Tôhoku Math. Journ.
36 (1984), 439–452.

ON THE STARK-SHINTANI CONJECTURE AND CYCLOTOMIC Z_p-EXTENSIONS OF CLASS FIELDS OVER REAL QUADRATIC FIELDS II

JIN NAKAGAWA

(Received October 5, 1983)

Introduction. Let p be a prime number, and denote by $\boldsymbol{Z}_p$ the ring of p-adic integers. In our previous paper [9], we have constructed certain cyclotomic $\boldsymbol{Z}_p$-extensions $M_\infty = \bigcup_{n\geqq 0} M_n$ such that the Stark-Shintani invariants for M_n are units of M_n for each $n \geqq 0$. In this paper, we study the image of these units in the completion of M_∞ at a prime over p.

Let F be a real quadratic field embedded in the real number field $\boldsymbol{R}$. Let M be a finite abelian extension of F in which exactly one of the two infinite primes of F, corresponding to the prescribed embedding of F into $\boldsymbol{R}$, splits. Let $\mathfrak{f}$ be the conductor of M/F. Denote by $H_F(\mathfrak{f})$ the group consisting of all narrow ray classes of F defined modulo $\mathfrak{f}$. Let G be the subgroup of $H_F(\mathfrak{f})$ corresponding to M by class field theory. Take a totally positive integer ν of F satisfying $\nu + 1 \in \mathfrak{f}$, and denote by the same letter ν the narrow ray class modulo $\mathfrak{f}$ represented by the principal ideal (ν). For each $c \in H_F(\mathfrak{f})$, set $\zeta_F(s, c) = \sum N(\mathfrak{a})^{-s}$, where $\mathfrak{a}$ runs over all integral ideals of F belonging to the ray class c. Then the Stark-Shintani ray class invariant $X_\mathfrak{f}(c)$ is defined by

$$X_\mathfrak{f}(c) = \exp(\zeta'_F(0, c) - \zeta'_F(0, c\nu)) \tag{1}$$

(Stark [12], [13], Shintani [11]). Put $X_\mathfrak{f}(c, G) = \prod_{g\in G} X_\mathfrak{f}(cg)$.

CONJECTURE ([12], [13], [11]). For some positive rational integer m, $X_\mathfrak{f}(c, G)^m$ is a unit of M ($\forall c \in H_F(\mathfrak{f})/G$). Moreover, $\{X_\mathfrak{f}(c, G)^m\}^{\sigma(c_0)} = X_\mathfrak{f}(cc_0, G)^m$ ($\forall c, c_0 \in H_F(\mathfrak{f})/G$), where σ is the Artin isomorphism of $H_F(\mathfrak{f})/G$ onto the Galois group $\mathrm{Gal}(M/F)$.

Denote by M^+ the maximal totally real subfield of M. Then Shintani proved that the conjecture is true if M^+ is abelian over the rational number field $\boldsymbol{Q}$ ([11]). In our previous paper, we have studied the integer m in the conjecture when M^+ is abelian over $\boldsymbol{Q}$, and we have constructed abelian extensions M of F with the following property (P) for an odd prime number p (cf. Theorem 1, Propositions 8, 9, 10 and 13 of [9]):

(P) Let $M_\infty = \bigcup_{n\geqq 0} M_n$ be the cyclotomic Z_p-extension of M. Then $X_{\mathfrak{f}_n}(c, G_n)$ is a unit of M_n for each $c \in H_F(\mathfrak{f}_n)/G_n$, where $\mathfrak{f}_n$ is the conductor of M_F/F and G_n is the subgroup of $H_F(\mathfrak{f}_n)$ corresponding to M_n ($\forall n \geqq 0$). Moreover, $X_{\mathfrak{f}_n}(c, G_n)^{\sigma(c_0)} = \pm X_{\mathfrak{f}_n}(cc_0, G_n)$ ($\forall c, c_0 \in H_F(\mathfrak{f}_n)/G_n$).

