ACTA ARITHMETICA
120.4 (2005)

Cohomology groups of the class groups over a $\mathbb{Z}_p$ extension

by

SOOGIL SEO (Seoul)

1. Introduction. Since Kummer found the class number formula for the maximal real subfield of the pth cyclotomic field $\mathbb{Q}(\mu_p)$ the relations between the class groups and the quotient groups of the global units by the cyclotomic units have been a subject of study for a long time. The arguments of Euler systems (cf. [10], [12], [13]) by Kolyvagin and Rubin established a strong tie between these two objects.

The purpose of this short note is to study the relations of the cohomology groups of certain Galois groups with coefficients in the class groups and those of the quotient of the units modulo cyclotomic units. Even if the Galois module of a class group and the quotient of the units modulo cyclotomic units need not be isomorphic, the cohomology groups are shown to be isomorphic over the $\mathbb{Z}_p$ extension $\mathbb{Q}(\mu_{p^\infty})$.

The cohomology groups of the "p-primary parts" of ideal class groups and those of the quotients of global units modulo cyclotomic units (together with their own cohomology groups) over the basic $\mathbb{Z}_p$ extension have been studied for many years. Specially Iwasawa gave many interesting results on the cohomology groups on these objects over $\mathbb{Z}_p$ extensions (cf. [5]–[7]).

Using a result of Iwasawa and the computations of the cohomology groups of circular units due to R. Gold and J. Kim (cf. [3], [8]) we will show the following theorem. Let μ_n be the set of nth roots of unity in a fixed algebraic closure $\mathbb{Q}^{\mathrm{alg}}$ of the rational field $\mathbb{Q}$, and $\zeta_n \in \mu_n$ be a primitive nth root of unity. Let Cl_n be the class group of $K_n := \mathbb{Q}(\zeta_{p^n} + \zeta_{p^n}^{-1})$. Let E_n, C_n be the group of units and cyclotomic units of K_n respectively. Finally, let $\mathbf{H}^i(G, M)$ denote the Tate cohomology group of G with coefficients in a G-module M.

THEOREM 1.1. *Let P be a p-subgroup of $G(K_n/\mathbb{Q})$. Then*

$$\mathbf{H}^i(P, \mathrm{Cl}_n) \simeq \mathbf{H}^i(P, E_n/C_n) \quad \textit{for all } i \textit{ and } n.$$

2000 *Mathematics Subject Classification*: 11R18, 11R34, 11R37, 11S25, 11S31.

This work was supported in part by Yonsei University Research Fund of 2005.

For the cohomology groups of "prime-to-p parts" we start with a result of Schoof. In his recent paper [14], Schoof showed that the cohomology groups of these two objects are isomorphic for the maximal real subfield $K_1 = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ of the pth cyclotomic field. More precisely, let $p > 2$ be a prime and H be a subgroup of the Galois group $G(K_1/\mathbb{Q})$. Let E_1, C_1 be the units and cyclotomic units of K_1, and Cl_1 the class group of K_1. Then Schoof's result (§5 of [14]) states that for each choice of a generator of H there are natural isomorphisms

$$\mathbf{H}^i(H, \mathrm{Cl}_1) \simeq \mathbf{H}^i(H, E_1/C_1) \quad \text{for each } i.$$

We extend his method to the maximal real subfield K_n of the p^nth cyclotomic field. We will prove the following theorem.

Theorem 1.2. *Let H be a subgroup of $G(K_n/\mathbb{Q})$ with order $\#(H)$ prime to p. Then*

$$\mathbf{H}^i(H, \mathrm{Cl}_n) \simeq \mathbf{H}^i(H, E_n/C_n) \quad \textit{for all } i \textit{ and } n.$$

As an immediate corollary of Theorems 1.1 and 1.2, we have

Corollary 1.3. *Let G be any subgroup of $G(K_n/\mathbb{Q})$. Then*

$$\mathbf{H}^i(G, \mathrm{Cl}_n) \simeq \mathbf{H}^i(G, E_n/C_n) \quad \textit{for all } i.$$

We have recently been informed that the result above when K_n has prime power conductor and G is a Sylow subgroup of $G(K_n/\mathbb{Q})$ has already appeared in the paper by Greither and Cornacchia (cf. [2]). Their approach, which we think is more elegant, is different from ours which is elementary and computational.

Let K_∞ be the basic $\mathbb{Z}_p$ extension of K_1. Let $G_n = G(K_n/\mathbb{Q})$ and $G_\infty = G(K_\infty/\mathbb{Q})$. Let $E_\infty, C_\infty, \mathrm{Cl}_\infty$ denote the inverse limits of E_n, C_n, Cl_n respectively with respect to the norm maps. As an immediate corollary we obtain the following

Corollary 1.4. *For all i, we have the $\varprojlim \mathbb{Z}[G_n]$-module isomorphism*

$$\mathbf{H}^i(G_\infty, \mathrm{Cl}_\infty) \simeq \mathbf{H}^i(G_\infty, E_\infty/C_\infty).$$

In §2 we start with the basic arithmetic of cyclotomic units, which will be used in the subsequent section. The arithmetic of cyclotomic units is essential to compute the cohomology groups of certain Galois groups with coefficients in the cyclotomic units. In order to compute the cohomology of certain Galois groups with coefficients in class groups we need to recall the basic tools of class field theory. In the computation of the cohomology of the prime-to-p parts, the key ingredient is Schoof's method which combines the arithmetic of cyclotomic units with classical class field theory which gives information on the class groups together with the class number formula. In §3 we will prove our theorems.

