ACTA ARITHMETICA
105.1 (2002)

A note on the ideal class group of the cyclotomic $\mathbb{Z}_p$-extension of a totally real number field

by

Humio Ichimura (Yokohama)

1. Introduction. Let p be a fixed prime number (not necessarily odd), k a fixed totally real number field, and k_∞/k the cyclotomic $\mathbb{Z}_p$-extension. Let k_n be the nth layer of k_∞/k with $k_0 = k$, and A_n the Sylow p-subgroup of the ideal class group of k_n. Denote by

$$A_\infty = \varinjlim A_n$$

the inductive limit with respect to the inclusion maps $k_n \to k_m$ $(n < m)$. It is conjectured that $A_\infty = \{0\}$ (see Greenberg [1]). Let $\widetilde{A}_0$ be the image of A_0 in A_∞. Concerning the conjecture, Greenberg [1, Theorem 1] proved the following:

Theorem 1. *Assume that there is only one prime ideal of k over p and that it is totally ramified in k_∞. Then $A_\infty = \{0\}$ if $\widetilde{A}_0 = \{0\}$.*

The purpose of the present note is to give (1) the following rather stronger version of this theorem (under the same assumptions), and (2) corresponding assertions when p splits completely in k. Let $\Gamma = \mathrm{Gal}(k_\infty/k)$, and A_∞^Γ the elements of A_∞ fixed by Γ. Clearly, $\widetilde{A}_0 \subseteq A_\infty^\Gamma$.

Theorem 2. *Under the assumptions of Theorem 1, $A_\infty^\Gamma/\widetilde{A}_0 = \{0\}$.*

Theorem 1 follows from Theorem 2 and the following assertion which is known to specialists.

Proposition 1. *Under the general setting of this section, $A_\infty = \{0\}$ if and only if $A_\infty^\Gamma = \{0\}$.*

Let L_n be the maximal pro-p abelian extension over k_n such that $L_n \supseteq k_\infty$ and L_n/k_∞ is unramified, and let F_n be the Hilbert p-class field of k_n.

2000 *Mathematics Subject Classification*: Primary 11R23.

Partially supported by Grant-in-Aid for Scientific Research (C) (No.13640036), the Ministry of Education, Culture, Sports, Science and Technology of Japan.

Clearly, we have $F_n k_\infty \subseteq L_n$. It is known (Sumida [6, Lemma 1]) that if the equality $F_n k_\infty = L_n$ holds for some $n = n_0$, then it holds for all $n \geq n_0$. For this, see also Lemma 3 and (1) in Section 3.

THEOREM 3. *Assume that p splits completely in k and that the Leopoldt conjecture holds for (k, p). Then $A_\infty^\Gamma / \widetilde{A}_0 = \{0\}$ if $F_n k_\infty = L_n$ for some n.*

Corresponding to Theorem 1, we obtain, from Theorem 3 and Proposition 1, the following:

THEOREM 4. *Under the assumptions of Theorem 3, $A_\infty = \{0\}$ if $\widetilde{A}_0 = \{0\}$ and $F_n k_\infty = L_n$ for some n.*

In the previous paper [2, Propositions 1, 3], we proved the assertions of Theorems 2, 3 when p is odd and k is a real abelian field with $[k : \mathbb{Q}]$ not divisible by p.

We show Theorem 2 by re-arranging some arguments in [1, pp. 267–269]. We can say that Theorem 2 is essentially contained in [1]. We show Theorem 3 similarly to [2, Proposition 3], using some skillful arguments of [1, p. 270].

REMARK 1. (1) Under the assumptions of Theorem 1, it is known and easy to show that $F_n k_\infty = L_n$ for all n. (2) The sufficient condition for $A_\infty = \{0\}$ in Theorem 4 is also necessary. This is because $A_\infty = \{0\}$ if and only if $L = \bigcup_n L_n$ is a finite extension over k_∞ (cf. [1, Proposition 2]). (3) Taya [8, Theorem 4] gave a condition for $A_\infty = \{0\}$ similar to Theorem 4 when p is odd and k is a real quadratic field in which p splits. In [7], Sumida proved an assertion on the p-ideal class group of k_∞ similar to Theorem 4. His theorem is given in a very general setting where k is not necessarily totally real, p does not necessarily split completely in k, and k_∞ / k is an arbitrary $\mathbb{Z}_p$-extension.