In this paper, we assume that M has the property (P) for an odd prime number p with $p \nmid [M:F]$. Further we assume that the following condition (D) is satisfied:

(D) For any subfield M' of M/F with $M' \not\subset M^+$, any prime divisor $\mathfrak{p}$ of $\mathfrak{f}$ is a divisor of $\mathfrak{f}(M')$ or a divisor of p, where $\mathfrak{f}(M')$ is the conductor of M'/F. Moreover, if $\mathfrak{p}$ is a prime divisor of p with $\mathfrak{p} \nmid \mathfrak{f}(M')$, then the decomposition field of $\mathfrak{p}$ in M'/F is $(M')^+$.

For a number field k, denote by $E(k)$, $A(k)$ and $h(k)$ the group of units of k, the ideal class group of k and the class number of k respectively. Put $E(M)^- = \{u \in E(M); N_{M/M^+}(u) = 1\}$. Denote by $C(M)$ the subgroup of $E(M)$ generated by -1 and $X_{\mathfrak{f}}(c, G)$ ($c \in H_F(\mathfrak{f})/G$). Then we can show that $C(M)$ is a subgroup of $E(M)^-$, and we can rewrite Arakawa's class number formula as follows (cf. [1], [9]):

$$(2) \qquad h(M)/h(M^+) = [E(M)^- : C(M)] \times (\text{a power of } 2)\,.$$

Put $E_n^- = E(M_n)^-$, $C_n = C(M_n)$ and $h_n^- = h(M_n)/h(M_n^+)$ ($n \geqq 0$). If there is a prime divisor $\mathfrak{p}$ of p with $\mathfrak{p} \nmid \mathfrak{f}$, then we replace C_0 by the subgroup generated by -1 and $X_{\mathfrak{f}}(c, G)^{2^e}$ ($c \in H_F(\mathfrak{f})/G$), where e is the number of such prime divisors $\mathfrak{p}$ of p. In §1, we shall prove the following theorem which is analogous to classical results on cyclotomic units and elliptic units.

THEOREM 1. *Notation and assumption being as above, we have*

$$(\mathrm{i}) \qquad h_n^- = [E_n^- : C_n] \times (\text{a power of } 2) \qquad (n \geqq 0)\,,$$

$$(\mathrm{ii}) \qquad N_{n,m}(C_m) = C_n \qquad (m \geqq n \geqq 0)\,,$$

where $N_{n,m}$ is the norm map of M_m to M_n.

COROLLARY. *Put $B_n = \{c \in A(M_n); N_{M_n/M_n^+}(c) = 1$, the order of c is odd$\}$. If h_1^- is prime to p, then the natural homomorphism $B_n \to B_m$ is injective for any $m \geqq n \geqq 0$.*

In §4, we shall study the image of C_n in the completion of M_∞ at a prime over p by using a result of Coleman ([4]). §§2-3 are devoted to preparations for the arguments in §4. As a consequence of Theorem 1 of [9], Theorem 1 and the main result in §4 (Theorem 3), we obtain

THEOREM 2. *Let p be an odd prime which splits in F ($p = \mathfrak{p}\mathfrak{p}'$).*

Take an integer α of F such that $\alpha > 0$, $\alpha' < 0$, $\alpha \in \mathfrak{p}$, $\alpha \notin \mathfrak{p}^2$ and $\alpha \notin \mathfrak{p}'$ (α' is the conjugate of α). Put $\alpha\alpha' = -ap$, and assume that a is a quadratic residue modulo p and $T_{F/Q}(\alpha)$ is not. Let $M = F(\sqrt{\alpha})$ and let $X_{\mathfrak{f}}(1, G) = (x + y\sqrt{\alpha})/2$, where x and y are integers of F. If y is prime to $\mathfrak{p}$ then h_n^- is prime to p for any $n \geqq 0$.

REMARK. By (i) of Theorem 1, $\mathfrak{p} \nmid (y)$ implies $p \nmid h_0^-$. On the other hand, the general theory of Z_p-extensions tells that $p \nmid h_1^-$ implies $p \nmid h_n^-$ ($^\forall n \geqq 0$). But in general, $p \nmid h_0^-$ does not imply $p \nmid h_0^-$ ($^\forall n \geqq 0$).