Acknowledgements. We are grateful to the referee for helpful comments and suggestions.

2. Basic arithmetic of cyclotomic units.

We begin with the notion of cyclotomic units (cf. [1], [16] and [17]), which will play a crucial rule in our arguments. Let p denote a fixed odd prime. As defined in the introduction, let K_n be the maximal real subfield of the cyclotomic field $\mathbb{Q}(\mu_{p^n})$. The group $C(p^n)$ of *cyclotomic numbers* of $\mathbb{Q}(\mu_{p^n})$ is defined to be the multiplicative group generated over $\mathbb{Z}$ by

$$\{\pm\zeta_{p^n}, 1-\zeta_{p^n}^a \mid 1 \le a \le p^n-1\}.$$

One can show that $C(p^n)$ is equal to the group generated as Galois module of the group ring $\mathbb{Z}[G(\mathbb{Q}(\mu_{p^n})/\mathbb{Q})]$ by $1-\zeta_{p^n}$. We define the group C_n of *cyclotomic* or *circular units* of K_n to be the intersection of the group E_n of units of K_n with $C(p^n)$,

$$C_n = E_n \cap C(p^n).$$

This group C_n can be shown to be equal to the group generated by -1 and the units of the following forms:

$$\zeta_{p^n}^{1-a}\frac{1-\zeta_{p^n}^{2a}}{1-\zeta_{p^n}^{2}}, \qquad 1<a<p^n/2,\ (a,p)=1.$$

Let σ denote a fixed generator of the Galois group $G(\mathbb{Q}(\mu_{p^n})/\mathbb{Q})$. We can associate to σ a primitive root g modulo p^n with $\sigma(\zeta_{p^n}) = \zeta_{p^n}^g$. The σ induces a natural generator of the Galois group of $G(K_n/\mathbb{Q})$ which will be denoted by the same σ if no ambiguity can arise. By a direct computation, one can show that C_n is generated as Galois module of the group ring $\mathbb{Z}[G(K_n/\mathbb{Q})]$ by

$$\eta := (\zeta_{p^n}-\zeta_{p^n}^{-1})^{\sigma-1} = \frac{\sigma(\zeta_{p^n}-\zeta_{p^n}^{-1})}{\zeta_{p^n}-\zeta_{p^n}^{-1}}.$$

We have the following lemma on the cohomology groups with coefficients in the group of cyclotomic units. We will use mainly the fact that the zeroth Tate cohomology of the circular units vanishes. For an abelian extension L/K we denote by $N_{L/K}$ the norm map from L to K.

Lemma 2.1. *Let G be any subgroup of $G(K_n/\mathbb{Q})$. Then $\mathbf{H}^i(G,C_n)=0$ for all even i. If G is either a p-subgroup or $\#(G)$ is a prime number then the order of $\mathbf{H}^i(G,C_n)$ is equal to $\#(G)$ for all odd i.*

Proof. It follows from the above argument that

$$C_n/\{\pm1\} = (\zeta_{p^n}-\zeta_{p^n}^{-1})^{(\sigma-1)\mathbb{Z}[G(K_n/\mathbb{Q})]} \simeq I_{G(K_n/\mathbb{Q})},$$

where $I_{G(K_n/\mathbb{Q})}$ denotes the augmentation ideal $(\sigma-1)\mathbb{Z}[G(K_n/\mathbb{Q})]$ of the group ring $\mathbb{Z}[G(K_n/\mathbb{Q})]$. By the well known fact that $\mathbf{H}^0(G, I_{G(K_n/\mathbb{Q})}) = 0$

we have a surjection

$$\mathbf{H}^0(G, \{\pm 1\}) \to \mathbf{H}^0(G, C_n) \to 0.$$

We will use the following convenient notation. Let $(s, p) = 1$. We denote by σ_s the element of $G(\mathbb{Q}(\mu_{p^n})/\mathbb{Q})$ such that $\sigma_s(\zeta_{p^n}) = \zeta_{p^n}^s$. We will use the same notation for a subfield if no confusion can arise. One sees easily that the norm $N_{K_n/\mathbb{Q}}$ of η is equal to -1,

$$N_{K_n/\mathbb{Q}}(\eta) = (\zeta_{p^n} - \zeta_{p^n}^{-1})^{(\sigma-1)\sum_{i=0}^{(p-3)/2} \sigma^i} = (\zeta_{p^n} - \zeta_{p^n}^{-1})^{(\sigma_{-1}-1)} = -1,$$

by taking $\sigma^{(p-1)/2} = \sigma_{-1}$ into account. This shows that the norm map N_G of G has the value -1 at $\eta^{1+\sigma+\cdots+\sigma^{a-1}}$ where $a = \#(G(K_n/\mathbb{Q})/G)$. It follows that the above surjection is trivial and $\mathbf{H}^0(G, C_n)$ vanishes.

Suppose now that $\#(G)$ is a prime number. As E_n/C_n is finite, the Herbrand quotient of C_n is equal to that of E_n which is equal to $1/\#(G)$. Hence in this case $\#(\mathbf{H}^i(G, C_n)) = \#(G)$ for all odd i. Finally, if G is a p-group then the conclusion follows from Theorem 2 of [8]. This completes the proof. ∎

Remark. Note that if G is a p-group then the first cohomology groups $\mathbf{H}^1(G, C(n))$ of G with coefficients in the circular units $C(n)$ of the nth cyclotomic field $\mathbb{Q}(\mu_n)$ (not of K_n) are more explicitly known from the concrete computations (cf. [3], [8]):

$$\mathbf{H}^1(G, C(n)) \simeq \mathbb{Z}/g\mathbb{Z},$$

where $\#(G) = g$. Notice also that in general $C(n)$ is not equal to C_n.

