap N_{n,0}k_n^\times$ such that

$$R(k_n/k, E'_n) \cong (E'_0 \cap N_{n,0}k_n^\times)/N_{n,0}E'_n \cong (\Pi_n/\Pi'_n) \oplus (E_0 \cap N_{n,0}k_n^\times)/N_{n,0}E_n$$

for all $n \gg 0$. By Lemma 5, Leopoldt's conjecture for k and p implies that $\sharp D_n \leq \sharp A_n^\Gamma$ is bounded as $n \to \infty$. Since $N_{m,n} : D_m \to D_n$ is surjective, $N_{m,n}$ is an isomorphism for all $m \geq n \gg 0$. This implies that $(\Pi') = \langle(\varepsilon)|\varepsilon \in N_{n,0}E'_n\rangle \subset I_0$ is constant for all $n \gg 0$. Further we see that $(\Pi) = \langle(\varepsilon)|\varepsilon \in E'_0 \cap N_{n,0}k_n^\times\rangle \subset I_0$ is also constant for all $n \geq t_0$ by Leopoldt's conjecture and Lemma 2. Let

$$(\Pi)/(\Pi') \cong \mathbf{Z}/p^{n_1}\mathbf{Z} \oplus \mathbf{Z}/p^{n_2}\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/p^{n_{s'}}\mathbf{Z}$$

as an abelian group. Put $a = \max_{1\leq i\leq s'}\{n_i\}$ and let a_i be an element in $E'_0 \cap N_{n+a,0}k_{n+a}^\times$ such that $\{(a_i)\}$ is a basis of (Π) and that $\{(a_i^{p^{n_i}})\}$ is a basis of (Π'). Let b_i be an element in $N_{n+a,0}E'_{n+a}$ such that $(b_i) = (a_i^{p^{n_i}})$. For $n \geq t_0$, we have $b_i/a_i^{p^{n_i}} = \pm\varepsilon_i^{p^a}$ for some $\varepsilon \in E_0$ by Lemma 3. Put $a'_i = a_i\varepsilon^{p^{a-n_i}}$ and $b'_i = a_i'^{p^{n_i}} = \pm b_i$. By Lemma 2, we have $\varepsilon_i \in E_0 \cap N_{n,0}k_n^\times$ and $a'_i \in E'_0 \cap N_{n,0}k_n^\times$. By Lemma 4, $-1 \in N_{n,0}E'_n$ and $b'_i \in N_{n,0}E'_n$. Put $\Pi_n = \langle a'_i\rangle_{1\leq i\leq s'}$ and $\Pi'_n = \langle b'_i\rangle_{1\leq i\leq s'}$. Then we easily see $E'_0 \cap N_{n,0}E'_n = \Pi_n \oplus (E_0 \cap N_{n,0}E_n)$ and $N_{n,0}E'_n = \Pi'_n \oplus N_{n,0}E_n$. By Lemma 5, $\mathrm{Inf}^2_{n,m} : R(k_n/k, E_n) \to R(k_m/k, E_m)$ is an isomorphism for $m \geq n \gg 0$. Therefore we have

$$\Pi_n/\Pi'_n \cong \mathrm{Ker}(\mathrm{Inf}^2_{n,m} : R(k_n/k, E'_n) \to R(k_n/k, E'_m))$$

$$= \mathrm{Ker}(\mathrm{Inf}^2_{n,m} : H^2(k_n/k, E'_n) \to H^2(k_n/k, E'_m))$$

for $m \geq n + a$. □

Theorem 2. *Assume* (B)*. The following statements are equivalent.*

(1) $A'_\infty = 0$.

(2) $A'_0 \cong H^1(k_n/k, E'_n)$ *for some* n *and*
$\mathrm{rk}_p R(k_m/k, E'_m) = \mathrm{rk}_p(R(k_m/k, E'_m)/j_m(R(k_m/k, E_m)))$ *for all* $m \gg 0$.

