ACTA ARITHMETICA
LXXII.4 (1995)

Class numbers of certain real abelian fields

by

Jae Moon Kim (Inchon)

0. Introduction. We fix an odd prime q. Let p be an odd prime such that $p \equiv 1 \bmod q$. Let

$$g(t) = (1-t)^{p-2} + \frac{1}{2}(1-t)^{p-3} + \ldots + \frac{1}{p-1}.$$

We will consider $g(t)$ as an element in $\mathbb{F}_p[t]$, where $\mathbb{F}_p$ is the finite field with p elements. If necessary, we will also view $g(t)$ as a polynomial in $\mathbb{Z}_p[t]$, where $\mathbb{Z}_p$ is the ring of p-adic integers. It is not hard to see that

$$tg(1-t) \equiv \frac{(1-t)^p - (1-t^p)}{p} \bmod p.$$

This polynomial

$$f(t) = \frac{(1-t)^p - (1-t^p)}{p}$$

in $\mathbb{F}_p[t]$ was first introduced by D. Mirimanoff around 1905 and has been exhaustively studied since then. For instance, he used the polynomial $f(t)$ to prove the following striking criterion of A. Wieferich: if the Fermat quotient $(2^{p-1}-1)/p$ is not congruent to 0 mod p, then the first case of the Fermat's Last Theorem is true (see [8]).

In this paper, we will study class numbers of certain real abelian fields by using the polynomial $g(t)$. Our work is based on the observation that $g(t)$ comes from a Coates–Wiles series. To be precise, let

$$h_t(x) = \prod_{w \in R} ((1+x)^w - t),$$

where $R = \{w \in \mathbb{Z}_p \mid w^{p-1} = 1\}$ is the group of the $(p-1)$th roots of 1 in $\mathbb{Z}_p$. Viewing $h_t(x)$ as an element of $\mathbb{Z}_p[t][[x]]$, i.e., as a power series in x

This work was partially supported by the Basic Science Research Institute program, Ministry of Education, #BSRI-94-1414.

with coefficients in $\mathbb{Z}_p[t]$, we have the following expansion (see [6]):

$$h_t(x) = (1-t)^{p-1} + g_1(t)x^{p-1} + (\text{higher terms})$$

with

$$g_1(t) \equiv g(t) \bmod p.$$

To see why $h_t(x)$ is a Coates–Wiles series, let $t = s$ be a root of 1 in $\mathbb{Z}_p$. Then $h_s(x)$ is indeed a Coates–Wiles series (see [1], [10]).

In Section 1 of this paper we will use the above expansion of $h_t(x)$ to factorize certain principal ideals into a product of prime ideals. In Section 2, we discuss class numbers of certain real abelian fields. Before we state the main theorems, we first explain several notations that will be used throughout this paper.

For each integer $n \geq 1$, we choose a primitive nth root ζ_n of 1 so that $\zeta_m^{m/n} = \zeta_n$ whenever $n \mid m$. Let $k_0 = \mathbb{Q}(\zeta_p)$, $k_n = \mathbb{Q}(\zeta_{p^{n+1}})$, $K_0 = \mathbb{Q}(\zeta_{pq})$ and $K_n = \mathbb{Q}(\zeta_{p^{n+1}q})$. We denote the unique subfield of k_n of degree p^n over $\mathbb{Q}$ by $\mathbb{Q}_n$. Let $F_0 = \mathbb{Q}(\zeta_q)$, $F_n = \mathbb{Q}_n(\zeta_q)$, $F_0^+ = \mathbb{Q}(\zeta_q + \zeta_q^{-1})$ and $F_n^+ = \mathbb{Q}_n(\zeta_q + \zeta_q^{-1})$. Thus for $E = k, K, F$ and F^+, E_n is the nth layer of the basic $\mathbb{Z}_p$-extension of E_0. We denote the Galois groups $\mathrm{Gal}(F_0/\mathbb{Q})$ and $\mathrm{Gal}(F_0^+/\mathbb{Q})$ by Δ and Δ^+, respectively, and use the same letters Δ, Δ^+ for those Galois groups isomorphic to $\mathrm{Gal}(F_0/\mathbb{Q})$, $\mathrm{Gal}(F_0^+/\mathbb{Q})$. Elements of Δ^+ and Δ will be arranged as $\Delta^+ = \{\tau_1, \tau_2, \ldots, \tau_l = \mathrm{id}\}$ and $\Delta = \{\pm\tau_1, \pm\tau_2, \ldots, \pm\tau_l\}$ with $l = \frac{1}{2}\varphi(q)$. For each $\tau \in \Delta$, let $p(\tau)$ be the integer modulo q corresponding to τ under the natural isomorphism $\Delta \simeq (\mathbb{Z}/q\mathbb{Z})^\times$. Note that $p(-\tau) = -p(\tau)$. Finally, we let σ be the topological generator of $\Gamma = \varprojlim \mathrm{Gal}(K_n/K_0)$ which maps ζ_{p^n} to $\zeta_{p^n}^{1+p}$ for each $n \geq 1$ and ζ_q to ζ_q. Restrictions of σ to various subfields k_n, F_n, F_n^+ and K_n of $K_\infty = \bigcup_{n\geq 0} K_n$ are also denoted by σ.