1. Proof of Theorem 1.

In this section, we prove Theorem 1 and Corollary. First, we prove

LEMMA 1.1. *$C(M)$ is a subgroup of $E(M)^-$.*

PROOF. Put $\eta = X_{\mathfrak{f}}(c, G)$ and $\beta = T_{M/M^+}(\eta)$. It follows from (P) and (1) that $\eta^{\sigma(\nu)} = \pm\eta^{-1}$. Since $\sigma(\nu)$ is the generator of Gal(M/M^+), this implies that $N_{M/M^+}(\eta) = \pm 1$. If $N_{M/M^+}(\eta) = -1$, $\eta = (\beta + \sqrt{\beta^2 + 4})/2$. Since $\beta \in M^+$, η is a totally real algebraic number of M. Hence $\eta \in M^+$. This contradicts to $N_{M/M^+}(\eta) = -1$. q.e.d.

Now we prove the equality (2). Let χ be a character of $H_F(\mathfrak{f})/G$ with $\chi(\nu) = -1$. It follows from (1) that

$$L'_F(0, \chi) = \sum_{c \in H_F(\mathfrak{f})/\langle G, \nu\rangle} \chi(c) \log X_{\mathfrak{f}}(c, G) . \tag{3}$$

Denote by $\mathfrak{f}_\chi$ and $\tilde{\chi}$ the conductor of χ and the primitive character associated to χ respectively. Then we have

$$L_F(s, \chi) = L_F(s, \tilde{\chi}) \prod_{\mathfrak{p} | \mathfrak{f}, \mathfrak{p} \nmid \mathfrak{f}_\chi} (1 - \tilde{\chi}(\mathfrak{p}) N(\mathfrak{p})^{-s}) . \tag{4}$$

It follows from the functional equation of $L_F(s, \tilde{\chi})$ that $L_F(0, \tilde{\chi}) = 0$. Hence we obtain

$$L'_F(0, \chi) = L'_F(0, \tilde{\chi}) \prod_{\mathfrak{p} | \mathfrak{f}, \mathfrak{p} \nmid \mathfrak{f}_\chi} (1 - \tilde{\chi}(\mathfrak{p})) . \tag{5}$$

It is easy to see that $\tilde{\chi}(\mathfrak{p}) = \tilde{\chi}(\nu) = -1$ in (5) under the assumption (D). On the other hand, the analytic class number formula at $s = 0$ (cf. p. 200 of Stark [14]) tells us

$$h(M)/h(M^+) = (R(M^+)/R(M)) \prod_{\chi, \chi(\nu) = -1} L'_F(0, \tilde{\chi}) , \tag{6}$$

where $R(M)$ and $R(M^+)$ are regulators of M and M^+ respectively. The equality (2) follows from (3), (5), (6) and a slightly modified version of the Frobenius determinant formula.

PROOF OF THEOREM 1. Let $F_\infty = \bigcup_{n \geqq 0} F_n$ be the cyclotomic Z_p-

extension of F ($[F_n: F] = p^n$). Since $[M: F]$ is prime to p, $M_n = MF_n$ and any subfield of M_n/F is a composition of a subfield of M with a subfield of F_n. This implies that the condition (D) is satisfied for M_n. Hence the equality (2) is also valid for M_n. This proves the first half of Theorem 1. Let $m \geqq n \geqq 1$. Denote by $\mathfrak{P}(\mathfrak{f}_n)$ the set of prime divisors of $\mathfrak{f}_n$. Then $\mathfrak{P}(\mathfrak{f}_m) = \mathfrak{P}(\mathfrak{f}_n)$. Let $\varphi: H_F(\mathfrak{f}_m)/G_m \to H_F(\mathfrak{f}_n)/G_n$ be the natural surjective homomorphism, and let ν_n be the ν for $\mathfrak{f}_n$. For any character χ of $H_F(f_n)/G_n$ with $\chi(\nu_n) = -1$, put $\chi' = \chi \circ \varphi$. Then χ' is a character of $H_F(\mathfrak{f}_m)/G_m$ with $\chi'(\nu_m) = -1$. Since $\mathfrak{P}(\mathfrak{f}_m) = \mathfrak{P}(\mathfrak{f}_n)$, the equality (4) implies that $L_F(s, \chi) = L_F(s, \chi')$. Then it follows from (3) that