We briefly recall class field theory which will be used later. Let L/K be a cyclic extension of either local or global fields. Let $\mathbb{A}_L$ denote the multiplicative group $L^\times$ or the idele class group Ic_L according as the extension is local or global. Then class field theory tells us there is an isomorphism (Artin map)

$$\mathbf{H}^i(G(L/K), \mathbb{A}_L) \simeq \begin{cases} G(L/K) & \text{if } i \text{ is even,} \\ 0 & \text{if } i \text{ is odd.} \end{cases} \tag{1}$$

Let L/K be an abelian extension of local fields. The inertia group $\mathrm{I}(L/K)$ of $G(L/K)$ has an isomorphism via class field theory,

$$\mathrm{I}(L/K) \simeq \mathbf{H}^0(G(L/K), U_L), \tag{2}$$

where U_L denotes the group of local units of L. Let $\mathfrak{P}$ be the prime of L over $\mathfrak{p} \in K$, and $\mathfrak{f}_{\mathfrak{P}}$ the residue field of $\mathfrak{P}$. Let U_L^i denote the group of all elements u of U_L which are 1 modulo $\mathfrak{P}^i$.

If L/K is an unramified extension then it follows from the isomorphism $U_L^{i-1}/U_L^i \simeq \mathfrak{f}_{\mathfrak{P}}$ for $i > 1$ and a filtration of U_L^1 by U_L^i that (see [15]) $\mathbf{H}^i(G(L/K), U_L^1) = 0$ for all i as $\mathbf{H}^i(G(L/K), \mathfrak{f}_{\mathfrak{P}}) = \mathbf{H}^i(G(\mathfrak{f}_{\mathfrak{P}}/\mathfrak{f}_{\mathfrak{p}}), \mathfrak{f}_{\mathfrak{P}})$

$= 0$. Hence the isomorphism $U_L/U_L^1 \simeq \mathfrak{f}_{\mathfrak{P}}^{\times}$ yields $\mathbf{H}^1(G(L/K), U_L) = \mathbf{H}^1(G(L/K), \mathfrak{f}_{\mathfrak{P}}^{\times}) = \mathbf{H}^1(G(\mathfrak{f}_{\mathfrak{P}}/\mathfrak{f}_{\mathfrak{p}}), \mathfrak{f}_{\mathfrak{P}}^{\times}) = 0$. Finally, class field theory tells us that $\mathbf{H}^2(G(L/K), U_L) = 0$.

If L/K is a totally ramified extension then the Galois group $G(L/K)$ acts trivially on the residue field $\mathfrak{f}_{\mathfrak{P}}$. In this case one can easily see that if the order of $G(L/K)$ is prime to p then the $\mathbf{H}^i(G(L/K), \mathfrak{f}_{\mathfrak{P}})$ are trivial. Applying the same reasoning one obtains

$$\mathbf{H}^i(G(L/K), U_L^1) = 0 \quad \text{for all } i. \tag{3}$$

It follows from (3) and the cohomology sequence induced from the short exact sequence of $0 \to U_L^1 \to U_L \to \mathfrak{f}_{\mathfrak{P}}^{\times} \to 0$ that

$$\mathbf{H}^i(G(L/K), U_L) \simeq \mathbf{H}^i(G(L/K), \mathfrak{f}_{\mathfrak{P}}^{\times}) \quad \text{for all } i. \tag{4}$$

Note that the isomorphism (4) is induced by the map $u \mapsto u \bmod \mathfrak{P}$. Now we suppose that L/K is equal to $K_{n,\mathfrak{P}}/\mathbb{Q}_p$ where $K_{n,\mathfrak{P}}$ denotes the field of completion of K_n at $\mathfrak{P}$, the prime over p, and H is any subgroup of $G(L/K)$ whose order $\#(H) = h$ is prime to p. Then (4) becomes

$$\mathbf{H}^i(H, U_L) \simeq \begin{cases} \mathfrak{f}_{\mathfrak{P}}^{\times}/(\mathfrak{f}_{\mathfrak{P}}^{\times})^h & \text{if } i \text{ is even,} \\ \mu_h(\mathfrak{f}_{\mathfrak{P}}^{\times}) & \text{if } i \text{ is odd,} \end{cases} \tag{5}$$

where $\mu_h(\mathfrak{f}_{\mathfrak{P}}^{\times})$ denotes the set of hth roots of unity in $\mathfrak{f}_{\mathfrak{P}}^{\times}$.