Now we state the main theorems of this paper:

THEOREM 2. *If p divides $\prod_{\chi\in\widehat{\Delta}^+,\chi\neq 1} B_{1,\chi\omega^{-1}}$, then p divides the class number of F_n^+ for all $n \geq 1$, where ω is the Teichmüller character on $\mathrm{Gal}(k_0/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$.*

THEOREM 3. *If p does not divide $\prod_{\chi\in\widehat{\Delta}^+,\chi\neq 1} B_{1,\chi\omega^{-1}}$, then the prime ideals of F_n^+ above p are of order prime to p in the ideal class group of F_n^+.*

It is well known, by the class number formula, that the relative class number $h_{K_0}^-$ of the field K_0 is given by the formula $h_{K_0}^- = Qw\prod_\varrho \left(-\frac{1}{2}B_{1,\varrho}\right)$, where the product is taken over all odd characters of $\mathrm{Gal}(K_0/\mathbb{Q})$. Hence $\prod_{\chi\in\widehat{\Delta}^+,\chi\neq 1} B_{1,\chi\omega^{-1}}$ contributes to $h_{K_0}^-$. Thus from Theorems 2 and 3 we obtain some information on the p-divisibility of $h_{F_n^+} = h_{F_n}^+$, the plus part of the class number of F_n, from that of the minus part $h_{K_0}^-$.

In Section 3, we prove a lemma to finish the proof of Theorem 2. This lemma treats certain relations among cyclotomic units. For a deeper analysis of the relations of cyclotomic units, we refer to [2]. We will apply the results of [2] to our special situation. A similar, but slightly different computation was performed in [7].

1. Factorization of a certain principal ideal. In this section, we start out with an explicit element ξ_n in F_n^+ whose norm to F_0^+ equals 1. So, by the Hilbert Theorem 90, ξ_n is of the form $\xi_n = \alpha_n^{\sigma-1}$ for some $\alpha_n \in F_n^+$. The aim of this section is to factorize the principal ideal (α_n) into a product of prime ideals of F_n^+. This factorization is crucial in the proofs of Theorems 2 and 3 of the following section.

Let

$$\xi_n = \prod_{w \in R} (\zeta_{p^{n+1}}^w - \zeta_q)(\zeta_{p^{n+1}}^w - \zeta_q^{-1}).$$

Then ξ_n is an element of F_n^+ since $\xi_n = N_{K_n/F_n^+}(\zeta_{p^{n+1}} - \zeta_q)$. Since each $\zeta_{p^{n+1}}^w - \zeta_q^{\pm 1}$ is a cyclotomic unit in K_n, so is ξ_n. Thus ξ_n can be thought of as a cyclotomic unit in F_n^+ in the sense of W. Sinnott (see [9]). One can easily check that $N_{F_n^+/F_0^+}(\xi_n) = 1$. Indeed,

$$\begin{aligned} N_{F_n^+/F_0^+}(\xi_n) &= N_{K_n/F_0^+}(\zeta_{p^{n+1}} - \zeta_q) = N_{K_0/F_0^+}(N_{K_n/K_0}(\zeta_{p^{n+1}} - \zeta_q)) \\ &= N_{K_0/F_0^+}(\zeta_p - \zeta_q) = N_{F_0/F_0^+}\Big(\prod_{1 \le i \le p-1} \zeta_p^i - \zeta_q\Big) \\ &= N_{F_0/F_0^+}\left(\frac{1-\zeta_q^p}{1-\zeta_q}\right) = 1. \end{aligned}$$

The last equality holds since $p \equiv 1 \bmod q$. Hence $\xi_n = \alpha_n^{\sigma-1}$ for some $\alpha_n \in F_n^+$ by the Hilbert Theorem 90.

LEMMA 1. *$\xi_n = \alpha_n^{\sigma-1}$ for some p-unit $\alpha_n \in F_n^+$.*

Proof. Let $K_\infty = \bigcup_{n \ge 0} \mathbb{Q}(\zeta_{p^{n+1}q})$ be the basic $\mathbb{Z}_p$-extension of K_0. Let $E'_\infty(C_\infty)$ be the group of p-units (cyclotomic units) of K_∞. In [4], Iwasawa proves that the cohomology group $H^1(\Gamma, E'_\infty)$ is a finite group, where $\Gamma = \mathrm{Gal}(K_\infty/K_0)$. But $H^1(\Gamma, C_\infty) \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^l$, where $l = \frac{1}{2}\varphi(q)$ (see [5]). Thus the induced map $H^1(\Gamma, C_\infty) \to H^1(\Gamma, E'_\infty)$ from the natural inclusion $C_\infty \to E'_\infty$ must be a zero map. Since the inflation maps on H^1 are injective, $H^1(G_n, C_n) \to H^1(G_n, E'_n)$ is a zero map, where $G_n = \mathrm{Gal}(K_n/K_0)$ and $C_n(E'_n)$ is the group of cyclotomic units (p-units) in K_n. Then by the cyclicity of the group G_n, $H^{-1}(G_n, C_n) \to H^{-1}(G_n, E'_n)$ is also a zero map, which means that a cyclotomic unit in K_n whose norm to K_0 equals 1 is of the form $\beta^{\sigma-1}$ for some p-unit $\beta \in K_n$. In particular, since

