BULL. AUSTRAL. MATH. SOC. 11R23, 11R29, 11R11
VOL. 57 (1998) [261–274]

CLASS NUMBERS OF REAL QUADRATIC FIELDS

JAE MOON KIM

Let $k = \mathbb{Q}(\sqrt{m})$ be a real quadratic field. It is well known that if 3 divides the class number of k, then 3 divides the class number of $\mathbb{Q}(\sqrt{-3m})$, and thus it divides $B_{1,\chi\omega^{-1}}$, where χ and ω are characters belonging to the fields k and $\mathbb{Q}(\sqrt{-3})$ respectively. In general, the main conjecture of Iwasawa theory implies that if an odd prime p divides the class number of k, then p divides $B_{1,\chi\omega^{-1}}$, where ω is the Teichmüller character for p.

The aim of this paper is to examine its converse when p splits in k. Let k_∞ be the $\mathbb{Z}_p$-extension of $k = k_0$ and h_n be the class number of k_n, the nth layer of the $\mathbb{Z}_p$-extension. We shall prove that if $p \mid B_{1,\chi\omega^{-1}}$, then $p \mid h_n$ for all $n \geqslant 1$. In terms of Iwasawa theory, this amounts to saying that if M_∞/k_∞ is nontrivial, then L_∞/k_∞ is nontrivial, where M_∞ and L_∞ are the maximal abelian p-extensions unramified outside p and unramified everywhere respectively.

1. INTRODUCTION

Fix a square free positive integer m and let $k = \mathbb{Q}(\sqrt{m})$. Class numbers of these real quadratic fields have been studied for a long time. Two outstanding formulas related to class numbers are the analytic (classical or p-adic) class number formula [**7**] and the index theorem of circular units discovered by Sinnott [**6**].

In this paper we study the class number of k by examining the p-divisibility of the class number for each prime p. When p=2, the answer is well known and can be easily checked either by considering the genus field of k or by using cohomological arguments: if the discriminant of k has at least three distinct prime divisors, then the class number is divisible by 2. Note that the converse of this statement is not true. For instance, the class number of $\mathbb{Q}(\sqrt{85})$ is 2 and that of $\mathbb{Q}(\sqrt{21})$ is 1. Both of these fields have discriminants with exactly two prime divisors.

The answer for p=3 is also known [**5, 7**]: if 3 divides the class number of k, then 3 divides the class number of $\mathbb{Q}(\sqrt{-3m})$. This can be proved either by applying the p-adic class number formular or by using the Kummer pairing as Scholz did [**5**]. The

Received 31st July, 1997
This work was partially supported by the Basic Science Research Institute program, Ministry of Education, Korea, #BSRI-96-1414, and was completed while the author was visiting the Ohio State University during the sabbatical year 1996-1997.

converse of this does not hold either. For example, the class number of $\mathbb{Q}(\sqrt{85})$ is 2, but that of $\mathbb{Q}(\sqrt{-255})$ is 12. Let χ be the nontrivial character belonging to k and ω be the Teichmüller character for $p=3$. Then $\chi\omega^{-1}$ belongs to the field $\mathbb{Q}(\sqrt{-3m})$ and $-B_{1,\chi\omega^{-1}}$ is the class number of $\mathbb{Q}(\sqrt{-3m})$. Thus we can rephrase the statement as 3 divides $B_{1,\chi\omega^{-1}}$ if 3 divides the class number of k.

This can be generalised to an arbitrary odd prime p by using the main conjecture of Iwasawa theory. Let ω be the Teichmüller character for p. Let k_∞ be the $\mathbb{Z}_p$-extension of k and M_∞ be its maximal abelian p-extension unramified outside p. Let f_χ be the Iwasawa power series in $\Lambda = \mathbb{Z}_p[[T]]$ corresponding to the p-adic L-function $L_p(s,\chi)$. Then by the main conjecture, which is a theorem now [**4**], $\mathrm{Gal}(M_\infty/k_\infty)$ is pseudo-isomorphic to $\Lambda/(f_\chi)$ as a Λ-module. We also have

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

Thus if p does not divide $B_{1,\chi\omega^{-1}}$, then f_χ is a unit in Λ. Hence $\mathrm{Gal}(M_\infty/k_\infty)$ is trivial, since it has no nonzero finite Λ-submodules (see [**3**, appendix]). Therefore $\mathrm{Gal}(L_\infty/k_\infty)$ is also trivial, where L_∞ is the maximal unramified Abelian p-extension of k_∞. Thus p does not divide the class number of k. To summarise, we proved:

Theorem 1. *Let $k=\mathbb{Q}(\sqrt{m})$ and p be an odd prime. If p divides the class number of k, then p divides $B_{1,\chi\omega^{-1}}$.*

The aim of this paper is to discuss the converse of theorem 1. According to the previous example for $p=3$, the converse cannot be true in general. However, we have the following result when p splits in k. For each $n \geqslant 0$, let h_n be the class number of k_n, the nth layer of the $\mathbb{Z}_p$-extension k_∞ of k.

Theorem 4. *Suppose an odd prime p splits in $k = \mathbb{Q}(\sqrt{m})$. If p divides $B_{1,\chi\omega^{-1}}$, then p divides h_n for all $n \geqslant 1$.*

For the proof of Theorem 4, we shall use circular units defined by Sinnott and his index Theorem [**6**]. In Section 2, we briefly review his definition of circular units and compute cohomology groups of them in the $\mathbb{Z}_p$-extension. In Section 3, we shall assume that p splits in k, so there are two prime ideals $\wp_0$ and $\widetilde{\wp}_0$ above p in k. Let $\wp_n$ and $\widetilde{\wp}_n$ be the prime ideals of k_n above $\wp_0$ and $\widetilde{\wp}_0$ respectively. We shall see that every circular unit δ_n of k_n whose norm to k_0 equals 1 has the property that $\delta_n = \alpha_n^{\sigma-1}$ for some $\alpha_n \in k_n$ satisfying $(\alpha_n) = \wp_n^{g_n}\widetilde{\wp}_n^{\widetilde{g}_n}$ for some integers g_n and $\widetilde{g}_n$, where σ is a topological generator of the Galois group $\Gamma = \mathrm{Gal}(k_\infty/k)$. Then we pick a special δ_n and show that

$$g_n - \widetilde{g}_n \equiv \pm\sqrt{d}B_{1,\chi\omega^{-1}} \bmod p\mathbb{Z}_p,$$

where d is the conductor of k. Finally, we apply this congruence to prove Theorem 4.