REMARK 2. At present, we have many numerical examples of (k, p) with $A_\infty = \{0\}$ but no counterexamples (see Kraft and Schoof [4], Kurihara [5], Sumida and the author [3]). For example, it is known that $A_\infty = \{0\}$ when $p = 3$ and $k = \mathbb{Q}(\sqrt{d})$ for all square free integers d with $1 < d < 10^4$ ([3, Proposition]). However, the conjecture is not yet proved to be true in general.

2. Proof of Theorem 2. In this section, we show Theorem 2 by re-arranging some arguments of [1, pp. 267–269]. In what follows, we assume that the prime ideals of k over p are totally ramified in k_∞. Let E_n be the group of units of k_n. The following lemma is proved in [1, p. 269, line 15].

LEMMA 1. *Under the assumptions of Theorem 1, the order $|E_0 / N_{n/0} E_n|$ is bounded as $n \to \infty$. Here, $N_{n/0}$ is the norm map from $k_n^\times$ to $k^\times$.*

Let I_n be the group of fractional ideals of k_n, and I_∞ the inductive limit of I_n with respect to the inclusion maps $k_n \to k_m$ $(n < m)$. We often regard ideals of k_n as elements of I_∞. For an ideal $\mathfrak{A} \in I_n$ $(0 \le n \le \infty)$, $[\mathfrak{A}]_n$ denotes the ideal class of k_n represented by $\mathfrak{A}$. We put $B_n = A_n^{\Gamma}$, the elements of A_n invariant under the action of Γ. The following lemma is a detailed version of [1, Corollary].

LEMMA 2. *Assume that the assumptions of Theorem* 1 *hold or that the Leopoldt conjecture holds for* (k, p). *Let* h' *be the non-p-part of the class number of* k. *Then, for any natural numbers* m, l *and any prime ideal* $\mathfrak{P}$ *of* k_m *over* p, *the ideal* $\mathfrak{P}^{h'}$ *becomes a* p^l*th power of a principal ideal in* I_∞.

Proof. It is known that the order of B_n is bounded as $n \to \infty$ under the assumption of the lemma. For this, see [1, Proposition 1] and line 14 of [1, p. 269]. Let t be an integer such that p^t is a multiple of $|B_n|$ for all n. There exists a unique prime ideal $\widetilde{\mathfrak{P}}$ of k_{m+l+t} over $\mathfrak{P}$, and the ideal class $[\widetilde{\mathfrak{P}}^{h'}]_{m+l+t}$ is contained in B_{m+l+t}, because the primes of k over p are totally ramified in k_∞. Then $\mathfrak{P}^{h'} = (\widetilde{\mathfrak{P}}^{h'p^t})^{p^l}$, and $\widetilde{\mathfrak{P}}^{h'p^t}$ is a principal ideal of k_{m+l+t}. The assertion follows from this. ■

Proof of Theorem 2. We fix a topological generator γ of Γ. Assume that the assumptions of Theorem 1 hold. Let $[\mathfrak{A}]_\infty$ be an element of A_∞^{Γ} with $\mathfrak{A} \in I_\infty$. We have $\mathfrak{A}^{\gamma-1} = (x)$ for some $x \in k_\infty^\times$. Take an integer n such that $\mathfrak{A} \in I_n$ and $x \in k_n^\times$. We have $\varepsilon = N_{n/0}x \in E_0$. By Lemma 1, we see that