Let $\mathbb{U}_n$ denote the group of unit ideles, which is the subgroup of the idele group consisting of unit elements at all finite places of K_n. As K_n is unramified at all primes except the prime $\mathfrak{P}$, the cohomology group $\mathbf{H}^i(H, \mathbb{U}_n)$ is isomorphic to $\mathbf{H}^i(H, U_{K_{n,\mathfrak{P}}})$, where $U_{K_{n,\mathfrak{P}}}$ denotes the group of local units of $K_{n,\mathfrak{P}}$. It follows from (5) that for all i, $\mathbf{H}^i(H, \mathbb{U}_n)$ is isomorphic to a cyclic group of order h, more precisely,

$$\mathbf{H}^i(H, \mathbb{U}_n) \simeq \begin{cases} \mathfrak{f}_{\mathfrak{P}}^{\times}/(\mathfrak{f}_{\mathfrak{P}}^{\times})^h & \text{if } i \text{ is even,} \\ \mu_h(\mathfrak{f}_{\mathfrak{P}}^{\times}) & \text{if } i \text{ is odd.} \end{cases} \tag{6}$$

Let $\alpha_1 : \mathbf{H}^1(H, C_n) \to \mathbf{H}^1(H, E_n)$ and $\alpha_2 : \mathbf{H}^1(H, E_n) \to \mathbf{H}^1(H, \mathbb{U}_n)$ be induced by the natural maps $C_n \to E_n$ and $E_n \to \mathbb{U}_n$ respectively.

Lemma 2.2. *Let H be a subgroup of $G(K_n/\mathbb{Q})$ with $\#(H) = h$ prime to p. Then the composite map $\alpha_2 \circ \alpha_1$ is surjective.*

Proof. Put $(p-1)/2h = h'$. Let $\varepsilon = \eta^{2(\sigma^{h'}-1)/(\sigma-1)}$. Then ε defines a cocycle of $\mathbf{H}^1(H, C_n)$. The map $\alpha_2 \circ \alpha_1$ can be identified with $c \mapsto c \bmod \mathfrak{P}$ for $c \in C_n$ via the isomorphism (6). It follows from $\varepsilon \equiv g^{2h'} \bmod (1 - \zeta_{p^n})$ that the image of ε has order h and hence $\alpha_2 \circ \alpha_1$ maps ε to a generator of $\mathbf{H}^1(H, \mathbb{U}_n)$. ■

3. Cohomology groups of class groups. Let $K(n)$ be the p^nth cyclotomic field $\mathbb{Q}(\mu_{p^n})$ and $\mathrm{Cl}(n)$ the ideal class group of $K(n)$. Let $E(n), C(n)$ be the groups of units and circular units of $K(n)$ respectively. Thus E_n and C_n are subgroups of $E(n)$ and $C(n)$ respectively which are fixed under complex conjugation. Write

$$G(m,n) := G(K(m)/K(n)) \quad \text{and} \quad G_{(m,n)} := G(K_m/K_n).$$

We fix a generator $\sigma_{m,n}$ of $G(m,n) \simeq G_{(m,n)}$. Let $N_{m,n}$ be the norm map from $\mathrm{Cl}(m)$ to $\mathrm{Cl}(n)$ and $\tau_{n,m}$ the homomorphism from $\mathrm{Cl}(n)$ to $\mathrm{Cl}(m)$ induced by the natural injection from the fractional ideals of $K(n)$ to $K(m)$. Let N_m be the composite map of $N_{m,n}$ and $\tau_{n,m}$,

$$\begin{tikzcd}
\mathrm{Cl}(m) \arrow[r, "N_{m,n}"] \arrow[dr, "N_m"'] & \mathrm{Cl}(n) \arrow[d, "\tau_{n,m}"] \\
 & \mathrm{Cl}(m)
\end{tikzcd}$$

Then $\mathbf{H}^1(G(m,n), \mathrm{Cl}(m))$ can be identified with the kernel of N_m modulo $\mathrm{Cl}(m)^{(\sigma_{m,n}-1)}$. We need the following theorem of Iwasawa.

Theorem 3.1 (Iwasawa [5, Theorem 11]). *For $m \geq n \geq 0$,*

$$\mathbf{H}^1(G(m,n), \mathrm{Cl}(m)) \simeq \mathrm{Ker}(\tau_{n,m}). \ ∎$$

We first compare the cohomology groups of certain Galois groups with coefficients in class groups and with coefficients in the quotient of the units by the circular units when G is a p-group. Very useful is the following theorem due to Iwasawa.

Theorem 3.2 (Iwasawa [5, Theorem 13]). *For $m \geq n \geq 0$,*

$$\mathbf{H}^0(G(m,n), \mathrm{Cl}(m)) \simeq \mathbf{H}^0(G(m,n), E(m)),$$
$$\mathbf{H}^1(G(m,n), \mathrm{Cl}(m)) \times \mathbb{Z}/p^{m-n}\mathbb{Z} \simeq \mathbf{H}^1(G(m,n), E(m)). \ ∎$$

Let $\Delta := G(K(1)/\mathbb{Q})$. Let Ξ be the set of p-adic-valued Dirichlet characters of Δ. For each χ in Ξ we let $\mathbb{Z}_p(\chi)$ denote the ring generated over $\mathbb{Z}_p$ by the values of χ. As p does not divide $\#(\Delta)$ the semisimple group ring $\mathbb{Z}_p[\Delta]$ decomposes into a product of discrete valuation rings, $\mathbb{Z}_p[\Delta] \simeq \prod_{\chi\in\Xi} \mathbb{Z}_p(\chi)$, and each $\mathbb{Z}_p[\Delta]$-module M has the corresponding decomposition

$$M = \prod_{\chi\in\Xi} (M \otimes_{\mathbb{Z}[\Delta]} \mathbb{Z}_p(\chi)).$$

We write $M(\chi) := M \otimes_{\mathbb{Z}[\Delta]} \mathbb{Z}_p(\chi)$. A character χ is called *even* or *odd* according as χ takes the value 1 or -1 at the complex conjugation. We denote by Ξ^+ the set of all even characters and by Ξ^- the set of all odd characters. Hence the product of $\mathrm{Cl}(n)(\chi)$ (resp. $E(n)(\chi)$, $C(n)(\chi)$, etc.)

