

## RELATIONS OF IDEALS OF CERTAIN REAL ABELIAN FIELDS

JAE MOON KIM

ABSTRACT. Let  $k$  be a real abelian field and  $k_\infty$  be its  $\mathbb{Z}_p$ -extension for an odd prime  $p$ . Let  $A_n$  be the Sylow  $p$ -subgroup of the ideal class group of  $k_n$ , the  $n$ th layer of the  $\mathbb{Z}_p$ -extension. By using the main conjecture of Iwasawa theory, we have the following: If  $p$  does not divide  $\prod_{\chi \in \widehat{\Delta}_k, \chi \neq 1} B_{1, \chi \omega^{-1}}$ , then  $A_n = \{0\}$  for all  $n \geq 0$ , where  $\Delta_k = \text{Gal}(k/\mathbb{Q})$  and  $\omega$  is the Teichmüller character for  $p$ .

The converse of this statement does not hold in general. However, we have the following when  $k$  is of prime conductor  $q$ : Let  $q$  be an odd prime different from  $p$  and let  $k$  be a real subfield of  $\mathbb{Q}(\zeta_q)$ . If  $p \mid \prod_{\chi \in \widehat{\Delta}_{k,p}, \chi \neq 1} B_{1, \chi \omega^{-1}}$ , then  $A_n \neq \{0\}$  for all  $n \geq 1$ , where  $\Delta_{k,p}$  is the Galois group  $\text{Gal}(k_{(p)}/\mathbb{Q})$  and  $k_{(p)}$  is the decomposition field of  $k$  for  $p$ .

### 0. Introduction.

Let  $k$  be a number field and  $k_\infty = \bigcup_{n \geq 0} k_n$  be a  $\mathbb{Z}_p$ -extension of  $k$  for a prime  $p$ . Let  $A_n$  be the Sylow  $p$ -subgroup of the ideal class group of  $k_n$  and  $A_\infty = \varprojlim A_n$  be the inverse limit of  $A_n$  under the norm maps. During the past few decades, the growth of  $\#A_n$  and the structure of  $A_\infty$  have been studied exhaustively after K.Iwasawa. Let  $e_n$  be the exact power of  $p$  of  $\#A_n$ . K.Iwasawa([3]) found that there are integers  $\mu$ ,  $\lambda \geq 0$  and  $\nu$  such that  $e_n = \mu p^n + \lambda n + \nu$  for  $n \gg 0$ . These constants  $\mu$ ,  $\lambda$  and  $\nu$  are called the Iwasawa invariants for  $k_\infty/k$ . Later in 1979, B.Ferrero and L.Washington proved that  $\mu = 0$  when  $k$  is an abelian field and  $k_\infty$  is the cyclotomic  $\mathbb{Z}_p$ -extension of  $k$ ([1]). Around

---

Received June 5, 1998.

1991 Mathematics Subject Classification: primary:11R23, secondary:11R29.

Key words and phrases: main conjecture, Iwasawa invariants, circular units .

This paper was supported by research fund of Inha University, 1997.

at the same time, R.Greenberg conjectured  $\lambda = 0$  when  $k$  is a totally real field and gave a number of examples supporting his conjecture in ([2]).

Note that when  $k$  is a real abelian field,  $k$  admits only one  $\mathbb{Z}_p$ -extension for each  $p$ , namely the cyclotomic  $\mathbb{Z}_p$ -extension since the Leopoldt's conjecture holds in this case([10]). Thus when  $k$  is a real abelian field, according to Iwasawa-Ferrero-Washington,  $e_n = \lambda n + \nu$  for  $n \gg 0$ . And if the Greenberg conjecture holds, then  $e_n = \nu$  is independent of  $n$  for  $n \gg 0$  and  $A_n$  capitulates in  $k_\infty$ . The aim of this paper is to discuss conditions for  $A_n = \{0\}$ , i.e.,  $\lambda = \nu = 0$  when  $k$  is real abelian. In the following theorem a sufficient condition for  $\lambda = \nu = 0$  is given in terms of Bernoulli numbers.