$N_{K_n/K_0}(\prod_{w\in R}(\zeta_{p^{n+1}}^w-\zeta_q))=1$, we have

$$\prod_{w\in R}(\zeta_{p^{n+1}}^w-\zeta_q)=\beta^{\sigma-1}\quad\text{for some } p\text{-unit } \beta\in K_n.$$

Thus

$$\begin{aligned}\prod_{w\in R}(\zeta_{p^{n+1}}^w-\zeta_q)^{p^n-1}&=N_{K_n/F_n}\Big(\prod_{w\in R}(\zeta_{p^{n+1}}^w-\zeta_q)\Big)^{(p^n-1)/(p-1)}\\&=N_{K_n/F_n}(\beta^{(p^n-1)/(p-1)})^{\sigma-1}.\end{aligned}$$

Note that $\prod_{w\in R}(\zeta_{p^{n+1}}^w-\zeta_q)^{p^n}=u^{\sigma-1}$ for some cyclotomic unit $u\in F_n$ since $p^nH^{-1}(G_n,C_{F_n})=0$. Here C_{F_n} is the group of cyclotomic units of F_n. Therefore

$$\prod_{w\in R}(\zeta_{p^{n+1}}^w-\zeta_q)=(uN_{K_n/F_n}(\beta^{-(p^n-1)/(p-1)}))^{\sigma-1}.$$

Put $\alpha_n=N_{F_n/F_n^+}(uN_{K_n/F_n}(\beta^{-(p^n-1)/(p-1)}))$. Then $\xi_n=\alpha_n^{\sigma-1}$ and α_n is a p-unit in F_n^+. This proves the lemma.

Fix a prime ideal $\wp_0$ of F_0^+ above p and let $\wp_n$ be the prime ideal of F_n^+ above $\wp_0$. Then $\{\wp_0^{\tau_i}\mid\tau_i\in\Delta^+\}$ and $\{\wp_n^{\tau_i}\mid\tau_i\in\Delta^+\}$ are the sets of all prime ideals of F_0^+ and F_n^+ above p. For each $\wp_n^{\tau_i}$, there are two prime ideals in F_n above $\wp_n^{\tau_i}$. By abuse of notation, we write them as $\wp_n^{\tau_i}$ and $\wp_n^{-\tau_i}$. This will not cause any confusion. Since primes of F_n above p totally ramify in K_n, above each prime ideal $\wp_n^{\pm\tau_i}$ there is a unique prime ideal $\widetilde{\wp}_n^{\pm\tau_i}$ in K_n. For each $\tau\in\Delta=\{\pm\tau_1,\dots,\pm\tau_l\}$, let $F_{n,\wp_n^\tau}$ be the completion of F_n at $\wp_n^\tau$, and let $\varphi_\tau:F_n\to F_{n,\wp_n^\tau}$ be the natural embedding. Put $s_\tau=\varphi_\tau(\zeta_q)$, which is a qth root of 1 in $\mathbb{Z}_p$. For brevity, we write s for $s_{\mathrm{id}}=\varphi_{\mathrm{id}}(\zeta_q)$. Then $s_\tau^{p(\tau)}=\varphi_\tau(\zeta_q)^{p(\tau)}=\varphi_\tau(\zeta_q^{p(\tau)})=\varphi_\tau(\zeta_q^\tau)$. Since the completion of F_n^τ at $\wp_n^\tau$ is the same as the completion of F_n at $\wp_n$, we have $s_\tau^{p(\tau)}=\varphi_\tau(\zeta_q^\tau)=\varphi_{\mathrm{id}}(\zeta_q)=s$. Therefore $s_\tau=s^{p(\tau^{-1})}$ and $s_\tau^{p(\tau')}=s^{p(\tau^{-1})p(\tau')}=s^{p(\tau^{-1}\tau')}$ for any $\tau,\tau'\in\Delta$.

THEOREM 1. *Let ξ_n be as before and write $\xi_n=\alpha_n^{\sigma-1}$ for some p-unit $\alpha_n\in F_n^+$ as in Lemma 1. If $(\alpha_n)=\wp_n^{\sum_{1\le i\le l}a_i\tau_i}$ is the factorization in F_n^+, then $a_i\equiv 2g(s^{p(\tau_i^{-1})})\bmod p$, where $g(t)$ is the polynomial defined in the introduction.*

Remark. If $\xi_n=\alpha_n^{\sigma-1}=(\alpha_n')^{\sigma-1}$ for another p-unit α_n', then $\alpha_n=\alpha_n'\alpha_0$ for some p-unit α_0 in F_0^+. Since the primes of F_0^+ above p totally ramify in F_n^+, their ramification indices are p^n. Hence a_i's are uniquely determined mod p^n, so mod p.