$$\sum_{c_0 \in H_F(\mathfrak{f}_n)/\langle G_n, \nu_n\rangle} \chi(c_0) \log X_{\mathfrak{f}_n}(c_0, G_n) = \sum_{c \in H_F(\mathfrak{f}_m)/\langle G_m, \nu_m\rangle} \chi'(c) \log X_{\mathfrak{f}_m}(c, G_m)$$
$$= \sum_{c_0 \in H_F(\mathfrak{f}_n)/\langle G_n, \nu_n\rangle} \chi(c_0)\{\sum_{c \in \varphi^{-1}(c_0)} \log X_{\mathfrak{f}_m}(c, G_m)\} .$$

This implies that $X_{\mathfrak{f}_n}(c_0, G_n) = \prod_{c \in \varphi^{-1}(c_0)} X_{\mathfrak{f}_m}(c, G_m)$. Since $\sigma(\operatorname{Ker} \varphi) = \operatorname{Gal}(M_m/M_n)$, we obtain $X_{\mathfrak{f}_n}(\varphi(c), G_n) = \pm N_{n,m}(X_{\mathfrak{f}_m}(c, G_m))$. Hence $N_{n,m}(C_m) = C_n$. When $n = 0$, it follows from (5) that

$$L'_F(0, \chi') = L'_F(0, \chi) \prod_{\mathfrak{p} | \mathfrak{f}_m, \mathfrak{p} \nmid \mathfrak{f}} (1 - \chi(\mathfrak{p}))$$
$$= L'_F(0, \chi) \times 2^e \qquad (e = \#\{\mathfrak{p}; \mathfrak{p} | p, \mathfrak{p} \nmid \mathfrak{f}\}) .$$

The rest of the proof goes similarly to that of the case $n \geqq 1$. This completes the proof of Theorem 1.

Put $\Gamma = \operatorname{Gal}(M_\infty/M)$ $(\cong \boldsymbol{Z}_p)$. Take a topological generator γ of Γ and fix it. Put $\Gamma_n = \operatorname{Gal}(M_\infty/M_n)$ and $\Delta = \operatorname{Gal}(M_\infty/F_\infty)$. Then $\operatorname{Gal}(M_\infty/F) = \Gamma \times \Delta$ and Δ is naturally isomorphic to $\operatorname{Gal}(M/F)$. Put $\rho = (\sigma(\nu_n))_{n \geqq 0} \in \operatorname{proj\,lim} \operatorname{Gal}(M_n/F) = \operatorname{Gal}(M_\infty/F)$. Obviously $\rho \in \Delta$, $\rho^2 = 1$ and $\rho \neq 1$. Put $r = [M^+: F]$, and let $\sigma_1, \cdots, \sigma_r$ $(\in \Delta)$ be a complete set of representatives of $\Delta/\langle\rho\rangle$. Put $\eta_n = X_{\mathfrak{f}_n}(1, G_n)$. It follows from the assumption (P) that $X_{\mathfrak{f}_n}(c, G_n) = \pm X_{\mathfrak{f}_n}(1, G_n)^{\sigma(c)}$ for any $c \in H_F(\mathfrak{f}_n)/G_n$ and $X_{\mathfrak{f}_n}(c, G_n)^{\sigma(\nu_n)} = X_{\mathfrak{f}_n}(c, G_n)^{-1}$. Hence C_n is generated by -1 and $\eta_n^{\sigma_i\gamma^j}$ $(1 \leqq i \leqq r, 0 \leqq j \leqq p^n - 1)$. Furthermore, (i) of Theorem 1 implies that the units $\eta_n^{\sigma_i\gamma^j}$ $(1 \leqq i \leqq r, 0 \leqq j \leqq p^n - 1)$ are multiplicatively independent. Denote by $\boldsymbol{Z}[\Gamma_n/\Gamma_m]$ the group ring of Γ_n/Γ_m over the ring of rational integers $\boldsymbol{Z}$ $(m \geqq n \geqq 0)$. Then $C_m/\pm 1$ is a free $\boldsymbol{Z}[\Gamma_n/\Gamma_m]$-module of rank rp^n generated by $\eta_m^{\sigma_i\gamma^j}$ $(1 \leqq i \leqq r,\ 0 \leqq j \leqq p^n - 1)$. This implies that $H^k(\Gamma_n/\Gamma_m, C_m) = 0$ for any k, $m \geqq n \geqq 0$. Since Γ_n/Γ_m is a cyclic group of order p^{m-n}, $H^1(\Gamma_n/\Gamma_m, C_m) = 0$ implies that $\operatorname{Ker}(N_{n,m}: C_m \to C_n) = (C_m)^{\omega_n}$, where $\omega_n = \gamma^{p^n} - 1$. Further, $H^0(\Gamma_n/\Gamma_m, C_m) = 0$ implies that $C_m \cap M_n = N_{n,m}(C_m) = C_n$. In particular, the natural homomorphism $E_n^-/C_n \to E_m^-/C_m$