**THEOREM 1.** *Let  $k$  be a real abelian field and let  $\Delta_k = Gal(k/\mathbb{Q})$ . If  $p$  does not divide  $\prod_{\chi \in \widehat{\Delta}_k, \chi \neq 1} B_{1, \chi \omega^{-1}}$ , then  $A_n = \{0\}$  for all  $n \geq 0$ , where  $\omega$  is the Teichmüller character for  $p$ .*

We will briefly sketch the proof of Theorem 1 in Section 1 by using the main conjecture of Iwasawa theory which was first proved by B.Mazur and A.Wiles([8]). The rest of this paper is devoted to a discussion of the converse of Theorem 1. Namely, we will examine what happens if  $p$  divides  $\prod B_{1, \chi \omega^{-1}}$ . When  $k = \mathbb{Q}(\sqrt{85})$  and  $p = 3$ ,  $B_{1, \chi \omega^{-1}} = -12$  but the class number of  $k$  is 2, so  $A_0 = \{0\}$ . Thus the converse of Theorem 1 is not true in general. However, in [5], the following is proved when  $[k : \mathbb{Q}] = 2$  and  $p$  splits in  $k$ : Let  $k$  be a real quadratic field and  $p$  be an odd prime which splits in  $k$ . If  $p$  divides  $B_{1, \chi \omega^{-1}}$ , then  $A_n \neq \{0\}$  for  $n \geq 1$ .

In this paper, we will generalize this to an arbitrary real abelian field of prime conductor  $q$ . The main tools for the generalization are certain relations of prime ideals of  $k_n$  above  $p$  coming from circular units of  $k_n$ . In Section 2, we will briefly review circular units of abelian fields defined by W.Sinnott([9]) and find relations of prime ideals of  $k_n$  above  $p$ . Finally, in Section 3, we will prove the following theorem :

**THEOREM 3.** *Let  $q$  be an odd prime and let  $k$  be a real sub-field of  $\mathbb{Q}(\zeta_q)$ . Let  $p$  be an odd prime such that  $p \nmid [k : \mathbb{Q}]$ . If  $p \mid \prod_{\chi \in \widehat{\Delta}_{k,p}, \chi \neq 1} B_{1, \chi \omega^{-1}}$ , then  $A_n \neq \{0\}$  for all  $n \geq 1$ .*

**1. Proof of theorem 1**

**THEOREM 1.** *If  $p$  does not divide  $\prod_{\chi \in \widehat{\Delta}_k, \chi \neq 1} B_{1, \chi \omega^{-1}}$ , then  $A_n = \{0\}$  for all  $n \geq 0$ .*

*Proof.* Let  $L_\infty$  and  $M_\infty$  be the maximal unramified and  $p$ -ramified abelian  $p$ -extensions of  $k_\infty$  respectively. Let  $Y = Gal(M_\infty/k_\infty)$ , and let  $Y_1 = \bigoplus_{\chi \neq 1} Y(\chi)$  be the direct sum of the  $\chi$ -components  $Y(\chi)$  of  $Y$  for each nontrivial  $\chi \in \widehat{\Delta}_k$ . Then by the main conjecture,  $Y(\chi)$  is pseudo-isomorphic to  $\Lambda/(f_\chi)$ , where  $\Lambda = \mathbb{Z}_p[[T]]$  and  $f_\chi$  is the power series in  $\Lambda$  giving rise to the  $p$ -adic  $L$ -function. Note that

$$f_\chi(0) = L_p(0, \chi) = -B_{1, \chi \omega^{-1}}.$$

Let  $f = \prod_{\chi \in \widehat{\Delta}_k, \chi \neq 1} f_\chi$ . Then  $Y_1 = \bigoplus_{\chi \neq 1} Y(\chi)$  is pseudo-isomorphic to  $\Lambda/(f)$  and

$$f(0) = \prod_{\chi} f_\chi(0) = \pm \prod_{\chi} B_{1, \chi \omega^{-1}}.$$

Since  $p \nmid \prod_{\chi} B_{1, \chi \omega^{-1}}$  by assumption,  $p \nmid f(0)$ . Therefore  $f$  is a unit in  $\Lambda$ . Hence  $Y_1$  is pseudo-isomorphic to  $\Lambda/(f) = \{0\}$ , i.e., there is a  $\Lambda$ -module homomorphism  $Y_1 \rightarrow 0$  with a finite kernel. But since each  $Y(\chi)$  does not have a finite  $\Lambda$ -submodule (see the appendix of [7]),  $Y_1 = \{0\}$ . Therefore  $Gal(L_\infty/k_\infty)$ , a quotient of  $Y_1$ , is also trivial. Since  $Gal(L_\infty/k_\infty) \simeq \varprojlim A_n$  and since  $A_m \rightarrow A_n$  is surjective for  $m > n$  by class field theory,  $A_n$  is trivial for all  $n \geq 0$ .  $\square$