2. Circular Units

Let F be an abelian field. For each $n > 2$, let $F_n = F \cap \mathbb{Q}(\zeta_n)$ and $C_{F_n} = N_{\mathbb{Q}(\zeta_n)/F_n}(C_{\mathbb{Q}(\zeta_n)})$, where $C_{\mathbb{Q}(\zeta_n)}$ is the group of the cyclotomic units of $\mathbb{Q}(\zeta_n)$ in the usual sense. We define the group of circular units C_F of F as the multiplicative subgroup of $F^\times$ generated by C_{F_n} together with -1 (see [**6**]). 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. For example, when $F = k = \mathbb{Q}(\sqrt{m})$, $C_k = \langle N_{\mathbb{Q}(\zeta_d)/k}(C_{\mathbb{Q}(\zeta_d)}), -1\rangle$, where d is the conductor of k (d will always mean the conductor of k throughout this paper). To see this, first observe that $k \cap \mathbb{Q}(\zeta_n)$ is either $\mathbb{Q}$ or k. If $k \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$, then $C_{k_n} = \{1\}$. Otherwise, $\mathbb{Q}(\zeta_n)$ contains $\mathbb{Q}(\zeta_d)$ as a subfield and thus $N_{\mathbb{Q}(\zeta_n)/k}(C_{\mathbb{Q}(\zeta_n)})$ is contained in $N_{\mathbb{Q}(\zeta_d)/k}(C_{\mathbb{Q}(\zeta_d)})$.

Fix an odd prime p with $(p, m) = 1$, and let $k_\infty = \bigcup_{n \geqslant 0} k_n$ be the $\mathbb{Z}_p$-extension of $k = k_0 = \mathbb{Q}(\sqrt{m})$. For each $n \geqslant 0$, we denote the group of circular units of k_n by C_n. It is not hard to show that

$$(*) \qquad C_n = C_{n-1}\left(N_{\mathbb{Q}(\zeta_{p^{n+1}d})/k_n}(C_{\mathbb{Q}(\zeta_{p^{n+1}d})})\right)\left(N_{\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}_n}(C_{\mathbb{Q}(\zeta_{p^{n+1}})})\right),$$

where $\mathbb{Q}_n$ is the subfield of $\mathbb{Q}(\zeta_{p^{n+1}})$ whose degree over $\mathbb{Q}$ is p^n. Thus the generators of C_n are given so explicitly that we can compute the cohomology groups of circular units in the $\mathbb{Z}_p$-extension. Another feature of the circular units is the following index theorem discovered by Sinnott [**6**].

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.*

Before we compute the cohomology groups of C_n, we set up some notation. For each integer $s \geqslant 1$, we choose a primitive sth root ζ_s of 1 so that $\zeta_t^{t/s} = \zeta_s$ if $s \mid t$. Let $K = \mathbb{Q}(\zeta_d)$, $F = \mathbb{Q}(\zeta_p)$ and $K' = \mathbb{Q}(\zeta_{pd})$. We denote their cyclotomic $\mathbb{Z}_p$-extensions by K_∞, F_∞, and K'_∞. Let σ be the topological generator of the Galois group $\Gamma = \mathrm{Gal}\left(K'_\infty/K'\right)$ which maps ζ_{p^n} to $\zeta_{p^n}^{1+p}$ for all $n \geqslant 1$. Restrictions of σ to various subfields are also denoted by σ. Let $\Delta = \mathrm{Gal}(K/k)$, $\overline{\Delta} = \mathrm{Gal}(K/\mathbb{Q})$ and $\Delta_k = \mathrm{Gal}(k/\mathbb{Q}) = \{id, \rho\}$. Elements of Δ or $\overline{\Delta}$ will be denoted by τ's. Let R be the set of all roots of 1 in $\mathbb{Z}_p$, that is, $R = \{\omega \in \mathbb{Z}_p \mid \omega^{p-1} = 1\}$. Then R can be regarded as the Galois group $\mathrm{Gal}(F/\mathbb{Q})$ or any Galois group isomorphic to it such as $\mathrm{Gal}(F_n/\mathbb{Q}_n)$. For $m > n$, let $G_{m,n}$ be the Galois group $\mathrm{Gal}\left(K'_m/K'_n\right)$ and $N_{m,n}$ be the norm map $N_{K'_m/K'_n}$ from K'_m to K'_n. We shall abbreviate $G_{m,0}$ and $N_{m,0}$ to G_m and N_m respectively. $G_{m,n}$ will also mean the Galois groups $\mathrm{Gal}(k_m/k_n)$, $\mathrm{Gal}(F_m/F_n)$ and $\mathrm{Gal}(\mathbb{Q}_m/\mathbb{Q}_n)$. Similarly $N_{m,n}$ will have various meanings. Finally we fix a generator ψ_n of the character group of $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$

https://doi.org/10.1017/S0004972700031646 Published online by Cambridge University Press

such that $\psi_n(\sigma) = \zeta_{p^n}$. Thus ψ_n is an even character of order p^n with conductor p^{n+1} such that $\psi_n^p = \psi_{n-1}$.

Theorem 2. *Suppose p splits in k. For $m > n \geqslant 0$, we have the following.*

$$C_m^{G_{m,n}} = C_n, \tag{1}$$

$$\widehat{H}^0(G_{m,n}, C_m) \simeq \mathbb{Z}/p^{m-n}\mathbb{Z}, \tag{2}$$

$$\widehat{H}^{-1}(G_{m,n}, C_m) \simeq \left(\mathbb{Z}/p^{m-n}\mathbb{Z}\right)^2. \tag{3}$$

Proof of (1): It is clear that $C_n \subset C_m^{G_{m,n}}$. To prove the converse, we invoke a theorem of Ennola on relations of cyclotomic units [**1**]: If a cyclotomic unit $\xi = \prod_{1 \leqslant a < n} (1 - \zeta_n^a)^{x_a}$ in $\mathbb{Q}(\zeta_n)$ is a root of 1 for some integers x_a, then $Y(\theta, \xi) = 0$ for every even character θ of conductor n, where $Y(\theta, \xi) = \sum_{1 \leqslant a < n} \theta(a) x_a$.