Proof. Take m and n such that they satisfy the assertion in Lemma 6. Using Lemma 1 and Lemma 6, we obtain the following commutative diagram with exact columns:

$$\begin{array}{ccccccccc}
0 & \to & H^1(k_m/k, E'_m) & \to & A'_0 & \to & {A'_m}^{\Gamma} & \to & \mathrm{Ker}(\mathrm{Inf}^2_{m,\infty}) \oplus R_m & \to & 0 \\
 & & \uparrow \mathrm{Inf}^1_{n,m} & & \| & & \uparrow i_{n,m} & & \uparrow \mathrm{Inf}^2_{n,m} & & \\
0 & \to & H^1(k_n/k, E'_n) & \to & A'_0 & \to & {A'_n}^{\Gamma} & \to & \mathrm{Ker}(\mathrm{Inf}^2_{n,\infty}) \oplus R_n & \to & 0,
\end{array}$$

where $R_n = R(k_n/k, E_n)$.

Assume (1). By Proposition 2, it follows $A'_0 \cong H^1(k_n/k, E'_n)$ for some n. A map $i_{m,\infty} : {A'_m}^{\Gamma} \to {A'_\infty}^{\Gamma}$ is a zero map if and only if $R(k_m/k, E_m)$ is trivial for $m \gg 0$. Therefore $\mathrm{rk}_p R(k_m/k, E'_m) = \mathrm{rk}_p(R(k_m/k, E'_m)/j_m(R(k_m/k, E_m)))$ follows.

Assume (2). By Lemma 6, $R(k_m/k, E_m)$ is trivial for $m \gg 0$. By the above diagram, $i_{m,\infty} : {A'_m}^{\Gamma} \to {A'_\infty}^{\Gamma}$ is a zero map for $m \gg 0$. By Proposition 2, the assertion follows. □

By [5, Theorem 2], $A_\infty = 0$ if and only if A_n^Γ/D_n for $n \gg 0$. By the following proposition and Theorem 2, we can show this assertion.

Proposition 4. *Assume* (B) *and that* $i_{0,n}(A'_0)$ *is trivial. For* $n \gg 0$*,*

$$\mathrm{Ker}(H^0(k_n/k, A'_n) \to H^1(k_n/k, D_n)) \cong A_n^\Gamma/D_n \cong R(k_n/k, E_n),$$

$${A'_n}^{\Gamma}/(A_n^\Gamma/D_n) \cong R(k_n/k, E'_n)/j_n(R(k_n/k, E_n)).$$

Proof. From a short exact sequence $0 \to D_n \to A_n \to A'_n \to 0$, we have

$$A_n^\Gamma/D_n \cong \mathrm{Ker}(H^0(k_n/k, A'_n) \to H^1(k_n/k, D_n)).$$

By Lemma 1, we obtain the following exact sequence:

$$0 \;\to\; {A_n}^{\Gamma}/(D_n i_{0,n}(A_0)) \;\to\; R(k_n/k, E_n) \;\to\; 0.$$

Hence by Lemma 6, the assertions immediately follow. □

3.2 Examples

Let k be a real quadratic field in which p splits. In this case, Leopoldt's conjecture immediately follows for all k and p. If $A'_n = A_n/D_n$ is trivial for all $n \geq 0$, $\sharp A_n = \sharp D_n \leq \sharp A_n^\Gamma$ is bounded as $n \to \infty$ by Proposition 3.

Theorem 3. *Let k be a real quadratic field in which p splits. Suppose that A'_n is not trivial for some $n \geq 0$. Then the following statements are equivalent.*
(1) $A'_\infty = 0$.
(2) (a) $A'_0 \cong H^1(k_n/k, E'_n)$ *for some* n,
(b) $R(k_m/k, E'_m)$ *is cyclic as an abelian group for all* $m \gg 0$,
(c) $R(k_m/k, E'_m)/j_m(R(k_m/k, E_m))$ *is not trivial for all* $m \gg 0$.