**2. Relations of prime ideals above  $p$**

Let  $P_n$  be the multiplicative subgroup of  $\mathbb{Q}(\zeta_n)^\times$  generated by  $\{\pm 1\}$  and  $\{1 - \zeta_n^a \mid 0 < a < n\}$ . Then the group  $C_{\mathbb{Q}(\zeta_n)}$  of cyclotomic units of  $\mathbb{Q}(\zeta_n)$  is defined to be

$$C_{\mathbb{Q}(\zeta_n)} = E_{\mathbb{Q}(\zeta_n)} \cap P_n,$$

where  $E_{\mathbb{Q}(\zeta_n)}$  is the unit group of  $\mathbb{Q}(\zeta_n)$ . In general, for an abelian field  $F$ , W.Sinnott defines the group of circular units of  $F$  as follows([9]). For each  $n > 2$ , let

$$F_n = F \cap \mathbb{Q}(\zeta_n) \text{ and } C_{F_n} = N_{\mathbb{Q}(\zeta_n)/F_n}(C_{\mathbb{Q}(\zeta_n)}).$$

Then the group  $C_F$  of circular units of  $F$  is defined to be the multiplicative subgroup of  $F^\times$  generated by  $C_{F_n}$  together with  $-1$ . Note that if  $n$  is prime to the conductor of  $F$ , then  $F_n = \mathbb{Q}$  and so  $C_{F_n} = \{1\}$ . Thus there are only finitely many  $n$ 's to be considered in the definition of  $C_F$ .

Let  $k$  be a real subfield of  $\mathbb{Q}(\zeta_q)$  for an odd prime  $q$  and let  $k_\infty = \bigcup_{n \geq 0} k_n$  be the  $\mathbb{Z}_p$ -extension of  $k = k_0$  for an odd prime  $p$  with  $(p, q) = 1$ . Here,  $k_n$  means the  $n$ th layer of the  $\mathbb{Z}_p$ -extension, not  $k \cap \mathbb{Q}(\zeta_n)$ . For each  $n \geq 0$ , we denote the group of circular units of  $k_n$  by  $C_n$ . Then the index theorem of W.Sinnott says the following ([9]):

INDEX THEOREM. *Let  $E_n$  be the unit group of  $k_n$  and  $h_n$  be the class number of  $k_n$ . Then  $[E_n : C_n] = 2^{c_n} h_n$  for some integer  $c_n$ .*