over χ in $\varXi^+$ is just the ideal class group (resp. the units, the circular units, etc.) of K_n,

$$\prod_{\chi\in\varXi^+}\mathrm{Cl}(n)(\chi)=\mathrm{Cl}_n,\qquad \prod_{\chi\in\varXi^+}E(n)(\chi)=E_n,\qquad \prod_{\chi\in\varXi^+}C(n)(\chi)=C_n.$$

The objects appearing in Theorems 3.1 and 3.2 are $\mathbb{Z}_p[G(m,n)\times\varDelta]$-modules. As $p\nmid\#(\varDelta)$, for any $\mathbb{Z}_p[G(m,n)\times\varDelta]$-module M the functor $M\mapsto M(\chi)$ is exact and hence the short exact sequence of modules

$$0\to N_{G(m,n)}M\to M^{G(m,n)}\to M^{G(m,n)}/N_{G(m,n)}M\to 0$$

shows that

$$0\to N_{G(m,n)}M(\chi)\to M^{G(m,n)}(\chi)\to \mathbf{H}^0(G(m,n),M)(\chi)\to 0.$$

This proves that the cohomology functor commutes with the χ-functor,

$$\mathbf{H}^0(G(m,n),M)(\chi)\simeq\mathbf{H}^0(G(m,n),M(\chi)).$$

In a similar way we have an isomorphism on the first cohomology,

$$\mathbf{H}^1(G(m,n),M)(\chi)\simeq\mathbf{H}^1(G(m,n),M(\chi)).$$

The two isomorphisms above will be very useful in our subsequent arguments. As pointed out by Iwasawa (p. 552 of [5]), the proofs of the above Theorems 3.1 and 3.2 show that all these isomorphisms are Galois equivariant. Hence we have

$$\mathbf{H}^1(G(m,n),\mathrm{Cl}(m)(\chi))\simeq\mathbf{H}^1(G(m,n),\mathrm{Cl}(m))(\chi)\simeq\mathrm{Ker}(\tau_{n,m})(\chi),$$
$$\mathbf{H}^0(G(m,n),\mathrm{Cl}(m)(\chi))\simeq\mathbf{H}^0(G(m,n),E(m)(\chi)),$$
$$\mathbf{H}^1(G(m,n),\mathrm{Cl}(m)(\chi))\times(\mathbb{Z}/p^{m-n}\mathbb{Z})(\chi)\simeq\mathbf{H}^1(G(m,n),E(m)(\chi)).$$

As already noted by Iwasawa (*ibid.*), $\varDelta$ acts trivially on the cyclic factor $\mathbb{Z}/p^{m-n}\mathbb{Z}$ and hence $(\mathbb{Z}/p^{m-n}\mathbb{Z})(\chi)=0$ for $\chi\neq 1$. This fact will be reproved in terms of cohomology. If we sum all objects above over all even characters $\varXi^+$ then Theorems 3.1 and 3.2 can be rephrased as follows. For $m\geq n\geq 0$,

$$\mathbf{H}^1(G_{(m,n)},\mathrm{Cl}_m)\simeq\mathrm{Ker}(\tau^+_{n,m}),\tag{3.1}$$

$$\mathbf{H}^0(G_{(m,n)},\mathrm{Cl}_m)\simeq\mathbf{H}^0(G_{(m,n)},E_m),\tag{3.2}$$

$$\mathbf{H}^1(G_{(m,n)},\mathrm{Cl}_m)\times\mathbb{Z}/p^{m-n}\mathbb{Z}\simeq\mathbf{H}^1(G_{(m,n)},E_m).\tag{3.3}$$

Moreover for the p-group $G(m,n)$, from the remark after Lemma 2.1, we have an isomorphism of the cohomology group,

$$\mathbf{H}^1(G(m,n),C(m))\simeq\mathbb{Z}/p^{m-n}\mathbb{Z},$$

which is the highest p-power order cyclic subgroup of $\mathbf{H}^1(G(m,n),E(m))$. By computing the generator of $\mathbf{H}^1(G_{(m,n)},C_m)$, we will show that the first cohomology $\mathbf{H}^1(G_{(m,n)},C_m)$ corresponds exactly to the cyclic subgroup $\mathbb{Z}/p^{m-n}\mathbb{Z}$ inside $\mathbf{H}^1(G_{(m,n)},E_m)$ in (3.3).

First we will claim that $\mathbf{H}^1(G_{(m,n)}, C_m)$ injects into $\mathbf{H}^1(G_{(m,n)}, E_m)$. We have the injectivity (cf. [8], [9]) of the cohomology map induced from $C(m) \to E(m)$,

$$0 \to \mathbf{H}^1(G(m,n), C(m)) \to \mathbf{H}^1(G(m,n), E(m)).$$

As $\#(\Delta)$ is prime to p we can take the χ parts, which preserves the injectivity:

$$0 \to \mathbf{H}^1(G(m,n), C(m))(\chi) \to \mathbf{H}^1(G(m,n), E(m))(\chi).$$

Again applying the same reasoning we have

$$0 \to \mathbf{H}^1(G_{(m,n)}, C_m) \to \mathbf{H}^1(G_{(m,n)}, E_m).$$

In order to show that $\mathbf{H}^1(G_{(m,n)}, C_m)$ corresponds to the cyclic factor $\mathbb{Z}/p^{m-n}\mathbb{Z}$ inside $\mathbf{H}^1(G_{(m,n)}, E_m)$ via (3.3) we need to explain the isomorphisms of Theorems 3.1 and 3.2 (cf. [4], [5]).