One can show that $g(s)=g(s^{-1})$ for any $(p-1)$th root s in $\mathbb{Z}_p$ (see [6]).

Thus

$$g(s^{p(-\tau_i^{-1})}) = g(s^{-p(\tau_i^{-1})}) = g(s^{p(\tau_i^{-1})}),$$

and $g(s^{p(\tau_i^{-1})})$ is well defined for each $\tau_i \in \Delta^+$.

Proof of Theorem 1. To compute a_i, we read the prime factorization $(\alpha_n) = \wp_n^{\Sigma a_i \tau_i}$ in the field $K_{n,\tilde{\wp}_n^{\tau_i}}$ (or in $K_{n,\tilde{\wp}_n^{-\tau_i}}$). Since $\pi_n = \zeta_{p^{n+1}} - 1$ generates the prime ideal of $K_{n,\tilde{\wp}_n^{\tau_i}}$, we have $(\alpha_n) = \wp_n^{\Sigma a_i \tau_i} = (\pi_n)^{a_i}$. Hence $\alpha_n = \pi_n^{a_i}\eta$ for some unit η in $K_{n,\tilde{\wp}_n^{\tau}}$. Note that $\eta^{\sigma-1} \equiv 1 \bmod (\pi_n^p)$. We claim that $\pi_n^{\sigma-1} \equiv 1 + \pi_n^{p-1} \bmod (\pi_n^p)$. First, notice that for each $1 \le k \le p-1$, $\zeta_{p^{n+1}}^{1+kp} - 1 = \zeta_{p^{n+1}}\zeta_{p^n}^k - 1 \equiv \zeta_{p^{n+1}} - 1 \bmod (\zeta_{p^n} - 1)$. Thus

$$\begin{aligned}\prod_{1\le k\le p-1} (\zeta_{p^{n+1}}^{1+kp} - 1) &\equiv \prod_{1\le k\le p-1} (\zeta_{p^{n+1}} - 1)\\ &= (\zeta_{p^{n+1}} - 1)^{p-1} \bmod (\zeta_{p^n} - 1).\end{aligned}$$

Therefore

$$\begin{aligned}\pi_n^{\sigma-1} &= \frac{\zeta_{p^{n+1}}^{1+p} - 1}{\zeta_{p^{n+1}} - 1} = \zeta_{p^n} + \frac{\zeta_{p^n} - 1}{\zeta_{p^{n+1}} - 1}\\ &= \zeta_{p^n} + \prod_{1\le k\le p-1} (\zeta_{p^{n+1}}^{1+kp} - 1)\\ &\equiv 1 + (\zeta_{p^{n+1}} - 1)^{p-1} \bmod (\zeta_{p^n} - 1)\end{aligned}$$

as claimed. Hence

$$(\pi_n^{a_i}\eta)^{\sigma-1} \equiv (1 + \pi_n^{p-1})^{a_i} \equiv 1 + a_i\pi_n^{p-1} \bmod (\pi_n^p).$$

On the other hand, by putting $x = \zeta_{p^{n+1}} - 1$ and $t = s_\tau$ in $\prod_{w\in R}((1+x)^w - t) = (1-t)^{p-1} + g_1(t)x^{p-1} + (\text{higher terms})$, we obtain

$$\prod_{w\in R} (\zeta_{p^{n+1}}^w - s_\tau) \equiv 1 + g(s_\tau)\pi_n^{p-1} \bmod (\pi_n^p).$$

Hence if we view $\xi_n = \prod_{w\in R}(\zeta_{p^{n+1}}^w - \zeta_q)(\zeta_{p^{n+1}}^w - \zeta_q^{-1})$ as an element of $K_{n,\tilde{\wp}_n^{\tau}}$, we have

$$\begin{aligned}\xi_n &= \prod_{w\in R} (\zeta_{p^{n+1}}^w - s_\tau)(\zeta_{p^{n+1}}^w - s_\tau^{-1})\\ &\equiv (1 + g(s_\tau)\pi_n^{p-1})(1 + g(s_\tau^{-1})\pi_n^{p-1})\\ &\equiv 1 + (g(s_\tau) + g(s_\tau^{-1}))\pi_n^{p-1} \bmod (\pi_n^p).\end{aligned}$$

Thus $1 + a_i\pi_n^{p-1} \equiv \alpha_n^{\sigma-1} = \xi_n \equiv 1 + (g(s_{\tau_i}) + g(s_{\tau_i}^{-1}))\pi_n^{p-1} \bmod (\pi_n^p)$. Therefore $a_i \equiv g(s_{\tau_i}) + g(s_{\tau_i}^{-1}) \equiv 2g(s_{\tau_i}) \equiv 2g(s^{p(\tau_i^{-1})}) \bmod (\pi_n)$, hence mod p.