is injective for any $m \geqq n \geqq 0$. Thus we have proved

PROPOSITION 1.2. (i) *$H^k(\Gamma_n/\Gamma_m, C_m) = 0$, for any k, $m \geqq n \geqq 0$.*

(ii) *$C_m \cap E_n = C_n$, hence the natural homomorphism $E_n^-/C_n \to E_m^-/C_m$ is injective for any $m \geqq n \geqq 0$.*

(iii) *$0 \to (C_m)^{\omega_n} \to C_m \xrightarrow[N_{n,m}]{} C_n \to 0$ (exact), for any $m \geqq n \geqq 0$.*

To prove the corollary to Theorem 1, we need the following lemma.

LEMMA 1.3. *Let B_n be as in the corollary. Then we have an injective homomorphism*

$$\mathrm{Ker}\,(B_n \to B_m) \to \mathrm{Ker}\,(N_{n,m}\colon E_m^- \to E_n^-)/(E_m^- \cap (E_m)^{\omega_n}),$$

for any $m \geqq n \geqq 0$.

PROOF. Let $c \in \mathrm{Ker}\,(B_n \to B_m)$. Take an ideal $\mathfrak{a}$ of M_n in the class c. It is easy to see that $\mathfrak{a}$ can be taken to satisfy $\mathfrak{a} = (\alpha)$ for some $\alpha \in M_m$ with $\alpha^\rho = \alpha^{-1}$. Then we put $\varepsilon = \alpha^{\omega_n}$. Since $\gamma_n = \gamma^{p^n}$ induces the identity map on M_n, $\mathfrak{a}^{\gamma_n} = \mathfrak{a}$, hence $(\alpha^{\gamma_n}) = (\alpha)$ as principal ideals of M_m. So $\varepsilon = \alpha^{\omega_n} = \alpha^{\gamma_n - 1}$ is a unit of M_m. Since $\alpha^\rho = \alpha^{-1}$, $\varepsilon \in E_m^-$. On the other hand, $N_{n,m}(\varepsilon) = N_{n,m}(\alpha^{\omega_n}) = 1$. Hence we define a map $\mathrm{Ker}\,(B_n \to B_m) \to \mathrm{Ker}\,(N_{n,m}\colon E_m^- \to E_n^-)/(E_m^- \cap (E_m)^{\omega_n})$ by $c \mapsto \varepsilon \bmod (E_m^- \cap (E_m)^{\omega_n})$. It is easy to check that this map is a well-defined injective homomorphism. q.e.d.

Now we prove the corollary to Theorem 1. Since $[M\colon F]$ is prime to p, any prime of M lying over p is totally ramified in M_∞/M. Hence $p \nmid h_1^-$ implies $p \nmid h_n^-$ for all $n \geqq 0$ by a well known fact in the theory of Z_p-extensions (cf. Theorem 6 of Iwasawa [6]). By (i) of Theorem 1, the order of the group E_n^-/C_n is prime to p. Since Γ_n/Γ_m is a cyclic group of order p^{m-n}, we have $H^k(\Gamma_n/\Gamma_m, E_m^-/C_m) = 0$. By (i) of Proposition 1.2, we have $H^k(\Gamma_n/\Gamma_m, C_m) = 0$. Hence we obtain $H^k(\Gamma_n/\Gamma_m, E_m^-) = 0$. Since $(E_m^-)^{\omega_n} \subset E_m^- \cap (E_m)^{\omega_n} \subset \mathrm{Ker}\,(N_{n,m}\colon E_m^- \to E_n^-)$, and since $H^1(\Gamma_n/\Gamma_m, E_m^-) = \mathrm{Ker}\,(N_{n,m}\colon E_m^- \to E_n^-)/(E_m^-)^{\omega_n}$, we have $\mathrm{Ker}\,(N_{n,m}\colon E_m^- \to E_n^-) = E_m^- \cap (E_m)^{\omega_n} = (E_m^-)^{\omega_n}$. Hence $\mathrm{Ker}\,(B_n \to B_m) = 0$ by Lemma 1.3. This completes the proof of the corollary.