Let V' denote the principal ideals of K_m which are fixed under the Galois action of $G(m,n)$,

$$V' := \{(\alpha) = \alpha O_{K(m)} \mid \alpha \in K(m),\ \tau((\alpha)) = (\alpha),\ \forall \tau \in G(m,n)\},$$

where $O_{K(m)}$ denotes the ring of integers of $K(m)$. Each $(\alpha) \in V'$ defines a unit $\varepsilon_{\sigma_{m,n}}$ such that $\varepsilon_{\sigma_{m,n}} = \alpha^{\sigma_{m,n}-1}$. This defines a homomorphism from V' to the first cohomology $\mathbf{H}^1(G(m,n), E(m)) \approx \mathbf{H}^{-1}(G(m,n), E(m))$. And conversely, each cocycle ε defines, via Hilbert's theorem 90, an element α in $K(m)$ such that $\varepsilon = \alpha^{\sigma_{m,n}-1}$. Then the principal ideal (α) belongs to V'. The kernel, denoted by $P(K_n)O_{K(m)}$, of this map can easily be found to be the principal ideals of $K(m)$ coming from $K(n)$,

$$P(K_n)O_{K(m)} = \{\beta O_{K(m)} \mid \beta \in K(n)\}.$$

We have now completely described an isomorphism

$$\mathbf{H}^{-1}(G(m,n), E(m)) \simeq V'/P(K_n)O_{K(m)}.$$

We need to describe the right hand side in detail. Let $\mathfrak{p}_m$ denote the unique prime ideal of $K(m)$ lying over p. As the extension $K(m)/K(n)$ is unramified outside the prime $\mathfrak{p}_m$, any ideal of $K(m)$ which is prime to $\mathfrak{p}_m$ and invariant under the Galois action of $G(m,n)$ comes from ideals of $K(n)$ and hence

$$V' = \langle \mathfrak{p}_m \rangle \oplus \left\{ aO_{K(m)} \;\middle|\; \begin{array}{l} a \in K(m),\ (\mathfrak{a}, \mathfrak{p}_n) = 1, \\ aO_{K(m)} = \mathfrak{a}O_{K(m)} \text{ for some ideal } \mathfrak{a} \text{ of } K(n) \end{array} \right\}.$$

It follows that

$$\mathbf{H}^{-1}(G(m,n), E(m)) \simeq \langle \mathfrak{p}_m \bmod P(K_n)O_{K(m)} \rangle \oplus \mathrm{Ker}(\tau_{n,m}).$$

We recall that the complex conjugation is denoted by σ_{-1}. By taking the plus parts into account we obtain

$$\mathbf{H}^{-1}(G_{(m,n)}, E_m) \simeq \langle \mathfrak{p}_m^+ \bmod P(K_n)O_{K_m} \rangle \oplus \mathrm{Ker}(\tau_{n,m}^+),$$

where $\mathfrak{p}_m^+$ denotes the prime ideal $((1-\zeta_{p^m})^{(\sigma_{-1}+1)})$ of K_m.

We are ready to show that the first factor $\langle \mathfrak{p}_m^+ \bmod P(K_n)O_{K_m}\rangle$ ($\simeq \mathbb{Z}/p^{m-n}\mathbb{Z}$) on the right hand side above corresponds to $\mathbf{H}^1(G_{(m,n)}, C_m)$. The principal prime

$$\mathfrak{p}_m = (1-\zeta_{p^m})^{(1+\sigma_{-1})}$$

defines a cocycle $(1-\zeta_{p^m})^{(1+\sigma_{-1})(\sigma_{m,n}-1)}$ of $\mathbf{H}^{-1}(G_{(m,n)}, C(m))$, which is a circular unit. We claim that this cocycle generates $\mathbf{H}^{-1}(G_{(m,n)}, C_m)$. Suppose that the order p^j of $(1-\zeta_{p^m})^{(1+\sigma_{-1})(\sigma_{m,n}-1)}$ is less than p^{m-n}, $j < m-n$. Then there is a circular unit c_j in C_m such that

$$((1-\zeta_{p^m})^{p^j})^{(1+\sigma_{-1})(\sigma_{m,n}-1)} = c_j^{\sigma_{m,n}-1}.$$

It follows that $(1-\zeta_{p^m})^{(1+\sigma_{-1})p^j} = c_j\alpha_n$ for some α_n in K_n, which is impossible by a simple ramification argument. Hence we have proved the isomorphisms $\mathbf{H}^1(G_{(m,n)}, C_m) \simeq \langle \mathfrak{p}_m \bmod P(K_n)O_{K_m}\rangle$ and

$$\mathbf{H}^{-1}(G_{(m,n)}, E_m) \simeq \mathbf{H}^1(G_{(m,n)}, C_m) \oplus \operatorname{Ker}(\tau_{n,m}^+).$$

By (3.1), the kernel of $\tau_{n,m}^+$ being isomorphic to $\mathbf{H}^1(G_{(m,n)}, \mathrm{Cl}_m)$, the above equation becomes

$$\mathbf{H}^{-1}(G_{(m,n)}, E_m)/\mathbf{H}^1(G_{(m,n)}, C_m) \simeq \mathbf{H}^1(G_{(m,n)}, \mathrm{Cl}_m).$$