$$N_{m/0}x = \varepsilon^{p^{m-n}} \in N_{m/0}E_m$$

for a sufficiently large $m \ge n$. Then $N_{m/0}x = N_{m/0}\eta$ for some $\eta \in E_m$. From this, $x\eta^{-1} = y^{\gamma-1}$ for some $y \in k_m^\times$, and hence

$$\mathfrak{A}^{\gamma-1} = (x\eta^{-1}) = (y^{\gamma-1}).$$

Therefore, the ideal $\mathfrak{A}(y)^{-1}$ of k_m is Γ-invariant. Then we see that $\mathfrak{A}(y)^{-1} = \mathfrak{B}\mathfrak{C}$ for some $\mathfrak{B} \in I_0$ and a product $\mathfrak{C}$ of prime ideals of k_m over p. Therefore, by Lemma 2, we see that $[\mathfrak{A}]_\infty^{h'} \in \widetilde{A}_0$. From this, we obtain $A_\infty^{\Gamma}/\widetilde{A}_0 = \{0\}$. ■

Proof of Proposition 1. Though this is more or less known, we give a proof for the sake of completeness. It suffices to show that the condition $A_\infty \ne \{0\}$ implies $A_\infty^{\Gamma} \ne \{0\}$. Assume that $A_\infty \ne \{0\}$. Let H_n be the kernel of the natural map $A_n \to A_\infty$. As $A_\infty \ne \{0\}$, $A_n/H_n \ne \{0\}$ for some n. Then we see that there exists a class $[\mathfrak{A}]_n \in A_n$ with $\mathfrak{A} \in I_n$ such that $[\mathfrak{A}]_n \notin H_n$ but $[\mathfrak{A}]_n^{\gamma-1} \in H_n$. This is because p-groups acting on p-groups have nontrivial fixed points. Therefore, we obtain $A_\infty^{\Gamma} \ne \{0\}$. ■

REMARK 3. Let D_n be the classes in A_n which contain a product of prime ideals of k_n over p. We have $D_n \subseteq B_n$ since the primes of k over p are totally ramified in k_∞. Assume that the Leopoldt conjecture holds for

(k, p). Then, in [1, p. 270], it is shown that $A_\infty = \{0\}$ when $B_n = D_n$ for all sufficiently large n. This assertion also follows from Proposition 1 and Lemma 2.

3. Proof of Theorem 3. Let p and k be as in Section 1. For a prime ideal $\mathfrak{p}$ of k_n over p, let $k_{n,\mathfrak{p}}$ be the completion of k_n at $\mathfrak{p}$, and $\mathfrak{U}_{n,\mathfrak{p}}$ the group of principal units of $k_{n,\mathfrak{p}}$. Denote by $\mathfrak{U}_n = \prod_{\mathfrak{p}|p} \mathfrak{U}_{n,\mathfrak{p}}$ the group of semi-local units of k_n at p, where $\mathfrak{p}$ runs over the primes of k_n over p. We put

$$\mathfrak{V}_n = \bigcap_{m \geq n} N_{m/n} \mathfrak{U}_m$$

and

$$\widetilde{\mathfrak{U}}_n = \Big\{ (u_\mathfrak{p}) \in \mathfrak{U}_n \,\Big|\, \prod_{\mathfrak{p}|p} (u_\mathfrak{p}, k_m/k_n, \mathfrak{p}) = 1, \ \forall m \geq n \Big\}.$$

Here, $N_{m/n}$ is the norm map from $k_m^\times$ to $k_n^\times$, and $(*, k_m/k_n, \mathfrak{p})$ denotes the norm residue symbol at $\mathfrak{p}$ for the extension k_m/k_n. We have $\mathfrak{V}_n \subseteq \widetilde{\mathfrak{U}}_n$ by local class field theory. Let E_n be, as before, the group of units of k_n. Embed $k_n^\times$ diagonally into the product $\prod_{\mathfrak{p}|p} k_{n,\mathfrak{p}}^\times$, and let $\mathfrak{E}_n$ be the closure of $E_n \cap \mathfrak{U}_n$ in $\mathfrak{U}_n$. We see that $\mathfrak{E}_n \subseteq \widetilde{\mathfrak{U}}_n$ by the product formula for the norm residue symbols. On the quotient group $\widetilde{\mathfrak{U}}_n / \mathfrak{V}_n \mathfrak{E}_n$, the following assertion holds, which is essentially contained in [6].