Proof. Let (Π) and (Π') be the same groups as in the proof of Lemma 6. By Lemma 4, p is contained in $N_{n,0}E'_n$ for all n. Hence $(\Pi)/(\Pi')$ is a cyclic group. Since Γ and A_n are p-groups, A_n is trivial if and only if A_n^Γ is trivial. For $m \gg 0$, we have $(\Pi)/(\Pi') \cong R(k_m/k, E'_m)/j_m(R(k_m/k, E_m))$. Therefore the assertion follows by Theorem 2. □

By Proposition 4, (2) is equivalent to the following statements.
(a) $A'_0 \cong H^1(k_n/k, E'_n)$ for some n,
(b) ${A'_m}^\Gamma$ is cyclic as an abelian group for all $m \gg 0$,
(c) ${A'_m}^\Gamma/(A_m^\Gamma/D_m)$ is not trivial for all $m \gg 0$.
We will give examples of k to which we can apply Theorem 3.

Example 1. Let $k = \mathbf{Q}(\sqrt{2659})$ and $p = 3$. The conjecture was verified for this case in [4]. Following [2], Fukuda and Taya defined invariants $n_0^{(n)}$ and $n_2^{(n)}$ for real quadratic fields k and odd prime numbers p which can be written as follows:

$$p^{n_0^{(n)}} = p^{n+1}\sharp(U_n/V_n\overline{E}'_n), \qquad p^{n_2^{(n)}} = p^{n+1}\sharp(U_n/V_n\overline{E}_n).$$

From the table of [4], $n_0 = n_0^{(0)} = 2$, $n_2 = n_2^{(0)} = 3$, $n_0^{(1)} = 2$, $n_2^{(1)} = 4$, $\sharp D_0 = p$, $\sharp A_0 = p$, $\sharp D_1 = p$, $\sharp A_1 = p^2$. Hence we have $\sharp A'_0 = 1$, $\sharp(U_0/V_0\overline{E}'_0) = p$ and $\sharp(U_1/V_1\overline{E}'_1) = 1$. By Theorem 1, we can verify the conjecture for k and p.

By the method in [7], we can verify the conjecture for this field and $p = 3$, using cyclotomic units in k_2.

Example 2. Let $k = \mathbf{Q}(\sqrt{12007})$ and $p = 3$. From the table of [3], $n_0 = 3$, $n_2 = 3$, $n_0^{(1)} = 3$, $n_2^{(1)} = 4$, $\sharp D_0 = p$, $\sharp A_0 = p$, $\sharp D_1 = p$, $\sharp A_1 = p^2$. Hence we have $\sharp A'_0 = 1$, $\sharp(U_0/V_0\overline{E}'_0) = p^2$ and $\sharp(U_1/V_1\overline{E}'_1) = p$. We cannot verify the conjecture for k and p in the same way.

However, by our criterion, we can verify the conjecture for this case in the following way. First we show that A'_n is cyclic as an abelian group for all n. Let ψ be the non-trivial Dirichlet character associated to k and $f_\psi(T)$ the Iwasawa polynomial associated to p-adic L-function $L_p(s,\psi)$ (see [10]). Then we see that $f_\psi(T)$ is reducible of degree 2 in $\mathbf{Z}_p[T]$ by computation. By the Iwasawa main conjecture proved in [16], $\mathrm{Gal}(M/k_\infty)$ is isomorphic to

$\mathbf{Z}_p \oplus \mathbf{Z}_p$ as an abelian group, where M is the maximal abelian p-extension of k unramified outside p (cf. [19]). Moreover, since $A_0 = D_0 \cong \mathbf{Z}/p\mathbf{Z}$ and A'_n is a quotient of $\mathrm{Gal}(M/k_\infty)$, A'_n is cyclic as an abelian group. Further, since ${A'_n}^{\Gamma_1} \supseteq A_n^{\Gamma_1}/D_n$, $\sharp D_n \geq \sharp A_n^{\Gamma_1}/\sharp {A'_n}^{\Gamma_1} = p^4/p^2 = p^2$ for $n \gg 1$ by Proposition 3. Hence we have $\sharp {A'_n}^{\Gamma} = p^2 \geq \sharp(A_n^{\Gamma}/D_n) \geq p^3/p^2 = p$ for $n \gg 1$. Therefore (a), (b) and (c) hold for k and p.