REMARK 1.4. If the number of prime divisors of p in M is one, $p \nmid h_0^-$ implies $p \nmid h_n^-$ for all $n \geqq 0$ (cf. Proposition 13.22 of Washington [15]).

2. A basis for the local units. In this section, we study the group of units of certain abelian extensions of the p-adic number field $\boldsymbol{Q}_p$. The results in this section are slight generalizations of some facts mentioned in Chapter 7 of Lang [7].

Let p be an odd prime number and let d (>0) be a divisor of $p-1$. Let Φ be the unique unramified extension of $\boldsymbol{Q}_p$ of degree d. Put $\Phi_n = \Phi(\zeta_n)$, where ζ_n is a primitive p^{n+1}-th root of unity in a fixed algebraic closure Ω of Φ. We choose $(\zeta_n)_{n\geq 0}$ to satisfy $\zeta_{n+1}^p = \zeta_n$ for any $n \geqq 0$. Put $\Phi_\infty = \bigcup_{n\geq 0} \Phi_n$, $H = \mathrm{Gal}(\Phi_\infty/\boldsymbol{Q}_p)$ and $\Gamma = \mathrm{Gal}(\Phi_\infty/\Phi_0)$. Since $[\Phi_0 : \boldsymbol{Q}_p]$ is prime to p, there is a finite subgroup Δ of H such that $H = \Gamma \times \Delta$ and Δ is naturally isomorphic to $\mathrm{Gal}(\Phi_0/\boldsymbol{Q}_p)$. Since Δ is an abelian group of exponent $p-1$, any character $\chi\colon \Delta \to \Omega^\times$ is $\boldsymbol{Z}_p^\times$-valued. Denote by $\hat{\Delta}$ the set of all $\boldsymbol{Z}_p^\times$-valued characters of Δ. Let ϕ be the unique element of Δ such that $\phi | \boldsymbol{Q}_p(\zeta_0) = id$ and $\phi | \Phi$ is the Frobenius automorphism of $\Phi/\boldsymbol{Q}_p$. Let τ be an element of Δ such that $\tau | \Phi = id$ and $\tau | \boldsymbol{Q}_p(\zeta_0)$ is a generator of $\mathrm{Gal}(\boldsymbol{Q}_p(\zeta_0)/\boldsymbol{Q}_p)$. Let $\kappa\colon \mathrm{Gal}(\Phi_\infty/\Phi) = \Gamma \times \langle\tau\rangle \to \boldsymbol{Z}_p^\times$ be the canonical character (i.e. κ is characterized by $\zeta_n^g = \zeta_n^{\kappa(g)}$ for any $n \geqq 0$ and any $g \in \Gamma \times \langle\tau\rangle$). Then $\mu_{p-1} = \kappa(\tau)$ is a primitive $(p-1)$-th root of unity in $\boldsymbol{Z}_p$. Let μ_d be a fixed primitive d-th root of unity in $\boldsymbol{Z}_p$. Define $\chi_{i,j} \in \hat{\Delta}$ by $\chi_{i,j}(\phi) = \mu_d^i$, $\chi_{i,j}(\tau) = \mu_{p-1}^j$ ($i \in \boldsymbol{Z}/d\boldsymbol{Z}$, $j \in \boldsymbol{Z}/(p-1)\boldsymbol{Z}$).