To prove $C_m^{G_{m,n}} \subset C_n$, it is enough to check the inclusion when $m = n + 1$. Suppose that $u \in C_{n+1}$ is fixed by $G_{n+1,n}$, that is $u^{\sigma^{p^n}} = u$. By $(*)$, $u = u_n v_{n+1}$ for some $u_n \in C_n$ and $v_{n+1} \in N_{K'_{n+1}/k_{n+1}}(C_{K'_{n+1}}) N_{F_{n+1}/\mathbb{Q}_{n+1}}(C_{F_{n+1}})$. Since $u_n^{\sigma^{p^n}} = u_n$, we have $v_{n+1}^{\sigma^{p^n}} = v_{n+1}$. Thus we may assume $u_n = 1$. Then we can write u as

$$u = \prod_{\substack{0 \leqslant l < p^n \\ 0 \leqslant k < p}} \left(\prod_{\substack{\omega \in R \\ \tau \in \Delta}} \left(\zeta_{p^{n+2}}^{\sigma^{l+kp^n}\omega} - \zeta_d^{\tau} \right)^{a_{l,k}} \left(\zeta_{p^{n+2}}^{\sigma^{l+kp^n}\omega} - \zeta_d^{\rho\tau} \right)^{b_{l,k}} \prod_{\omega \in R} \left(\zeta_{p^{n+2}}^{\sigma^{l+kp^n}\omega} - 1 \right)^{c_{l,k}} \right),$$

for some integers $a_{l,k}, b_{l,k}$ and $c_{l,k}$.

We apply Ennola's theorem to the relation $u^{\sigma^{p^n}-1} = 1$ with characters of the form $\psi_{n+1}^j \chi$ for $0 < j < p^{n+1}$, $(j,p) = 1$. Notice that

$$Y\left(\psi_{n+1}^j \chi, \prod_{\substack{\omega \in R \\ \tau \in \Delta}} \left(\zeta_{p^{n+2}}^{\sigma^{l+kp^n}\omega} - \zeta_d^{\tau} \right) \right) = (p-1) \frac{\phi(d)}{2} \psi_{n+1}^j \left(d\sigma^{l+kp^n} \right),$$

$$Y\left(\psi_{n+1}^j \chi, \prod_{\substack{\omega \in R \\ \tau \in \Delta}} \left(\zeta_{p^{n+2}}^{\sigma^{l+kp^n}\omega} - \zeta_d^{\rho\tau} \right) \right) = -(p-1) \frac{\phi(d)}{2} \psi_{n+1}^j \left(d\sigma^{l+kp^n} \right),$$

and

$$Y\left(\psi_{n+1}^j \chi, \prod_{\omega \in R} \left(\zeta_{p^{n+2}}^{\sigma^{l+kp^n}\omega} - 1 \right) \right) = 0.$$

Thus we have

$$\sum_{\substack{0 \leqslant l < p^n \\ 0 \leqslant k < p}} (a_{l,k} - b_{l,k}) \, \psi_{n+1}^j \left(\sigma^{l+kp^n} \right) = 0.$$

By letting j run through all the integers $0 < j < p^{n+1}$ with $p \nmid j$, we have a system of linear equations $AX = \mathbb{O}$, where A is a $\left(p^{n+1} - p^n\right) \times p^{n+1}$ matrix with entries $\psi_{n+1}^j\left(\sigma^{l+kp^n}\right)$ and $X = (\ldots, a_{l,k} - b_{l,k}, \ldots)^t$. Since rank $A = p^{n+1} - p^n$, the rank of solutions must be p^n. And we can exhibit p^n independent solutions explicitly. Namely, for each s, $0 \leqslant s < p^n$, let $X_s = (\ldots, f_{l,k}, \ldots)^t$ be such that

$$f_{l,k} = \begin{cases} 0 & \text{if } l \neq s \\ 1 & \text{if } l = s. \end{cases}$$

Then X_s is a solution since $\sum\limits_{0 \leqslant k < p} \psi_{n+1}^j\left(\sigma^{s+kp^n}\right) = 0$ for all j, and $\{X_s\}_{0 \leqslant s < p^n}$ is clearly linearly independent. Therefore if $X = (\ldots, a_{l,k} - b_{l,k}, \ldots)^t$ is a solution of $AX = \mathbb{O}$, then $a_{s,k} - b_{s,k}$ is independent of k for all s, $0 \leqslant s < p^n$, say $a_{s,k} - b_{s,k} = e_s$. Then we can write u as

$$u = \prod_{l,k,\omega,\tau} \left(\zeta_{p^{n+2}}^{\sigma^{l+kp^n}\omega} - \zeta_d^\tau\right)^{e_l} \prod_{\substack{l,k,\omega \\ \nu \in \overline{\Delta}}} \left(\zeta_{p^{n+2}}^{\sigma^{l+kp^n}\omega} - \zeta_d^\nu\right)^{b_{l,k}} \prod_{l,k,\omega} \left(\zeta_{p^{n+2}}^{\sigma^{l+kp^n}\omega} - 1\right)^{c_{l,k}}.$$

In this expression, the first product is in C_n, since $\prod\limits_{k,\omega,\tau} \left(\zeta_{p^{n+2}}^{\sigma^{l+kp^n}\omega} - \zeta_d^\tau\right)$ is in C_n. The second and the third products in the expression, on the other hand, are circular units of $\mathbb{Q}_{n+1}$. Thus we can write u as $u = v_n v$ for some $v_n \in C_n$ and $v \in C_{\mathbb{Q}_{n+1}}$, and v satisfies $v^{\sigma^{p^n}} = v$. Now write v as $v = \prod\limits_{l,k,\omega} \left(\zeta_{p^{n+2}}^{\sigma^{l+kp^n}\omega} - 1\right)^{d_{l,k}}$ and apply Ennola's Theorem to $v^{\sigma^{p^n} - 1} = 1$ with characters of the form ψ_{n+1}^j, $0 \leqslant j < p^{n+1}$, $p \nmid j$. After a similar computation, we see that v is a circular unit in $\mathbb{Q}_n$, hence $u \in C_n$. This proves (1). □

PROOF OF (2): For each $l \geqslant 0$, let $\delta_l = \prod\limits_{\substack{\omega \in R \\ \tau \in \Delta}} \left(\zeta_{p^{l+1}}^\omega - \zeta_d^\tau\right)$ and $\pi_l = \prod\limits_{\omega \in R} \left(\zeta_{p^{l+1}}^\omega - 1\right)$.