For each integer  $s \geq 1$ , we choose a primitive  $s$ th root  $\zeta_s$  of 1 so that  $\zeta_t^{\frac{t}{s}} = \zeta_s$  if  $s|t$ . Let  $K = \mathbb{Q}(\zeta_q)$ ,  $F = \mathbb{Q}(\zeta_p)$  and  $K' = \mathbb{Q}(\zeta_{pq})$ . We denote their cyclotomic  $\mathbb{Z}_p$ -extensions by  $K_\infty$ ,  $F_\infty$ , and  $K'_\infty$ . Let  $\sigma$  be the topological generator of the Galois group  $\Gamma = Gal(K'_\infty/K')$  which maps  $\zeta_{p^n}$  to  $\zeta_{p^n}^{1+p}$  for all  $n \geq 1$ . Restrictions of  $\sigma$  to various subfields are also denoted by  $\sigma$ . Let  $k_{(p)}$  be the decomposition subfield of  $k$  for  $p$  and let  $\Delta = Gal(K/k)$ ,  $\bar{\Delta} = Gal(K/\mathbb{Q})$ ,  $\Delta_p = Gal(K/k_{(p)})$ ,  $\Delta_k = Gal(k/\mathbb{Q})$  and  $\Delta_{k,p} = Gal(k_{(p)}/\mathbb{Q})$ . Let  $[k : \mathbb{Q}] = d$  and  $[k_{(p)} : \mathbb{Q}] = l$ , so there are  $l$  prime ideals in  $k$  above  $p$ . Elements of  $\Delta$ ,  $\bar{\Delta}$  or  $\Delta_p$  will be denoted by  $\tau$ 's and those of  $\Delta_k$  and  $\Delta_{k,p}$  by  $\rho$ 's. The Frobenius automorphism of  $K$  for  $p$  or its restriction to  $k$  is denoted by  $\tau_p$ . Let  $R$  be the set of all roots of 1 in  $\mathbb{Z}_p$ , i.e.,  $R = \{\omega \in \mathbb{Z}_p | \omega^{p-1} = 1\}$ . Then  $R$  can be regarded as the Galois group  $Gal(F/\mathbb{Q})$  or any Galois group isomorphic to it such as  $Gal(F_n/\mathbb{Q}_n)$ , where  $\mathbb{Q}_n$  is the subfield of  $F_n$  of degree  $p^n$  over  $\mathbb{Q}$ . For  $m > n$ , let  $G_{m,n}$  be the Galois group  $Gal(K'_m/K'_n)$  and  $N_{m,n}$  be the norm map  $N_{K'_m/K'_n}$  from  $K'_m$  to  $K'_n$ . We will abbreviate  $G_{m,0}$  and  $N_{m,0}$  by  $G_m$  and  $N_m$  respectively.  $G_{m,n}$  will also mean the Galois groups  $Gal(k_m/k_n)$ ,  $Gal(F_m/F_n)$  and  $Gal(\mathbb{Q}_m/\mathbb{Q}_n)$ . Similarly  $N_{m,n}$  will have various meanings. Finally we fix a generator  $\psi_n$  of the character group of  $Gal(\mathbb{Q}_n/\mathbb{Q})$  such that  $\psi_n(\sigma) = \zeta_{p^n}$ . Then we have the following cohomology groups of circular units([6]).

THEOREM. *Suppose  $p \nmid d = [k : \mathbb{Q}]$ . Then, for  $m > n \geq 0$ , we have*

the followings.

- (1)  $C_m^{G_{m,n}} = C_n,$
- (2)  $\widehat{H}^0(G_{m,n}, C_m) \simeq (\mathbb{Z}/p^{m-n}\mathbb{Z})^{l-1},$
- (3)  $\widehat{H}^{-1}(G_{m,n}, C_m) \simeq (\mathbb{Z}/p^{m-n}\mathbb{Z})^l.$

Fix a prime ideal  $\wp_0$  of  $k_{(p)}$  above  $p$ . We will also think of  $\wp_0$  as a prime ideal of  $k = k_0$ . Let  $\Delta_{k,p} = \{\rho_1, \dots, \rho_{l-1}, \rho_l = id\}$ . We denote the unique prime ideal of  $k_n$  (or of  $k_{(p)}\mathbb{Q}_n$ ) above  $\wp_0$  by  $\wp_n$ . Then  $\{\wp_n^{\rho_i} \mid 1 \leq i \leq l\}$  is the set of prime ideals of  $k_n$  above  $p$ .

Let  $C_\infty = \bigcup_{n \geq 0} C_n$  and  $E'_\infty = \bigcup_{n \geq 0} E'_n$ , where  $E'_n$  is the group of  $p$ -units of  $k_n$ . We know that  $H^1(\Gamma, C_\infty) \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^l$  by above theorem, where  $\Gamma = Gal(k_\infty/k)$ . On the other hand,  $H^1(\Gamma, E'_\infty)$  is a finite group([4]). Since  $\mathbb{Q}_p/\mathbb{Z}_p$  cannot have a nontrivial finite quotient, the induced homomorphism  $H^1(\Gamma, C_\infty) \rightarrow H^1(\Gamma, E'_\infty)$  is a zero map. Therefore  $H^1(G_n, C_n) \rightarrow H^1(G_n, E'_n)$  is also a zero map for every  $n \geq 1$  by the injectivity of the inflation maps on  $H^1$ .