2. Main theorems. Recall that $l = [F_0^+ : \mathbb{Q}]$ and that we arranged elements of Δ^+ as $\Delta^+ = \{\tau_1, \tau_2, \dots, \tau_{l-1}, \tau_l = \mathrm{id}\}$. Let $A' = (a_{ij})$ be the

$l \times l$ matrix with entries in $\mathbb{F}_p$ such that $a_{ij} \equiv g(s^{p(\tau_i^{-1}\tau_j)}) \bmod p$. Note that each row and column of A' has a fixed sum $g = \sum_{1\le i\le l} g(s^{p(\tau_i)})$. Let $A = (b_{ij})$ be the $l \times l$ matrix with entries in $\mathbb{F}_p$ such that

$$b_{ij} = \begin{cases} a_{ij} & \text{if } j \le l-1, \\ 1 & \text{if } j = l. \end{cases}$$

Below, we write $(a_1, \dots, a_n)^t$ for the column vector with entries $a_1, \dots, a_n$.

Lemma 2. *Suppose* $\det A \equiv 0 \bmod p$. *Then there exists* $\mathbf{b} = (b_1, \dots, b_l)^t$ *in* $\mathbb{F}_p^l$ *such that*

(i) $A'\mathbf{b} \equiv \mathbf{0} = (0, \dots, 0)^t \bmod p$,

(ii) $\mathbf{b}$ *is not a constant multiple of* $\mathbf{1} = (1, \dots, 1)^t$.

Proof. We examine the following two cases separately.

Case 1: $g \not\equiv 0 \bmod p$. By adding each column of A' to the last one, we have

$$\det A' = \det \left(\begin{array}{c|c} a_{ij}\atop{j\le l-1} & \begin{matrix} g \\ \vdots \\ g \end{matrix} \end{array} \right) = g \det A \equiv 0 \bmod p.$$

Hence $A'\mathbf{b} = \mathbf{0}$ has a nontrivial solution. This solution cannot be a multiple of $\mathbf{1}$, for otherwise, the row sum g would be 0.

Case 2: $g \equiv 0 \bmod p$. Since each row sum is 0, $\mathbf{1}$ is obviously a solution of $A'\mathbf{b} = \mathbf{0}$. To prove the existence of a solution which is not a multiple of $\mathbf{1}$, it is enough to check that the $\mathbb{F}_p$-rank of A' is less than or equal to $l-2$. Let B be the $(l-1) \times (l-1)$ matrix consisting of the first $(l-1) \times (l-1)$ entries in A'. By performing elementary row and column operations, we see that

$$\operatorname{rank} A' = \operatorname{rank} \left(\begin{array}{c|c} \multirow{2}{*}{B} & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \\ \hline 0 \ \dots \ 0 & 0 \end{array} \right) = \operatorname{rank} B.$$

By adding each row of A to the last one, we have

$$\det A = \det \left(\begin{array}{c|c} \multirow{2}{*}{B} & \begin{matrix} 1 \\ \vdots \\ 1 \end{matrix} \\ \hline 0 \ \dots \ 0 & l \end{array} \right) = l \det B.$$

Since $l \not\equiv 0 \bmod p$, $\det B \equiv 0 \bmod p$. Therefore $\operatorname{rank} A' = \operatorname{rank} B \le l-2$.

Let ω be the Teichmüller character on $\mathrm{Gal}(k_0/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ and χ be a character on Δ^+. For the proofs of the main theorems, we need the following

theorem which interprets $\det A$ in terms of the generalized Bernoulli numbers $B_{1,\chi\omega^{-1}}$.

THEOREM. $\det A \equiv 0 \bmod p$ *if and only if* $\prod_{\chi\in\widehat{\Delta}^+,\chi\neq 1} B_{1,\chi\omega^{-1}} \equiv 0 \bmod p$.

Proof. See Theorem 3 of [7].

Now we restate and prove the main theorems.

THEOREM 2. *If* $p \mid \prod_{\chi\in\widehat{\Delta}^+,\chi\neq 1} B_{1,\chi\omega^{-1}}$, *then* $p \mid h_{F_n^+}$ *for all* $n \geq 1$.

Proof. Since $h_{F_n^+} \mid h_{F_m^+}$ for all $n \leq m$ by the class field theory, it is enough to show that $p \mid h_{F_1^+}$. By the above theorem, we can assume that $\det A \equiv 0 \bmod p$. Then by Lemma 2, there exists a vector $\mathbf{b} = (b_1, \ldots, b_l)^t$ in $\mathbb{F}_p^l$ satisfying those two conditions (i), (ii) in the lemma. Suppose $p \nmid h_{F_1^+}$. Then, by the class field theory, we have

(iii) $p \nmid h_{F_0^+}$.

Moreover, the Sylow p-subgroup of E/C must be trivial (see [9]), where $E(C)$ is the group of units (cyclotomic units) in F_1^+. Thus, the cohomology groups $H^i(G_1, E/C)$ are trivial for all $i \in \mathbb{Z}$. Hence by considering the long exact sequence of cohomology groups coming from the short exact sequence $0 \to C \to E \to E/C \to 0$, we have

(iv) The homomorphism $H^{-1}(G_1, C) \to H^{-1}(G_1, E)$ induced by the inclusion $C \to E$ is an isomorphism.