Then δ_l, $\pi_l^{\sigma - 1} \in C_l$. Note that for $m > n \geqslant 0$,

$$N_{m,n}(\delta_m) = \prod_{\substack{\omega \in R \\ \tau \in \Delta}} \left(\zeta_{p^{n+1}}^\omega - \zeta_d^{p^{m-n}\tau}\right) = \delta_n,$$

since p splits in k and thus τ_p (Frobenius automorphism of $\mathbb{Q}(\zeta_d)$ for p) permutes Δ. In particular,

$$N_l(\delta_l) = \delta_0 = \prod_{\omega,\tau} \left(\zeta_p^\omega - \zeta_d^\tau\right) = \frac{\prod_\tau \left(1 - \zeta_d^{p\tau}\right)}{\prod_\tau \left(1 - \zeta_d^\tau\right)} = 1.$$

Also note that, for any $u \in C_n$, we can write u as $u = u_0 u_1 \cdots u_n$, where $u_0 \in C_0$ and for $k \geqslant 1$, u_k is of the form

$$(**) \qquad u_k = \delta_k^{\sum_{\substack{0\leqslant i<p^k \\ 0\leqslant j\leqslant 1}} a_{i,j}\sigma^i\rho^j} \pi_k^{(\sigma-1)\sum_{0\leqslant i<p^k} c_i\sigma^i}.$$

First we claim that $C_n = C_0 N_{m,n} C_m$. Clealy $C_0 N_{m,n} C_m$ is contained in C_n. To check the converse, let $u = u_0 u_1 \cdots u_n$, where u_k is as in $(**)$ for $k \geqslant 1$. Let $\sigma_s = \sigma^{p^s}$. Then $N_{m,k} = \sum_{0\leqslant i<p^{m-k}} \sigma_k^i$. For each i, $0 \leqslant i < p^{m-k}$, write $i = ap^{n-k} + b$ with $0 \leqslant a < p^{m-n}$, $0 \leqslant b < p^{n-k}$. Then

$$N_{m,k} = \sum_{a,b} \sigma_k^{ap^{n-k}+b} = \left(\sum_a \sigma_k^{ap^{n-k}}\right)\left(\sum_b \sigma_k^b\right) = \left(\sum_a \sigma_n^a\right)\left(\sum_b \sigma_k^b\right) = \left(\sum_b \sigma_k^b\right) N_{m,n}.$$

Therefore

$$\delta_k = N_{m,k}\delta_m = N_{m,n}\left(\delta_m^{\sum_b \sigma_k^b}\right) \text{ and } \pi_k^{\sigma-1} = N_{m,n}\left(\pi_m^{(\sigma-1)\sum_b \sigma_k^b}\right).$$

Hence $u_k \in N_{m,n} C_m$ for each k, $1 \leqslant k \leqslant n$.

Next we show that $C_0 \cap N_{m,n} C_m = C_0^{p^{m-n}}$. Obviously, $C_0^{p^{m-n}} \subset C_0 \cap N_{m,n} C_m$. For the converse, suppose $u \in C_0 \cap N_{m,n} C_m$ and write $u = N_{m,n}(v)$ for some $v \in C_m$. As before, we can write $v = v_0 v_1 \cdots v_m$ with v_k of the form in $(**)$ for $k \geqslant 1$. By taking N_n, we have $N_n(u) = N_n\big(N_{m,n}(v)\big) = N_m(v)$. Since $N_m(v_k) = N_k(v_k)^{p^{m-k}} = 1$ for $k \geqslant 1$, we obtain $u^{p^n} = v_0^{p^m}$. Thus $u^{-1} v_0^{p^{m-n}}$ is a p^nth root of 1 in k, hence equals 1. Therefore $u = v_0^{p^{m-n}} \in C_0^{p^{m-n}}$. Thus

$$\begin{aligned} \widehat{H}^0(G_{m,n}, C_m) &= C_n / N_{m,n} C_m = C_0 N_{m,n} C_m / N_{m,n} C_m \\ &= C_0 / C_0 \cap N_{m,n} C_m = C_0 / C_0^{p^{m-n}}. \end{aligned}$$

Note that C_0 is generated by $\prod_{\tau\in\Delta}(1-\zeta_d^\tau)$, $\prod_{\tau\in\Delta}(1-\zeta_d^{\rho\tau})$ and -1. But $\prod_{\tau\in\Delta}(1-\zeta_d^\tau)$ $\prod_{\tau\in\Delta}(1-\zeta_d^{\rho\tau}) = 1$. Hence

$$\widehat{H}^0(G_{m,n}, C_m) \simeq \mathbb{Z}/p^{m-n}\mathbb{Z}$$

https://doi.org/10.1017/S0004972700031646 Published online by Cambridge University Press

and is generated by $\prod_{\tau\in\Delta}(1-\zeta_d^\tau)$. ∎

Proof of (3): Let δ_n and π_n be as in the proof of (3). We saw that $N_n(\delta_n) = N_n(\pi_n^{\sigma-1}) = 1$. We shall prove

$$(***)\qquad \text{if } \delta_n^a\pi_n^{(\sigma-1)b}\in C_n^{\sigma-1},\text{ then } a\equiv b\equiv 0 \bmod p^n.$$

This would imply $\widehat{H}^{-1}(G_n,C_n)\simeq(\mathbb{Z}/p^n\mathbb{Z})^2$ and $\widehat{H}^{-1}(G_n,C_n)$ is generated by δ_n and $\pi_n^{\sigma-1}$ since the Herbrand quotient for C_n is p^n and $\widehat{H}^{-1}(G_n,C_n)$ is annihilated by p^n. Then from the inflation- restriction sequence

$$0\to H^1\left(G_n,C_m^{G_{m,n}}\right)\xrightarrow{inf}H^1(G_m,C_m)\xrightarrow{res}H^1(G_{m,n},C_m),$$

we obtain

$$0\to(\mathbb{Z}/p^n\mathbb{Z})^2\to(\mathbb{Z}/p^m\mathbb{Z})^2\to H^1(G_{m,n},C_m)$$

since the first cohomology group H^1 is isomorphic to $\widehat{H}^{-1}$. Thus $(\mathbb{Z}/p^{m-n}\mathbb{Z})^2$ injects into $H^1(G_{m,n},C_m)$. But we already know that its order is $p^{2(m-n)}$. Therefore $\widehat{H}^{-1}(G_{m,n},C_m)\simeq(\mathbb{Z}/p^{m-n}\mathbb{Z})^2$.