Remark. Notice that the Galois group Δ acts trivially on $\mathbf{H}^1(G_{(m,n)}, C_m)$. In fact for any δ in Δ, $\delta((1-\zeta_{p^m})^{(1+\sigma_{-1})(\sigma_{m,n}-1)})$ is cohomologous to $(1-\zeta_{p^m})^{(1+\sigma_{-1})(\sigma_{m,n}-1)}$. Hence for any nontrivial even character χ we have

$$\mathbf{H}^1(G_{(m,n)}, E_m(\chi)) \simeq \mathbf{H}^1(G_{(m,n)}, \mathrm{Cl}_m(\chi)).$$

It now follows from

$$0 \to \mathbf{H}^1(G_{(m,n)}, C_m) \to \mathbf{H}^1(G_{(m,n)}, E_m) \\ \to \mathbf{H}^1(G_{(m,n)}, E_m/C_m) \to \mathbf{H}^2(G_{(m,n)}, C_m)$$

and $\mathbf{H}^2(G_{(m,n)}, C_n) = 0$ (see Lemma 2.1) that

$$\mathbf{H}^1(G_{(m,n)}, E_m/C_m) \simeq \mathbf{H}^1(G_{(m,n)}, E_m)/\mathbf{H}^1(G_{(m,n)}, C_m) \\ \simeq \mathbf{H}^1(G_{(m,n)}, \mathrm{Cl}_m),$$

and from $\mathbf{H}^0(G_{(m,n)}, C_m) \to \mathbf{H}^0(G_{(m,n)}, E_m) \to \mathbf{H}^0(G_{(m,n)}, E_m/C_m) \to 0$ and $\mathbf{H}^0(G_{(m,n)}, C_n) = 0$ (Lemma 2.1) and (3.2) that

$$\mathbf{H}^2(G_{(m,n)}, E_m/C_m) \simeq \mathbf{H}^0(G_{(m,n)}, E_m) \simeq \mathbf{H}^0(G_{(m,n)}, \mathrm{Cl}_m).$$

We have proved the following theorem which is Theorem 1.1 of the introduction.

Theorem 3.3. *Let P be any p-subgroup of $G(K_m/\mathbb{Q})$. Then*

$$\mathbf{H}^i(P, \mathrm{Cl}_m) \simeq \mathbf{H}^i(P, E_m/C_m) \quad \textit{for all } i \textit{ and } m.$$

For the prime-to-p parts we need more computations. Let L be an abelian number field. As defined in the previous section, let E_L, C_L denote the groups of units and circular units of L respectively. Let $\mathbb{I}_L$ denote the idele group of L. Let $\mathbb{U}_L$ and $\mathbb{J}_L$ denote the subgroup of unit ideles inside $\mathbb{I}_L$ and the idele class group of L respectively. There exist fundamental exact sequences

$$\begin{gathered} 0 \to C_L \to \mathbb{U}_L \to \mathbb{U}_L/C_L \to 0, \\ 0 \to E_L/C_L \to \mathbb{U}_L/C_L \to \mathbb{U}_L/E_L \to 0, \\ 0 \to \mathbb{U}_L/E_L \to \mathbb{J}_L \to \mathrm{Cl}_L \to 0. \end{gathered} \tag{7}$$

They give a sequence

$$\mathbf{H}^0(H,\mathbb{U}_L) \xrightarrow{\beta_1} \mathbf{H}^0(H,\mathbb{U}_L/C_L) \xrightarrow{\beta_2} \mathbf{H}^0(H,\mathbb{U}_L/E_L) \xrightarrow{\beta_3} \mathbf{H}^0(H,\mathbb{J}_L). \tag{8}$$

By class field theory $\mathbf{H}^0(H,\mathbb{U}_L)$ can be identified with the inertia group of $\mathfrak{P}$, and $\mathbf{H}^0(H,\mathbb{J}_L)$ with the group H by (1). With these identifications one immediately sees that $\beta_3\circ\beta_2\circ\beta_1$ is the inclusion map from the decomposition group to the Galois group $G(L/K)$. Now the proof of the following lemma is straightforward.

Lemma 3.4. *Let $L/\mathbb{Q}$ be a totally ramified abelian extension. Then the inclusion map $\beta_3\circ\beta_2\circ\beta_1$ of* (8) *is an isomorphism.*

We now prove the theorem on prime-to-p parts, which is Theorem 1.2 of introduction.

Theorem 3.5. *Let H be a subgroup of $G(K_n/\mathbb{Q})$ with $\#(H)$ prime to p. Then*

$$\mathbf{H}^i(H,\mathrm{Cl}_n) \simeq \mathbf{H}^i(H,E_n/C_n) \quad \textit{for all } i \textit{ and } n.$$

Proof. As in §2 we let $\alpha_1 : \mathbf{H}^1(H,C_n) \to \mathbf{H}^1(H,E_n)$ and $\alpha_2 : \mathbf{H}^1(H,E_n) \to \mathbf{H}^1(H,\mathbb{U}_n))$ be induced from the natural maps. By Lemma 2.2 and (6) it follows that $\alpha_2\circ\alpha_1$ is an isomorphism, so α_1 is injective and α_2 surjective. Applying the isomorphism $\alpha_2\circ\alpha_1$ to the cohomology sequence induced from the short exact sequence $0 \to C_n \to \mathbb{U}_n \to \mathbb{U}_n/C_n \to 0$ and using $\mathbf{H}^2(H,C_n) = 0$ (Lemma 2.1) one obtains

$$\mathbf{H}^1(H,\mathbb{U}_n/C_n) = 0, \qquad \mathbf{H}^0(H,\mathbb{U}_n) \simeq \mathbf{H}^0(H,\mathbb{U}_n/C_n). \tag{9}$$