Let

$$\delta = \prod_{\substack{\omega \in R \\ \tau \in \Delta_p}} (\zeta_{p^2}^\omega - \zeta_q^\tau) \text{ and } \delta_i = \delta^{\rho_i} = \prod_{\substack{\omega \in R \\ \tau \in \Delta_p}} (\zeta_{p^2}^\omega - \zeta_q^{\tau \rho_i}).$$

As was shown in [6],  $N_1(\delta) = N_1(\delta_i) = 1$  and  $\{\delta_1, \dots, \delta_{l-1}, \pi_1^{\sigma-1}\}$  generates  $H^1(G_1, C_1)$ , where  $\pi_1 = \prod_{\omega \in R} (\zeta_{p^2}^\omega - 1)$ . Therefore, by the injectivity of  $H^1(G_1, C_1) \rightarrow H^1(G_1, E'_1)$ , we have

$$\delta = \alpha^{\sigma-1} \text{ and } \delta_i = \delta^{\rho_i} = \alpha_i^{\sigma-1}$$

for some  $p$ -units  $\alpha$  in  $k_1$  and  $\alpha_i = \alpha^{\rho_i}$ . That is, as an ideal,

$$(\alpha) = \wp_1^{\sum_{1 \leq i \leq l} g(\rho_i) \rho_i^{-1}}$$

for some integers  $g(\rho_i)$ . Note that these integers are determined uniquely modulo  $p$  by  $\delta$  since  $\wp_0$  ramifies totally in  $k_1$ . Then for each  $k$ ,  $1 \leq k \leq l-1$ ,  $(\alpha_k)$  is factorized as

$$(\alpha_k) = (\alpha)^{\rho_k} = \wp_0^{\sum_{1 \leq i \leq l} g(\rho_i) \rho_i^{-1} \rho_k} = \wp_1^{\sum_{1 \leq j \leq l} g(\rho_j^{-1} \rho_k) \rho_j}.$$

THEOREM 2. Let  $\delta = \alpha^{\sigma-1}$  and  $(\alpha) = \wp_1^{\sum_{1 \leq i \leq l} g(\rho_i)\rho_i^{-1}}$  as above. Let  $\chi$  be a nontrivial character of  $\Delta_{k,p}$  and  $\tau(\chi) = \sum_{1 \leq a < q} \chi(a)\zeta_q^a$  be the Gauss sum for  $\chi$ . Then

$$\sum_{1 \leq i \leq l} \chi(\rho_i)g(\rho_i) \equiv -\frac{q}{\tau(\chi)} B_{1, \chi\omega^{-1}} \pmod{(\zeta_{p^2} - 1)}.$$

*Proof.* For each  $i$ , we read the equation  $\delta_i = \alpha_i^{\sigma-1}$  in  $k_{1, \wp_1}$ , the completion of  $k_1$  at  $\wp_1$ . Since

$$(\alpha_i) = \wp_1^{\sum_{1 \leq j \leq l} g(\rho_j^{-1}\rho_i)\rho_j},$$

$\alpha_i = \pi_1^{g(\rho_i)} u$  for some unit  $u$  in  $k_{1, \wp_1}$ . Thus, in  $\mathbb{Q}_p(\zeta_{p^2})$ ,

$$\alpha_i = \pi^{(p-1)g(\rho_i)} \eta$$

for some unit  $\eta$  in  $\mathbb{Q}_p(\zeta_{p^2})$ , where  $\pi = \zeta_{p^2} - 1$ . Hence

$$\delta_i = \alpha_i^{\sigma-1} = \pi^{(p-1)g(\rho_i)(\sigma-1)} \eta^{\sigma-1}.$$

Since

$$\pi^{\sigma-1} \equiv 1 + \pi^{p-1} \text{ and } \eta^{\sigma-1} \equiv 1 \pmod{\pi^p},$$

we have

$$\delta_i \equiv 1 + (p-1)g(\rho_i)\pi^{p-1} \equiv 1 - g(\rho_i)\pi^{p-1} \pmod{\pi^p}.$$