It remains to show $(***)$. We shall prove this by induction on n. Suppose that $\delta_1^a\pi_1^{(\sigma-1)b}=u^{\sigma-1}$ for some $u\in C_1$. As before we can write $u=u_0u_1$, where $u_0\in C_0$ and u_1 is of the form in $(**)$. So we have $\delta_1^a\pi_1^{(\sigma-1)b}=u_1^{\sigma-1}$, where $u_1=\delta_1^{\sum a_{i,j}\sigma^i\rho^j}\pi_1^{(\sigma-1)\sum c_i\sigma^i}$. We apply Ennola's Theorem with the character $\psi_1\chi$ to this equation. Then we have

$$aY(\psi_1\chi,\delta_1)=(\psi_1(\sigma)-1)\left(\sum_{i,j}a_{i,j}\psi_1\chi(\sigma^i\rho^j)\right)Y(\psi_1\chi,\delta_1).$$

Since

$$Y(\psi_1\chi,\delta_1)=\sum_{\omega,\tau}\psi_1\chi(-\omega d+p^2\tau)=(p-1)\frac{\phi(d)}{2}\psi_1(d)\neq 0,$$

we get

$$a=(\psi_1(\sigma)-1)\left(\sum_{i,j}a_{i,j}\psi_1\chi(\sigma^i\rho^j)\right).$$

Note that $\sum a_{i,j}\psi_1\chi(\sigma^i\rho^j)$ is integral. Therefore $a\equiv 0 \bmod (\zeta_p-1)$, hence mod p. Since $N_1\delta_1=1$,

$$\delta_1^p=\frac{\delta_1^p}{N_1\delta_1}=\delta_1^{\sum_{0\leqslant i<p}(1-\sigma^i)}=\delta_1^{\left(\sum(1-\sigma^i)/(\sigma-1)\right)(\sigma-1)}\in C_1^{\sigma-1}.$$

https://doi.org/10.1017/S0004972700031646 Published online by Cambridge University Press

Then from $\delta_1^a\pi_1^{(\sigma-1)b} = u^{\sigma-1}$, we obtain $\pi_1^{(\sigma-1)b} = v^{\sigma-1}$ for some $v \in C_1$. This implies that $\pi_1^b = v\alpha_0$ for some $\alpha_0 \in k$. As ideals, we have $(\pi_1^b) = (\alpha_0)$, which is impossible unless $b \equiv 0 \bmod p$ since primes of k above p ramify totally in k_1.

Now we prove $(***)$ for n, assuming the result for $n-1$. Suppose $\delta_n^a\pi_n^{(\sigma-1)b} = u_n^{\sigma-1}$ for some $u_n \in C_n$. By applying $N_{n,n-1}$ to both sides, we have $\delta_{n-1}^a\pi_{n-1}^{(\sigma-1)b} = (N_{n,n-1}u_n)^{\sigma-1} \in C_{n-1}^{\sigma-1}$. Then by the induction hypothesis, $a \equiv b \equiv 0 \bmod p^{n-1}$. Let $a = p^{n-1}a_1$ and $b = p^{n-1}b_1$. Note that

$$\delta_n^{p^{n-1}} = (N_{n,1}\delta_n)\frac{\delta_n^{p^{n-1}}}{(N_{n,1}\delta_n)} = \delta_1\left(\delta_n^{\sum_{0\leqslant k<p^{n-1}}(1-\sigma^{kp})/(\sigma-1)}\right)^{\sigma-1}$$

and

$$\pi_n^{p^{n-1}(\sigma-1)} = \pi_1^{\sigma-1}\left(\pi_n^{\sum_k(1-\sigma^{kp})}\right)^{\sigma-1}.$$

Therefore $\delta_n^a\pi_n^{(\sigma-1)b} = u_n^{\sigma-1}$ reads $\delta_1^{a_1}\pi_1^{(\sigma-1)b} = v_n^{\sigma-1}$ for some $v_n \in C_n$. By the injectivity of the inflation map

$$\widehat{H}^{-1}(G_1, C_1) \simeq H^1(G_1, C_1) \xrightarrow{inf} H^1(G_n, C_n) \simeq \widehat{H}^{-1}(G_n, C_n),$$

$\delta_1^{a_1}\pi_1^{(\sigma-1)b_1}$ must be in $C_1^{\sigma-1}$. Thus $a_1 \equiv b_1 \equiv 0 \bmod p$ and so $a \equiv b \equiv 0 \bmod p^n$. This finishes the proof. ∎

REMARK. In the proof of (1), we did not use the splitting of p. So (1) is still valid even when p remains inert in k. If p remains inert in k, the Frobenius automorphism τ_p of $\mathbb{Q}(\zeta_d)$ for p is not in Δ. Thus

$$\prod_{\tau\in\Delta}(1-\zeta_d^\tau)^{-2} = \prod_{\tau\in\Delta}\frac{1-\zeta_d^{p\tau}}{1-\zeta_d^\tau} = \prod_{\omega,\tau}(\zeta_p^\omega - \zeta_d^\tau) = \delta_0 = N_1(\delta_1^{\tau_p}).$$

Therefore $\prod_{\tau\in\Delta}(1-\zeta_d^\tau) \in N_1(C_1)$. With this additional information, one can modify the proof of (2) to obtain:

THEOREM 2′. *Suppose p remains inert in k. For $m > n \geqslant 0$, we have*

$$(1') \qquad C_m^{G_{m,n}} = C_n,$$

$$(2') \qquad \widehat{H}^0(G_{m,n}, C_m) = \{0\},$$

$$(3') \qquad \widehat{H}^{-1}(G_{m,n}, C_m) \simeq \mathbb{Z}/p^{m-n}\mathbb{Z}.$$

3. Main results

Let p be an odd prime which splits in k and let $\delta_n = \prod_{\omega\in R,\tau\in\Delta}\left(\zeta_{p^{n+1}}^{\omega} - \zeta_d^{\tau}\right)$, $\pi_n = \prod_{\omega\in R}\left(\zeta_{p^{n+1}}^{\omega} - 1\right)$ as before. We know that δ_n and $\pi_n^{\sigma-1}$ generate $\widehat{H}^{-1}(G_n, C_n)$. Let E_n' be the group of p-units of k_n.