Let $\delta = \xi^{\Sigma_{i=1}^l b_i\tau_i} = \alpha^{(\Sigma b_i\tau_i)(\sigma-1)}$ with $\mathbf{b} = (b_1, \ldots, b_l)^t$ as before and $\xi = \xi_1$, $\alpha = \alpha_1$ as in Theorem 1. Then the principal ideal $(\alpha^{\Sigma b_i\tau_i})$ factorizes as

$$(\alpha^{\Sigma b_i\tau_i}) = \wp_1^{(2\Sigma_{j=1}^l g(s^{p(\tau_j^{-1})})\tau_j)(\Sigma_{i=1}^l b_i\tau_i)}.$$

In this expression,

$$\begin{aligned}\Big(\sum_{j=1}^{l} g(s^{p(\tau_j^{-1})})\tau_j\Big)\Big(\sum_{i=1}^{l} b_i\tau_i\Big) &= \sum_{1\leq i,j\leq l} g(s^{p(\tau_j^{-1})})b_i\tau_j\tau_i \\ &= \sum_{k=1}^{l}\Big(\sum_{\substack{i,j\\ \tau_j\tau_i=\tau_k}} g(s^{p(\tau_j^{-1})})b_i\Big)\tau_k \\ &= \sum_{k=1}^{l}\Big(\sum_{i=1}^{l} g(s^{p(\tau_k^{-1}\tau_i)})b_i\Big)\tau_k.\end{aligned}$$

Since $A'\mathbf{b} \equiv \mathbf{0}$, $\sum_{i=1}^l g(s^{p(\tau_k^{-1}\tau_i)})b_i \equiv 0 \bmod p$ for each $k = 1, \ldots, l$. Hence

$$(\alpha^{\Sigma b_i\tau_i}) = \wp_1^{\Sigma_{i=1}^l d_i\tau_i}$$

for some d_i satisfying $d_i \equiv 0 \bmod p$. Since $\wp_1^p = \wp_0$, we get

$$(\alpha^{\Sigma b_i \tau_i}) = I_0$$

for some ideal I_0 of F_0^+. But the subgroup of the ideal class group of F_0^+ consisting of ideal classes that become principal in F_1^+ is a p-group. Thus nonprincipal ideals of F_0^+ cannot capitulate in F_1^+ by (iii). Therefore

$$(\alpha^{\Sigma b_i \tau_i}) = I_0 = (\alpha_0)$$

for some $\alpha_0 \in F_1^+$, and thus $\alpha^{\Sigma b_i \tau_i} = \alpha_0 \eta'$ for some unit η' in F_1^+. Then we have

$$\delta = \xi^{\Sigma b_i \tau_i} = \alpha^{(\Sigma b_i \tau_i)(\sigma - 1)} = (\eta')^{\sigma - 1}.$$

Since the induced homomorphism $H^{-1}(G_1, C) \to H^{-1}(G_1, E)$ is an isomorphism by (iv), $(\eta')^{\sigma-1} = \eta^{\sigma-1}$ for some cyclotomic unit in F_1^+. However, this cannot happen by (ii) and the following lemma which will be proved in the next section.

LEMMA 3. *Let $\xi = \prod_{w \in R}(\zeta_{p^2}^w - \zeta_q)(\zeta_{p^2}^w - \zeta_q^{-1})$ as before. If $\xi^{\Sigma_{i=1}^l c_i \tau_i} = \eta^{\sigma-1}$ for some cyclotomic unit $\eta \in F_1^+$, then $c_1 \equiv \ldots \equiv c_l \bmod p$.*

THEOREM 3. *If $p \nmid \prod_{\chi \in \widehat{\Delta}^+, \chi \neq 1} B_{1,\chi\omega^{-1}}$, then the prime ideals of F_n^+ above p are of order prime to p in the ideal class group of F_n^+ for all $n \geq 0$.*

Proof. It is enough to show that the ideal class $[\wp_n]$ is of order prime to p. As in Lemma 2, we examine two cases separately.

Case 1: $g \not\equiv 0 \bmod p$. Since $\det A' = g \det A$, $\det A' \not\equiv 0 \bmod p$. Thus there exists $\mathbf{x} = (x_1, \ldots, x_l)^t$ such that $A'\mathbf{x} = (0, \ldots, 0, 1)^t$. Let ξ_n and α_n be as in Theorem 1. Then $(\alpha_n^{\Sigma_{i=1}^l x_i \tau_i}) = \wp_n^{\Sigma_{i=1}^l d_i \tau_i}$ for some d_i satisfying $d_l \equiv 1 \bmod p$ and $d_1 \equiv \ldots \equiv d_{l-1} \equiv 0 \bmod p$. Since $\wp_n^p = \wp_{n-1}$, we get

$$(*) \qquad (\alpha_n^{\Sigma x_i \tau_i}) = \wp_n I_{n-1}$$

for some ideal I_{n-1} of F_{n-1}^+ whose prime factors lie above p. Let mp^k be the order of the ideal class $[\wp_n]$ with $(m, p) = 1$. If $k \neq 0$, then $I_{n-1}^{mp^{k-1}}$ is a principal ideal in F_n^+. Therefore by raising both sides of $(*)$ to the power of dp^{k-1} we get a contradiction. Hence $k = 0$.