Lemma 3. *If the equality $\widetilde{\mathfrak{U}}_n = \mathfrak{V}_n \mathfrak{E}_n$ holds for some $n = n_0$, then it holds for all $n \geq n_0$.*

Proof. Let $m > n$. Using local class field theory, we can show that the inclusion map $k_n^\times \to k_m^\times$ induces an isomorphism

$$\widetilde{\mathfrak{U}}_n / \mathfrak{V}_n \cong \widetilde{\mathfrak{U}}_m / \mathfrak{V}_m.$$

For details, see [6, p. 695, line 17]. The assertion follows from this as $E_n \subseteq E_m$. ∎

Let M_n be the maximal pro-p abelian extension over k_n unramified outside p, and let L_n, F_n be the extensions of k_n defined in Section 1. From the definitions, we have $F_n k_\infty \subseteq L_n \subseteq M_n$. It is known that the reciprocity law map induces isomorphisms

$$\mathrm{Gal}(M_n/F_n k_\infty) \cong \widetilde{\mathfrak{U}}_n / \mathfrak{E}_n \quad \text{and} \quad \mathrm{Gal}(M_n/L_n) \cong \mathfrak{V}_n \mathfrak{E}_n / \mathfrak{E}_n.$$

For the former, see [9, Corollary 13.6], and for the latter, see [6, Proposition 1] or [3, Lemma 3]. From the above, one obtains the following isomorphism:

$$\mathrm{Gal}(L_n/F_n k_\infty) \cong \widetilde{\mathfrak{U}}_n / \mathfrak{V}_n \mathfrak{E}_n. \tag{1}$$

Proof of Theorem 3. We assume that p splits completely in k and that the Leopoldt conjecture holds for (k,p). We also assume that $F_{n_0}k_\infty = L_{n_0}$ for some integer n_0. Let $[\mathfrak{A}]_\infty$ be an element of A_∞^Γ with $\mathfrak{A} \in I_\infty$. We have

$$\mathfrak{A}^{\gamma-1} = (x) \tag{2}$$

for some $x \in k_\infty^\times$. Here, γ is the fixed topological generator of Γ. Take an integer n such that $n \geq n_0$, $\mathfrak{A} \in I_n$ and $x \in k_n^\times$. By (2), x is relatively prime to p. Embedding $k_n^\times$ into the product $\prod_{\mathfrak{p}|p} k_{n,\mathfrak{p}}^\times$ diagonally, we can also regard x as an element of $\mathfrak{U}_n$ (by raising $\mathfrak{A}$ and x to the $(p-1)$st power if necessary). By (2), we obtain

$$N_{n/0}x \in E_0. \tag{3}$$

From this, we see that for any $m \geq n$,

$$\prod_{\mathfrak{p}|p}(x, k_m/k_n, \mathfrak{p}) = \prod_{\mathfrak{p}|p}(N_{n/0}x, k_m/k, \mathfrak{p}') = 1$$

by the product formula for the norm residue symbols. Here, $\mathfrak{p}$ runs over the primes of k_n over p, and $\mathfrak{p}' = \mathfrak{p} \cap k$. Therefore, we obtain $x \in \widetilde{\mathfrak{U}}_n$. It is known ([1, p. 265]) that

$$E_0 \cap \mathfrak{U}_0^{p^{n+l}} \subseteq E_0^{p^{n+1}} \tag{4}$$

for some integer $l \geq 0$ as a consequence of the Leopoldt conjecture for (k,p). Since $n \geq n_0$ and $F_{n_0}k_\infty = L_{n_0}$, we obtain $\widetilde{\mathfrak{U}}_n = \mathfrak{V}_n\mathfrak{E}_n$ from Lemma 3 and (1). Then, as $x \in \widetilde{\mathfrak{U}}_n$, we have

$$x \equiv (N_{n+l/n}v)\varepsilon \bmod \mathfrak{U}_n^{p^l} \tag{5}$$

for some $v \in \mathfrak{U}_{n+l}$ and $\varepsilon \in E_n$.