Lemma 1. *The homomorphism $\widehat{H}^{-1}(G_n, C_n) \to \widehat{H}^{-1}\left(G_n, E_n'\right)$ induced by the inclusion $C_n \to E_n'$ is a zero map.*

Proof: Since G_n is cyclic, it is enough to show that $H^1(G_n, C_n) \to H^1\left(G_n, E_n'\right)$ is a zero map. By taking limits under the inflation maps, we have a homomorphism $H^1(\Gamma, C_\infty) \longrightarrow H^1\left(\Gamma, E_\infty'\right)$, where $C_\infty = \bigcup_{n\geqslant 0} C_n$ and $E_\infty' = \bigcup_{n\geqslant 0} E_n'$. By Theorem 2, $H^1(\Gamma, C_\infty) \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^2$. On the other hand, $H^1\left(\Gamma, E_\infty'\right)$ is a finite group [**2**]. Since $(\mathbb{Q}_p/\mathbb{Z}_p)^2$ cannot have a nontrivial finite quotient, the map $H^1(\Gamma, C_\infty) \to H^1\left(\Gamma, E_\infty'\right)$ is a zero map. Then the lemma follows from the injectivity of the inflation maps. $\square$

Thus $\delta_n = \alpha_n^{\sigma-1}$ for some p-unit α_n in k_n by the lemma. Let $\wp_n$ and $\widetilde{\wp}_n$ be the prime ideals of k_n above p as in the introduction. Then $(\alpha_n) = \wp_n^{g_n}\widetilde{\wp}_n^{\widetilde{g}_n}$ for some integers g_n and $\widetilde{g}_n$. If $\delta_n = \alpha_n^{\sigma-1} = \beta_n^{\sigma-1}$ for some other p-unit β_n, then $\alpha_n = \beta_n\alpha_0$ for some p-unit $\alpha_0 \in k_0$. Thus g_n and $\widetilde{g}_n$ are determined uniquely modulo p^n by δ_n since $\wp_0$ and $\widetilde{\wp}_0$ ramify totally in k_n. If $\delta_m = \alpha_m^{\sigma-1}$ with $(\alpha_m) = \wp_m^{g_m}\widetilde{\wp}_m^{\widetilde{g}_m}$ for $m > n$, then $\delta_n = N_{m,n}\delta_m = (N_{m,n}\alpha_m)^{\sigma-1}$ and $(N_{m,n}\alpha_m) = \wp_n^{g_m}\widetilde{\wp}_n^{\widetilde{g}_m}$. Therefore $g_m \equiv g_n$, $\widetilde{g}_m \equiv \widetilde{g}_n \bmod p^n$.

Theorem 3. *Let $\delta_n = \alpha_n^{\sigma-1}$ with $(\alpha_n) = \wp_n^{g_n}\widetilde{\wp}_n^{\widetilde{g}_n}$. Then $g_n - \widetilde{g}_n \equiv g_1 - \widetilde{g}_1 \equiv \pm\sqrt{d}B_{1,\chi\omega^{-1}} \bmod p\mathbb{Z}_p$.*

Remark. The signature in the theorem depends on the embedding of $\overline{\mathbb{Q}}$ into $\overline{\mathbb{Q}_p}$. Fix an embedding ι once and for all and assume that under this embedding, k_n is completed at $\wp_n$ rather than $\widetilde{\wp}_n$. We denote $\iota(\zeta_d)$ just by ζ_d. Let $p(\tau)$ be the integer modulo d corresponding to τ under the isomorphism $\overline{\Delta} \simeq (\mathbb{Z}/d\mathbb{Z})^\times$. Then $\iota(\zeta_d^\tau) = \iota\left(\zeta_d^{p(\tau)}\right) = \iota(\zeta_d)^{p(\tau)} = \zeta_d^{p(\tau)}$. Again we simply write ζ_d^τ for $\iota(\zeta_d^\tau) = \zeta_d^{p(\tau)}$ in $\overline{\mathbb{Q}_p}$.

Before we prove Theorem 3, we need the following proposition which is valid even when p remains inert in k.

Proposition 1.

$$\sum_{\substack{\omega\in R\\ \tau\in\overline{\Delta}}} \chi(\tau)\log_p\left(\zeta_{p^2}^{\omega} - \zeta_d^{\tau}\right) \equiv -\chi(p)\sqrt{d}B_{1,\chi\omega^{-1}} \bmod \left(\zeta_{p^2} - 1\right)^{p-1}.$$

PROOF: For $0 \leqslant i < p$, $0 \leqslant k < p$, let

$$T_i = \sum_{\omega \in R, \tau \in \overline{\Delta}} \chi(\tau) \log_p \left(\zeta_{p^2}^{\sigma^i \omega} - \zeta_d^{\tau}\right),$$

$$S_k = \sum_{0 \leqslant i < p} \psi^k(\sigma^i) t_I,$$

where $\psi = \psi_1$. When $k = 0$,

$$\begin{aligned}
S_0 &= \sum_{0 \leqslant i < p} T_i \\
&= \sum_{\tau \in \overline{\Delta}} \chi(\tau) \sum_{\substack{0 \leqslant i < p \\ \omega \in R}} \log_p \left(\zeta_{p^2}^{\sigma^i \omega} - \zeta_d^{\tau}\right) \\
&= \sum_{\tau \in \overline{\Delta}} \chi(\tau) \log_p \frac{1 - \zeta_d^{p^2 \tau}}{1 - \zeta_d^{p\tau}} \\
&= \left(\chi(p^{-2}) - \chi(p^{-1})\right) \sum_{\tau \in \overline{\Delta}} \chi(\tau) \log_p (1 - \zeta_d^{\tau}) \\
&= (1 - \chi(p)) \sum_{\substack{a \bmod d \\ (a,d)=1}} \chi(a) \log_p (1 - \zeta_d^{a}) \\
&= -\frac{1 - \chi(p)}{p - \chi(p)} p\sqrt{d} L_p(1, \chi).
\end{aligned}$$