Case 2: $g \equiv 0 \bmod p$. Since $\det A \not\equiv 0 \bmod p$, $\mathbb{F}_p$-rank $A' = l - 1$. Thus columns of A' except the last one are linearly independent over $\mathbb{F}_p$ and are contained in the subspace of $\mathbb{F}_p^l$ consisting of $\{\mathbf{y} = (y_1, \ldots, y_l)^t \in \mathbb{F}_p^l \mid y_1 + \ldots + y_l = 0\}$, which is of dimension $l - 1$. Therefore if we view A' as a linear map from $\mathbb{F}_p^l$ to $\mathbb{F}_p^l$, the image of A' is precisely the subspace described above. For each i, $1 \leq i \leq l - 1$, choose $\mathbf{b}_i$ in $\mathbb{F}_p^l$ such that $A'\mathbf{b}_i = (0, \ldots, 1, \ldots, 0, -1)^t$, with 1 at the ith place, -1 at the last place

and 0 elsewhere. Then as in the first case, we get

$$(**) \qquad \wp_n^{\tau_i - 1} I_{n-1} = (\beta_n)$$

for some $\beta_n \in F_n^+$. Note that $\wp_n^{\sum_{i=1}^{l} \tau_i}$ is the prime ideal of $\mathbb{Q}_n$, hence is principal. Thus by multiplying $(**)$ for $1 \le i \le l$ we see that $\wp_n^l I'_{n-1}$ is a principal ideal for some ideal I'_{n-1} whose prime factors lies above p. Since $p \nmid l$, we can check that $[\wp_n]$ is of order prime to p as in Case 1.

Let A_n be the Sylow p-subgroup of the ideal class group of F_n^+ and let $A_\infty = \varprojlim A_n$, where the limit is taken under the norm maps. It is well known that $A_\infty \simeq \mathbb{Z}_p^\lambda \oplus M$ for some finite group M which measures the capitulation. It is conjectured that the Iwasawa λ-invariant for F_∞^+/F_0^+ equals 0 and R. Greenberg gave several equivalent statements to this (see [3]). By using one of the equivalent statements (Theorem 2 of [3]), we have the following corollary.

Corollary. *Suppose $\lambda = 0$. Then $p \nmid \prod_{\chi \in \widehat{\Delta}^+, \chi \neq 1} B_{1,\chi\omega^{-1}}$ if and only if $A_\infty = \{0\}$.*

Proof. Theorem 2 takes care of the if part. For the converse, we need the assumption $\lambda = 0$. Since $\lambda = 0$, $\#A_n$ is bounded by $\#M$ as $n \to \infty$. Equivalently, every ideal class in $A_n^{G_n}$ contains an ideal whose prime factors lie above p by Theorem 2 of [3]. Thus if $p \nmid \prod_{\chi \in \widehat{\Delta}^+, \chi \neq 1} B_{1,\chi\omega^{-1}}$, then $A_n^{G_n} = \{0\}$ by Theorem 3. Since A_n and G_n are p-groups, $A_n = \{0\}$ for all n. Therefore $A_\infty = \{0\}$.

3. Proof of Lemma 3. In this section we prove Lemma 3 stated in the previous section. The proof is based on the work of V. Ennola ([2]) and is similar to that of Theorem 1 in [7]. In particular we need the following theorem:

Theorem (V. Ennola). *Let $\delta = \prod_{1 \le a < n} (1 - \zeta_n^a)^{x_a}$, $x_a \in \mathbb{Z}$, be a cyclotomic unit in $\mathbb{Q}(\zeta_n)$. For an even character $\chi \neq 1$ of conductor f belonging to $\mathbb{Q}(\zeta_n)$, define $Y(\chi, \delta)$ by*

$$Y(\chi, \delta) = \sum_{\substack{d \\ f \mid d \mid n}} \frac{1}{\varphi(d)} T(\chi, d, \delta) \prod_{p \mid d} (1 - \overline{\chi}(p)),$$

where

$$T(\chi, d, \delta) = \sum_{\substack{a=1 \\ (a,d)=1}}^{d-1} \chi(a) x_{na/d}.$$

If δ is a root of 1, then $Y(\chi, \delta) = 0$ for all even characters $\chi \neq 1$ belonging to $\mathbb{Q}(\zeta_n)$.