Therefore

$$\begin{aligned} \log_p \delta_i &\equiv \log_p(1 - g(\rho_i)\pi^{p-1}) \\ &\equiv -g(\rho_i)\pi^{p-1} - \frac{1}{2}(g(\rho_i)\pi^{p-1})^2 - \dots - \frac{1}{p}(g(\rho_i)\pi^{p-1})^p - \dots \\ &\equiv g(\rho_i) \pmod{\pi}, \end{aligned}$$

since  $\pi^{p(p-1)}/p \equiv -1 \pmod{\pi}$  and every other term is congruent to 0 mod  $\pi$ . Hence

$$\begin{aligned} \sum_{1 \leq i \leq l} \chi(\rho_i)g(\rho_i) &\equiv \sum_{1 \leq i \leq l} \chi(\rho_i)\log_p \delta_i \\ &= \sum_{1 \leq i \leq l} \chi(\rho_i)\log_p \left( \prod_{\substack{\omega \in R \\ \tau \in \Delta_p}} (\zeta_{p^2}^\omega - \zeta_q^{\tau \rho_i}) \right) \\ &= \sum_{\substack{\omega \in R \\ \tau \in \Delta_p, 1 \leq i \leq l}} \chi(\rho_i)\log_p (\zeta_{p^2}^\omega - \zeta_q^{\tau \rho_i}) \\ &= \sum_{\substack{\omega \in R \\ \tau \in \Delta}} \chi(\tau)\log_p (\zeta_{p^2}^\omega - \zeta_q^\tau) \\ &\equiv -\frac{q}{\tau(\chi)} B_{1, \chi \omega^{-1}} \pmod{\pi}. \end{aligned}$$

The last congruence comes from a slight modification of Proposition 1 of [5]. □

### 3. Application to the proof of theorem 3

Let  $A$  be the  $l \times l$  matrix with  $i$ th column

$$A^i = (g(\rho_1^{-1} \rho_i), \dots, g(\rho_l^{-1} \rho_i))^t$$

for  $1 \leq i \leq l - 1$  and the last column  $A^l = (1, \dots, 1)^t$ . It is not hard to see that (for instance, apply lemma 5.26 of [10])

$$\det A = \prod_{\substack{\chi \in \widehat{\Delta}_{k,p} \\ \chi \neq 1}} \sum_{1 \leq i \leq l} \chi(\rho_i)g(\rho_i).$$

Then we have

$$\det A \equiv \pm q^{\frac{l-1}{2}} \prod_{\substack{\chi \in \widehat{\Delta}_{k,p} \\ \chi \neq 1}} B_{1, \chi \omega^{-1}} \pmod{p\mathbb{Z}_p}$$

by Theorem 2, since  $\prod_{\tau} \tau(\chi) = q^{(l-1)/2}$ . Now we prove Theorem 3.

**THEOREM 3.** *Let  $q$  be an odd prime and let  $k$  be a real subfield of  $\mathbb{Q}(\zeta_q)$ . Let  $p$  be an odd prime such that  $p \nmid [k : \mathbb{Q}]$ . If  $p \mid \prod_{\chi \in \widehat{\Delta}_{k,p}, \chi \neq 1} B_{1,\chi\omega^{-1}}$ , then  $A_n \neq \{0\}$  for all  $n \geq 1$ .*

*Proof.* Suppose that  $p \mid \prod_{\chi(p)=1, \chi \neq 1} B_{1,\chi\omega^{-1}}$ . Then  $\det A \equiv 0 \pmod p$ . So there is a nontrivial vector  $B = (b_1, \dots, b_l)^t$  such that  $AB \equiv \mathbb{O} \pmod p$ . Consider  $\xi = \delta_1^{b_1} \cdots \delta_{l-1}^{b_{l-1}} \pi_1^{(\sigma^{-1})b_l}$ . Then

$$\xi = (\alpha_1^{b_1} \cdots \alpha_{l-1}^{b_{l-1}} \pi_1^{b_l})^{\sigma^{-1}}.$$

Since

$$(\alpha_i) = \wp_1^{\sum_{1 \leq j \leq l} g(\rho_j^{-1} \rho_i) \rho_j} \text{ and } (\pi_1) = \wp_1^{\sum_{1 \leq j \leq l} \rho_j},$$

we have

$$(\alpha_1^{b_1} \cdots \alpha_{l-1}^{b_{l-1}} \pi_1^{b_l}) = \wp_1^{\sum_{1 \leq j \leq l} (\sum_{1 \leq i \leq l-1} g(\rho_j^{-1} \rho_i) b_i + b_l) \rho_j}.$$