When $k \neq 0$,

$$\begin{aligned}
S_k &= \sum_{i, \omega, \tau} \psi^k \chi(\sigma^i \tau) \log_p \left(\zeta_{p^2}^{\sigma^i \omega} - \zeta_d^{\tau}\right) \\
&= \overline{\psi^k}(d) \sum_{1 \leqslant b \leqslant p^2 d} \psi^k \chi(b) \log_p \left(1 - \zeta_{p^2 d}^{b}\right) \\
&= -\frac{\overline{\psi^k}(d) p^2 d}{\tau\left(\overline{\psi^k} \chi\right)} L_p\left(1, \overline{\psi^k} \chi\right),
\end{aligned}$$

where $\tau\left(\overline{\psi^k}\chi\right)$ is the Gauss sum of the character $\overline{\psi^k}\chi$. Note that

$$\begin{aligned}
\tau\left(\overline{\psi^k}\chi\right) &= \sum_{1 \leqslant a < p^2 d} \overline{\psi^k} \chi(a) \zeta_{p^2 d}^{a} \\
&= \sum_{\substack{0 \leqslant x < d \\ 0 \leqslant y < p^2}} \overline{\psi^k} \chi(p^2 x + dy) \zeta_{p^2 d}^{p^2 x + dy}
\end{aligned}$$

$$= \overline{\psi^k}(d) \left(\sum_y \overline{\psi^k}(y) \zeta_{p^2}^y \right) \left(\sum_x \chi(x) \zeta_d^x \right)$$
$$= \overline{\psi^k}(d) \tau\left(\overline{\psi^k}\right) \tau(\chi).$$

We also have

$$\begin{aligned}
\tau\left(\overline{\psi^k}\right) &= \sum_{0 \leqslant y < p^2} \overline{\psi^k}(y) \zeta_{p^2}^y \\
&= \sum_{\substack{0 \leqslant i < p \\ \omega \in R}} \overline{\psi^k}\left(\sigma^i \omega\right) \zeta_{p^2}^{\sigma^i \omega} \\
&= \sum_{i,\omega} \zeta_p^{-ki} \zeta_{p^2}^{(1+ip)\omega} \\
&= \sum_{\omega} \zeta_{p^2}^{\omega} \left(\sum_i \zeta_p^{(\omega - k)i} \right) \\
&= p \zeta_{p^2}^{\omega(k)},
\end{aligned}$$

where $\omega(k)$ is the root of 1 in $\mathbb{Z}_p$ satisfying $\omega(k) \equiv k \bmod p$. Therefore, for $k \neq 0$,

$$S_k = -p\sqrt{d} \zeta_{p^2}^{-\omega(k)} L_p\left(1, \overline{\psi^k} \chi\right).$$

Thus we have a system of linear equations

$$\left(\psi^k\left(\sigma^i\right)\right) \begin{pmatrix} T_0 \\ T_1 \\ \vdots \\ T_{p-1} \end{pmatrix} = -p\sqrt{d} \begin{pmatrix} \dfrac{1-\chi(p)}{p-\chi(p)} L_p(1,\chi) \\ \vdots \\ \zeta_{p^2}^{-\omega(k)} L_p\left(1, \overline{\psi^k}\chi\right) \\ \vdots \end{pmatrix}.$$

By solving this equation, we have

$$T_0 = -\sqrt{d} \left(\frac{1-\chi(p)}{p-\chi(p)} L_p(1,\chi) + \sum_{1 \leqslant k \leqslant p-1} \zeta_{p^2}^{-\omega(k)} L_p\left(1, \overline{\psi^k}\chi\right) \right).$$

Since $L_p\left(1, \overline{\psi^k}\chi\right) \equiv L_p(1,\chi) \equiv L_p(0,\chi) = -B_{1,\chi\omega^{-1}} \bmod \zeta_p - 1$,

$$T_0 \equiv \sqrt{d} \left(1 - \chi(p) + \sum_{1 \leqslant k \leqslant p-1} \zeta_{p^2}^{\omega(k)} \right) B_{1,\chi\omega^{-1}} \bmod \zeta_p - 1.$$

Since $\zeta_{p^2}^{\omega(k)} \equiv \zeta_{p^2}^{k} \bmod (\zeta_p - 1)$, $1+\sum_k \zeta_{p^2}^{\omega(k)} \equiv (1-\zeta_p)/(1-\zeta_{p^2}) \equiv 0 \bmod \left(1-\zeta_{p^2}\right)^{p-1}$. Therefore $T_0 \equiv -\chi(p)\sqrt{d}B_{1,\chi\omega^{-1}} \bmod \left(\zeta_{p^2}-1\right)^{p-1}$. ∎

Proof of Theorem 3: We already know that $g_n \equiv g_1$ and $\widetilde{g}_n \equiv \widetilde{g}_1 \bmod p$. For brevity, we denote g_1 and $\widetilde{g}_1$ by g and $\widetilde{g}$. We read $\delta_1 = \alpha_1^{\sigma-1}$ in $\overline{\mathbb{Q}_p}$ under the embedding ι. Since k_1 is assumed to be completed at $\wp_1$, we have $(\alpha_1) = (\pi_1)^g$. Let $\pi = \zeta_{p^2}-1$. Then $(\alpha_1) = (\pi)^{g(p-1)}$ in $\mathbb{Q}_p(\zeta_{p^2})$. By taking $\rho \in \Delta_k$, we get $\delta_1^\rho = \alpha_1^{\rho(\sigma-1)}$ and $(\alpha_1^\rho) = \wp_1^{\widetilde{g}}\widetilde{\wp_1}^{g}$ in k_1, hence $(\alpha_1^\rho) = (\pi)^{\widetilde{g}(p-1)}$ in $\mathbb{Q}_p(\zeta_{p^2})$. Thus $\delta_1^{1-\rho} = \alpha_1^{(1-\rho)(\sigma-1)}$ and $\left(\alpha_1^{1-\rho}\right) = (\pi)^{(g-\widetilde{g})(p-1)}$. Hence, in $\mathbb{Q}_p(\zeta_{p^2})$,

$$\delta_1^{1-\rho} = \pi^{(g-\widetilde{g})(p-1)(\sigma-1)}\eta^{\sigma-1}$$

for some unit η in $\mathbb{Q}_p(\zeta_{p^2})$. It is easy to see that

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

Therefore

$$\delta_1^{1-\rho} \equiv 1 + (g-\widetilde{g})(p-1)\pi^{p-1} \equiv 1 + (\widetilde{g}-g)\pi^{p-1} \bmod (\zeta_p - 1).$$