We also need the following properties of Y which are easy to check. Let $\chi \neq 1$ be an even character belonging to $\mathbb{Q}(\zeta_n)$. Then

(i) $Y(\chi, \delta_1\delta_2) = Y(\chi, \delta_1) + Y(\chi, \delta_2)$.
(ii) If (root of 1)$\times\delta_1$ = (root of 1)$\times\delta_2$, then $Y(\chi, \delta_1) = Y(\chi, \delta_2)$.
(iii) For any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, $Y(\chi, \delta^\sigma) = \chi(\sigma)Y(\chi, \delta)$.
(iv) $Y(\chi, \delta^{\sigma-1}) = (\chi(\sigma) - 1)Y(\chi, \delta)$.

Now we sketch the proof of Lemma 3 briefly.

Sketch of proof. Suppose $\xi^{\Sigma_{i=1}^{l} c_i\tau_i} = \eta^{\sigma-1}$, with ξ, η as in the lemma. By (ii),

$$Y(\varrho, \xi^{\Sigma c_i\tau_i}) = Y(\varrho, \eta^{\sigma-1})$$

for any even character $\varrho \neq 1$ in $\mathrm{Gal}(K_1/\mathbb{Q})^\wedge$. By (i), (iv), we obtain

$$(*) \qquad \sum_{i=1}^{l} c_i\varrho(\tau_i)Y(\varrho, \xi) = (\varrho(\sigma) - 1)Y(\varrho, \eta).$$

Fix a nontrivial character ψ of $\mathrm{Gal}(\mathbb{Q}_1/\mathbb{Q})$. For a nontrivial character $\chi \in \widehat{\Delta}^+$, put $\varrho = \chi\psi$ in $(*)$. After a similar computation to that of Theorem 1 of [7], we have

$$(p-1)\sum_{i=1}^{l} c_i\chi(\tau_i) = (\psi(\sigma) - 1)\alpha(\chi)$$

for some algebraic integer $\alpha(\chi)$. By letting χ run through all the nontrivial even characters of $\widehat{\Delta}^+$, we have the following system of linear equations:

$$(p-1)T(c_1, \ldots, c_l)^t = (\psi(\sigma) - 1)(\ldots, \alpha(\chi), \ldots)^t,$$

where T is the $(l-1) \times l$ matrix with rows of the form $(\chi(\tau_1), \ldots, \chi(\tau_l))$. Let $L = \mathbb{Q}(\zeta_p, \alpha(\chi)\text{'s}, \chi(\tau_i)\text{'s})$, $\mathcal{O}_L$ be the ring of integers of L, and $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_L$ above p. Then we have

$$T(c_1, \ldots, c_l)^t \equiv (0, \ldots, 0)^t \bmod \mathfrak{P},$$

since $\psi(\sigma) - 1 \equiv \zeta_p - 1 \equiv 0 \bmod \mathfrak{P}$.

Let $\overline{T}$ be the matrix obtained by reducing the entries of T mod $\mathfrak{P}$. By using Lemma 1.2 of [7], one can check that the $\mathcal{O}_L/\mathfrak{P}$-rank of $\overline{T}$ is $l-1$. Hence $\{\overline{\mathbf{x}} = (\overline{x}_1, \ldots, \overline{x}_l)^t \in \mathcal{O}_L/\mathfrak{P} \mid \overline{T}\overline{\mathbf{x}} = (0, \ldots, 0)^t\}$ is one-dimensional. But $(1, \ldots, 1)^t$ obviously satisfies $T(1, \ldots, 1)^t = (0, \ldots, 0)^t$. Thus $(c_1, \ldots, c_l)^t \equiv \alpha(1, \ldots, 1)^t \bmod \mathfrak{P}$ for some $\alpha \in \mathcal{O}_L$. Therefore $c_1 \equiv \ldots \equiv c_l \bmod \mathfrak{P}$, hence mod p.

References

[1] J. Coates and A. Wiles, *On p-adic L-functions and elliptic units*, J. Austral. Math. Soc. 26 (1978), 1–25.
[2] V. Ennola, *On relations between cyclotomic units*, J. Number Theory 4 (1972), 236–247.
[3] R. Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. 98 (1976), 263–284.
[4] K. Iwasawa, *On cohomology groups of units for $\mathbb{Z}_p$-extensions*, ibid. 105 (1983), 189–200.
[5] J. M. Kim, *Cohomology groups of cyclotomic units*, J. Algebra 152 (1992), 514–519.
[6] —, *Coates–Wiles series and Mirimanoff's polynomial*, J. Number Theory, to appear.
[7] —, *Units and cyclotomic units in $\mathbb{Z}_p$-extensions*, Nagoya Math. J. (1995), to appear.
[8] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer, New York, 1972.
[9] W. Sinnott, *On the Stickelberger ideal and the circular units of a cyclotomic field*, Ann. of Math. 108 (1978), 107–134.
[10] L. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Math. 83, Springer, New York, 1980.

DEPARTMENT OF MATHEMATICS
INHA UNIVERSITY, INCHON, KOREA
E-mail: JMKIM@MUNHAK.INHA.AC.KR

Received on 17.8.1994
and in revised form on 2.11.1994 (2656)