It follows that β_1 in (8) with $L = K_n$ is an isomorphism and by Lemma 3.4 the composite map $\beta_3\circ\beta_2$ is also an isomorphism. Thus β_2 is injective and β_3 is surjective. Using these properties and (8) and (9), we have isomorphisms

$$\mathbf{H}^0(H,\mathrm{Cl}_n) \simeq \mathbf{H}^1(H,\mathbb{U}_n/E_n) \simeq \mathbf{H}^2(H,E_n/C_n), \tag{10}$$

and exact sequences

$$0 \to \mathbf{H}^0(H,\mathbb{U}_n/C_n) \xrightarrow{\beta_2} \mathbf{H}^0(H,\mathbb{U}_n/E_n) \to \mathbf{H}^1(H,E_n/C_n) \to 0, \tag{11}$$

$$0 \to \mathbf{H}^{-1}(H,\mathrm{Cl}_n) \to \mathbf{H}^0(H,\mathbb{U}_n/E_n) \xrightarrow{\beta_3} \mathbf{H}^0(H,\mathbb{J}_n) \to 0. \tag{12}$$

From (10)–(12) one obtains isomorphisms

$$\mathbf{H}^0(H, \mathrm{Cl}_n) \simeq \mathbf{H}^2(H, E_n/C_n), \qquad \mathbf{H}^{-1}(H, \mathrm{Cl}_n) \simeq \mathbf{H}^1(H, E_n/C_n).$$

As H is cyclic this completes the proof. ∎

As the isomorphisms appearing in our theorems are Galois equivariant, Theorems 3.3 and 3.5 give us the following corollary.

COROLLARY 3.6. *Let G be any subgroup of $G(K_n/\mathbb{Q})$. Then*

$$\mathbf{H}^i(G, \mathrm{Cl}_n) \simeq \mathbf{H}^i(G, E_n/C_n) \quad \text{for all } n \text{ and } i.$$

As defined in the introduction, let K_∞ be the basic $\mathbb{Z}_p$ extension of $K = K_1$, $K_\infty = \bigcup_n K_n$, $G_n = G(K_n/\mathbb{Q})$ and $G_\infty := G(K_\infty/\mathbb{Q})$. Let $E_\infty, C_\infty, \mathrm{Cl}_\infty$ denote the inverse limits of E_n, C_n, Cl_n respectively with respect to the norm maps. By taking inverse limits in Corollary 3.6 we have the following

COROLLARY 3.7. *For all i, we have the $\varprojlim \mathbb{Z}[G_n]$-module isomorphism*

$$\mathbf{H}^i(G_\infty, \mathrm{Cl}_\infty) \simeq \mathbf{H}^i(G_\infty, E_\infty/C_\infty).$$

References

[1] R. Coleman, *On an Archimedean characterization of the circular units*, J. Reine Angew. Math. 356 (1985), 161–173.

[2] P. Cornacchia and C. Greither, *Fitting ideals of class groups of real fields with prime power conductor*, J. Number Theory 73 (1998), 459–471.

[3] R. Gold and J. Kim, *Bases for cyclotomic units*, Compositio Math. 71 (1989), 13–27.

[4] K. Iwasawa, *A note on the group of units of an algebraic number field*, J. Math. Pures Appl. 35 (1956), 189–192.

[5] —, *On the theory of cyclotomic fields*, Ann. of Math. 70 (1959), 530–561.

[6] —, *On $\mathbb{Z}_l$-extensions of algebraic number fields*, ibid. 98 (1973), 246–326.

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

[8] J. Kim, *Cohomology groups of cyclotomic units*, J. Algebra 152 (1992), 514–519.

[9] J. Kim, S. Bae and I. Lee, *Cyclotomic units in $\mathbb{Z}_p$-extensions*, Israel J. Math. 75 (1991), 161–165.

[10] V. A. Kolyvagin, *Euler systems*, in: The Grothendieck Festschrift, Vol. 2, Birkhäuser, 1990, 435–483.

[11] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of Number Fields*, Grundlehren Math. Wiss. 323, Springer, 2000.

[12] K. Rubin, *The main conjecture*, Appendix to the second edition of S. Lang, *Cyclotomic Fields*, Springer, 1990.

[13] —, *Euler Systems*, Ann. of Math. Stud. 147, Princeton Univ. Press, 2000.

[14] R. Schoof, *Class numbers of real cyclotomic fields of prime conductor*, Math. Comp. 72 (2003), 913–937.

[15] J.-P. Serre, *Local Fields*, Grad. Texts in Math. 67, Springer, 1979.

[16] W. Sinnott, *On the Stickelberger ideal and the circular units of a cyclotomic field*, Ann. of Math. 108 (1978), 107–134.

[17] —, *On the Stickelberger ideal and the circular units of an abelian field*, Invent. Math. 62 (1980), 181–234.

Department of Mathematics
Yonsei University
134 Sinchon-Dong, Seodaemun-Gu
Seoul 120-749, South Korea
E-mail: sgseo@yonsei.ac.kr

Received on 26.1.2005
and in revised form on 27.9.2005 (4927)