Hence

$$\log_p \delta_1^{1-\rho} \equiv \log_p\left(1 + (\widetilde{g}-g)\pi^{p-1}\right) \bmod (\zeta_p - 1).$$

Now we compute both sides of this congruence.

$$\begin{aligned}
\text{LHS} &= \log_p \delta_1^{1-\rho} \\
&= \log_p \prod_{\substack{\omega\in R\\ \tau\in\Delta}} \left(\zeta_{p^2}^{\omega} - \zeta_d^{\tau}\right)^{1-\rho} \\
&= \log_p \prod_{\substack{\omega\in \underline{R}\\ \tau\in\underline{\Delta}}} \left(\zeta_{p^2}^{\omega} - \zeta_d^{\tau}\right)^{\chi(\tau)} \\
&= \sum_{\substack{\omega\in \underline{R}\\ \tau\in\underline{\Delta}}} \chi(\tau)\log_p\left(\zeta_{p^2}^{\omega} - \zeta_d^{\tau}\right) \\
&\equiv -\sqrt{d}B_{1,\chi\omega^{-1}} \bmod \pi.
\end{aligned}$$

On the other hand,

$$\begin{aligned}
\text{RHS} &= \log_p\left(1 + (\widetilde{g}-g)\pi^{p-1}\right) \\
&\equiv (\widetilde{g}-g)\pi^{p-1} - \frac{1}{2}\left((\widetilde{g}-g)\pi^{p-1}\right)^2 + \ldots + \frac{1}{p}\left((\widetilde{g}-g)\pi^{p-1}\right)^p - \ldots .
\end{aligned}$$

In this expression, every term except $\left((\widetilde{g}-g)\pi^{p-1}\right)^p/p$ is congruent to $0 \bmod \pi$, and $\pi^{(p-1)p}/p \equiv -1 \bmod \pi$. Therefore

$$\log_p\left(1+(\widetilde{g}-g)\pi^{p-1}\right) \equiv g-\widetilde{g} \bmod \pi.$$

By equating both sides, we obtain

$$g-\widetilde{g} \equiv -\sqrt{d}B_{1,\chi\omega^{-1}} \bmod \pi.$$

Since both sides are in $\mathbb{Z}_p$, the congruence holds mod $p\mathbb{Z}_p$. ∎

THEOREM 4. *Suppose an odd prime p splits in $k=\mathbb{Q}(\sqrt{m})$. If $p \mid B_{1,\chi\omega^{-1}}$, then $p \mid h_n$ for all $n \geqslant 1$.*

PROOF: By class field theory, it is enough to show that $p \mid h_1$. If $p \mid h_0$, then there is nothing to prove. So we assume that $p \nmid h_0$. In particular, there is no nontrivial capitulation from k_0 to k_1.

Let $\delta_1 = \alpha_1^{\sigma-1}$ and $(\alpha_1) = \wp_1^{g_1}\widetilde{\wp_1}^{g_1}$ as before. Since $p \mid B_{1,\chi\omega^{-1}}$, $g_1 \equiv \widetilde{g}_1 \bmod p$ by Theorem 3. Let g be such that $0 \leqslant g < p$ and $g_1 \equiv \widetilde{g}_1 \equiv g \bmod p$. Then

$$(\alpha_1) = (\wp_1\widetilde{\wp_1})^g I_0 = (\pi_1^g)I_0$$

for some ideal I_0 of k_0. Since there is no nontrivial capitulation, $I_0=(\alpha_0)$ for some $\alpha_0 \in k_0$. Hence $(\alpha_1) = (\pi_1^g\alpha_0)$ and $\delta_1 = \pi_1^{g(\sigma-1)}\eta_1^{\sigma-1}$ for some $\eta_1 \in E_1$. Thus $H^1(G_1,C_1) \to H^1(G_1,E_1)$ is not injective. From the short exact sequence $0 \to C_1 \to E_1 \to E_1/C_1 \to 0$, we get a long exact sequence

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

Therefore $(E_1/C_1)^{G_1} \otimes \mathbb{Z}_p \neq \{0\}$. Hence $p \mid [E_1 : C_1]$ and so $p \mid h_1$ by the index theorem. ∎

COROLLARY. *Let M_∞ and L_∞ be as in the introduction. If $\mathrm{Gal}(M_\infty/k_\infty)$ is nontrivial, then $\mathrm{Gal}(L_\infty/k_\infty)$ is also nontrivial.*

PROOF: As in the proof of Theorem 1, if $\mathrm{Gal}(M_\infty/k_\infty)$ is nontrivial, then f_χ is not a unit in Λ. Hence $f_\chi(0) = -B_{1,\chi\omega^{-1}}$ is divisible by p. Thus the corollary follows from Theorem 4. ∎

REFERENCES

[1] V. Ennola, 'On relations between cyclotomic units', *J. Number Theory* **4** (1972), 236–247.

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

https://doi.org/10.1017/S0004972700031646 Published online by Cambridge University Press

[3] S. Lang, *Cyclotomic fields*, Graduate Texts in Mathematics I and II **59**, **69** (Springer-Verlag, Berlin, Heidelberg, New York, 1990).

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

[5] A. Scholz, 'Über die Beziehung der Klassenzahlen quadratischer Körper zueinander', *J. Reine Angew Math.* **166** (1932), 201–203.

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

[7] L. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Mathematics **83** (Springer-Verlag, Berlin, Heidelberg, New York, 1980).

Department of Mathematics
Inha University
Inchon
Korea
e-mail: jmkim@math.inha.ac.kr

https://doi.org/10.1017/S0004972700031646 Published online by Cambridge University Press