By the method in [7], we can verify the conjecture for this field and $p = 3$, using cyclotomic units in k_3.

Acknowledgements
Section 3.1 of this paper was done in the author's master thesis [18]. He wishes to express his deep gratitude to Professor K. Iwasawa, from whose question the author started this work. He also wishes to express his gratitude to Professor H. Ichimura for valuable advice.

References

[1] S. U. Chase, D. K. Harrison, and A. Rosenberg, *Galois theory and cohomology of commutative rings*, Mem. Amer. Math. Soc. **52** (1965), 15–33.

[2] T. Fukuda and K. Komatsu, *On $\mathbf{Z}_p$-extensions of real quadratic fields*, J. Math.Soc.Japan **38** (1986), 95–102.

[3] T. Fukuda and H. Taya, *Computational research on Greenberg's conjecture for real quadratic fields*, Memoirs of the School of Sciences & Engineering Waseda Univ. **58** (1994), 175–203.

[4] ———, *The Iwasawa λ-invariants of $\mathbf{Z}_p$-extensions of real quadratic fields*, Acta Arith. **69** (1995), 277–292.

[5] R. Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. **98** (1976), 263–284.

[6] H. Ichimura, *On the ideal class group of the cyclotomic $\mathbf{Z}_p$-extension of a totally real number field*, preprint (1999).

[7] H. Ichimura and H. Sumida, *On the Iwasawa invariants of certain real abelian fields II*, Internat. J. Math. **7** (1996), 721–744.

[8] ———, *On the Iwasawa invariants of certain real abelian fields*, Tôhoku Math. J. **49** (1997), 203–215.

[9] K. Iwasawa, *A note on class numbers of algebraic number fields*, Abh. Math. Sem. Univ. Hamburg **20** (1956), 257–258.

[10] ———, *Lectures on p-adic L-functions*, Ann. of Math. Stud., vol. 74, Princeton Univ. Press: Princeton, N.J., 1972.

[11] ———, *On* $\mathbf{Z}_l$*-extensions of algebraic number fields*, Ann. of Math. **98** (1973), 246–326.

[12] ———, *On cohomology groups of units for* $\mathbf{Z}_p$*-extensions*, Amer. J. Math. **105** (1983), 189–200.

[13] J. S. Kraft and R. Schoof, *Computing Iwasawa modules of real quadratic number fields*, Compositio Math. **97** (1995), 135–155.

[14] S. Lang, *Cyclotomic fields I and II*, Graduate Texts in Math., vol. 121, Springer-Verlag: New York, 1990.

[15] A. Lannuzel and T. Nguyen Quang Do, *Conjectures de Greenberg et extensions pro-p-libres d'un corps de nombres*, preprint (1999).

[16] B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbf{Q}$, Invent. Math. **76** (1984), 179–330.

[17] J. Minardi, *Iwasawa modules for* $\mathbf{Z}_p^d$*-extensions of algebraic number fields*, Thesis, University of Washington (1986).

[18] H. Sumida, *On Greenberg's conjecture concerning and the Iwasawa polynomial*, Master thesis, University of Tokyo (1993), (in Japanese).

[19] ———, *Greenberg's conjecture and the Iwasawa polynomial*, J. Math. Soc. Japan **49** (1997), 689–711.

[20] H. Taya, *On the Iwasawa* λ*-invariants of real quadratic fields*, Tokyo J. Math. **16** (1993), 121–130.

Hiroki SUMIDA
Faculty of Integrated Arts and Sciences
Hiroshima University
Kagamiyama
Higashi-Hiroshima 739-8521, Japan
sumida@mis.hiroshima-u.ac.jp