Now, we distinguish the cases where p is odd and where $p = 2$. First, let p be odd. We see that $N_{m/0}\mathfrak{U}_m = \mathfrak{U}_0^{p^m}$ for any m since p is odd and p splits completely in k. Therefore, we obtain

$$N_{n/0}x \equiv N_{n/0}\varepsilon \bmod \mathfrak{U}_0^{p^{n+l}}$$

from (5). By (3), (4) and this congruence, we obtain $N_{n/0}(x\varepsilon^{-1}) = \eta^{p^n}$ for some $\eta \in E_0$, and hence $N_{n/0}(x\varepsilon^{-1}\eta^{-1}) = 1$. Therefore, $x\varepsilon^{-1}\eta^{-1} = y^{\gamma-1}$ for some $y \in k_n^\times$. From this and (2), it follows that the ideal $\mathfrak{A}(y)^{-1}$ of k_n is Γ-invariant. Then we can write $\mathfrak{A}(y)^{-1} = \mathfrak{B}\mathfrak{C}$ for some ideal $\mathfrak{B}$ of k and a product $\mathfrak{C}$ of prime ideals of k_n over p. From this and Lemma 2, we obtain $[\mathfrak{A}]_\infty^{h'} = [\mathfrak{B}]_\infty^{h'} \in \widetilde{A}_0$. The desired assertion follows from this when p is odd.

Next, let $p = 2$. Then we see that $N_{m/0}\mathfrak{U}_m^2 = \mathfrak{U}_0^{2^{m+1}}$ for any m since p splits completely in k. Thus, by (3)–(5), we obtain $N_{n/0}(x^2\varepsilon^{-2}) = \eta^{2^{n+1}}$ for some $\eta \in E_0$, and hence, $N_{n/0}(x\varepsilon^{-1}\eta^{-1}) = \pm 1$. Let ζ be a primitive 2^{n+2}nd root of unity, and put

$$\delta = \zeta^2 + \zeta + 1 + \zeta^{-1} + \zeta^{-2} = (\zeta^5 - 1)/(\zeta^3 - \zeta^2).$$

We easily see that $\delta \in E_n$ and $N_{n/0}\delta = -1$. Therefore, we have

$$N_{n/0}(x\varepsilon^{-1}\eta^{-1}) = 1 \quad \text{or} \quad N_{n/0}(x\varepsilon^{-1}\eta^{-1}\delta) = 1.$$

Using this, we obtain the desired assertion by an argument similar to the case $p \geq 3$. ■

Acknowledgements. The author is grateful to Hiroki Sumida for valuable conversations, especially on the proof of Theorem 3 for the case $p = 2$.

References

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

[2] H. Ichimura, *On a quotient of the unramified Iwasawa module over an abelian number field*, J. Number Theory 88 (2001), 175–190.

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

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

[5] M. Kurihara, *The Iwasawa λ-invariants of real abelian fields and the cyclotomic elements*, Tokyo J. Math. 22 (1999), 259–277.

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

[7] —, *On capitulation of S-ideal classes in $\mathbb{Z}_p$-extensions*, J. Number Theory 86 (2001), 163–174.

[8] H. Taya, *On cyclotomic $\mathbb{Z}_p$-extensions of real quadratic fields*, Acta Arith. 74 (1996), 107–119.

[9] L. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Springer, New York, 1996.

Department of Mathematics
Yokohama City University
22-2, Seto, Kanazawa-ku
Yokohama, 236-0027 Japan
E-mail: ichimura@yokohama-cu.ac.jp

Received on 26.4.2000
and in revised form on 19.12.2001 (3815)