Note that  $\sum_{1 \leq i \leq l-1} g(\rho_j^{-1} \rho_i) b_i + b_l$  is the  $j$ th entry of  $AB$ , which is congruent to  $0 \pmod p$ . Hence

$$(\alpha_1^{b_1} \cdots \alpha_{l-1}^{b_{l-1}} \pi_1^{b_l}) = \wp_1^{p \sum_{1 \leq j \leq l} c_j \rho_j} = I_0$$

for some ideal  $I_0$  of  $k_0$ . To finish the proof, we will show that  $p$  divides the class number  $h_1$  of  $k_1$ , which clearly implies that  $A_n \neq 0$  for  $n \geq 1$  by class field theory.  $\square$

If  $p$  divides the class number of  $k_0$ , there is nothing to prove. Otherwise, there is no nontrivial capitulation from  $k_0$  to  $k_1$ . Thus  $I_0$  must be a principal ideal  $I_0 = (\alpha_0)$  for some  $\alpha_0$  in  $k_0$ . Therefore

$$\alpha_1^{b_1} \cdots \alpha_{l-1}^{b_{l-1}} \pi_1^{b_l} = \alpha_0 u$$

for some unit  $u$  in  $k_1$ . Hence

$$\xi = (\alpha_1^{b_1} \cdots \alpha_{l-1}^{b_{l-1}} \pi_1^{b_l})^{\sigma^{-1}} = u^{\sigma^{-1}}.$$

Since  $B \not\equiv (0, \dots, 0)^t \pmod{p}$ ,  $\xi$  is not in  $C_1^{\sigma-1}$ . Thus we have a non-trivial kernel of the homomorphism  $H^1(G_1, C_1) \rightarrow H^1(G_1, E_1)$ , where  $E_1$  is the unit group of  $k_1$ . From the short exact sequence

$$0 \rightarrow C_1 \rightarrow E_1 \rightarrow E_1/C_1 \rightarrow 0,$$

we get a long exact sequence

$$0 \rightarrow C_0 \rightarrow E_0 \rightarrow (E_1/C_1)^{G_1} \rightarrow H^1(G_1, C_1) \rightarrow H^1(G_1, E_1) \rightarrow \dots$$

Since  $H^1(G_1, C_1) \rightarrow H^1(G_1, E_1)$  is not injective,

$$(E_1/C_1)^{G_1} \otimes \mathbb{Z}_p \neq \{0\}.$$

Therefore  $E_1/C_1 \otimes \mathbb{Z}_p \neq \{0\}$ . Then by the index theorem of W.Sinnott in Section 2, we have  $p|h_1$  as desired.

## References

- [1] B.Ferrero and L.Washington, *The Iwasawa invariant  $\mu_p$  vanishes for abelian number fields*, Ann.of Math. **109** (1979), 377–395.
- [2] R.Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. **98** (1976), 263–284.
- [3] K.Iwasawa, *On  $\mathbb{Z}_l$ -extensions of algebraic number fields*, Ann. of Math. **98** (1973), 246–326.
- [4] K.Iwasawa, *On cohomology groups of units for  $\mathbb{Z}_p$ -extensions*, Amer.J.Math. **105 No.1** (1983), 189–200.
- [5] J.M.Kim, *Class numbers of real quadratic fields*, Bull.Austral.Math.Soc. **57** (1998), 261–274.
- [6] J.M.Kim, *Circular units in the  $\mathbb{Z}_p$ -extensions of real abelian fields of prime conductor* (to appear).
- [7] S.Lang, *Cyclotomic Fields*, G.T.M. 59, 69, Springer-Verlag, New York.
- [8] B.Mazur and A.Wiles, *Class fields of abelian extensions of  $\mathbb{Q}$* , Invent.Math. **76** (1984), 179–330.
- [9] W.Sinnott, *On the Stickelberger ideal and the circular units of an abelian field*, Invent.Math. **62** (1980), 181–234.
- [10] L.Washington, *Introduction to Cyclotomic Fields*, G.T.M.83, Springer-Verlag, New York, 1980.

Department of Mathematics  
 Inha University  
 Incheon, Korea  
*E-mail:* jmkim@math.inha.ac.kr