For any $\boldsymbol{Z}_p[\Delta]$-module A, put $A(\chi) = e(\chi)A$, where $e(\chi) = (1/\# \Delta) \sum_{g\in\Delta} \chi^{-1}(g)g$ ($\in \boldsymbol{Z}_p[\Delta]$). Then $A(\chi) = \{a \in A; ga = \chi(g)a \text{ for any } g \in \Delta\}$, and $A = \bigoplus_{\chi\in\hat{\Delta}} A(\chi)$.

Let $\mathfrak{o}$ and $\mathfrak{o}_n$ be the ring of integers of Φ and Φ_n respectively ($n \geqq 0$). Let $\mathfrak{p}$ and $\mathfrak{p}_n$ be the maximal ideal of $\mathfrak{o}$ and $\mathfrak{o}_n$ respectively. Put $\pi_n = \zeta_n - 1$ ($n \geqq 0$). Then $\mathfrak{p} = p\mathfrak{o}$ and $\mathfrak{p}_n = \pi_n\mathfrak{o}_n$. Denote by V the group of (p^d-1)-th roots of unity in Φ. Put $U_n = \{u \in \mathfrak{o}_n; u \equiv 1 \bmod \mathfrak{p}_n\}$. Denote by $N_{n,m}$ the norm map of Φ_m to Φ_n ($m \geqq n \geqq 0$), and put $U_\infty = \mathrm{proj\,lim}\, U_n$ (the limit is taken with respect to $N_{n,m}$). Then U_∞ is a compact $\boldsymbol{Z}_p[H]$-module and $U_\infty = \bigoplus_\chi U_\infty(\chi)$. Let Λ be the ring of formal power series in an indeterminate T with coefficients in $\boldsymbol{Z}_p$: $\Lambda = \boldsymbol{Z}_p[[T]]$. Let γ be a fixed topological generator of Γ ($\cong \boldsymbol{Z}_p$). Obviously, $U_\infty(\chi) = \mathrm{proj\,lim}\, U_n(\chi)$ and $U_\infty(\chi)$ is a compact Γ-module, hence a compact Λ-module (the action of T is given by $(1+T)u = u^\gamma$ for any $u \in U_\infty(\chi)$). The Λ-module structure of $U_\infty(\chi)$ is given by the following proposition which can be proved by the same arguments as in Chapter 7 of [7].

PROPOSITION 2.1. *For any $\chi \in \hat{\Delta}$ with $\chi \neq \chi_{0,0}$, the natural projection $U_\infty(\chi) \to U_n(\chi)$ induces an isomorphism $U_\infty(\chi)/\omega_n U_\infty(\chi) \simeq U_n(\chi)$, where $\omega_n = (1+T)^{p^n} - 1$ ($n \geqq 0$). If $\chi \neq \chi_{0,0}, \chi_{0,1}$, then we have a Λ-isomorphism $U_\infty(\chi) \cong \Lambda$.*

Let $\chi \neq \chi_{0,0}, \chi_{0,1}$. We are going to construct a basis for $U_\infty(\chi)$ over Λ. Take an element λ of V with $\lambda \neq 1$, and put $b = \lambda - 1$. Then b is a unit of $\mathfrak{o}$ and $b^\phi = \lambda^\phi - 1 = \lambda^p - 1$, because $\phi|_\Phi$ is the Frobenius automorphism of Φ. For any unit x of $\mathfrak{o}$, denote by $\omega(x)$ the unique element of V such that $\omega(x) \equiv x \bmod \mathfrak{p}$. Put $v_n = \omega(b)^{-\phi^{-n}}(b^{\phi^{-n}} - \pi_n)$. Obviously $v_n \in U_n$, and it is easy to check $N_{n,m}(v_m) = v_n$ for any $m \geqq n \geqq 0$. Hence $v = (v_n)_{n \geqq 0}$ is an element of U_∞. Now we claim that we can choose $\lambda \in V$ such that $v^{e(\chi)} = (v_n^{e(\chi)})_{n \geqq 0}$ is a basis for $U_\infty(\chi)$ over Λ. To prove this, we define homomorphisms $\psi_k: \mathfrak{o}_0^\times \to \mathfrak{o}/\mathfrak{p}$ $(1 \leqq k \leqq p-2)$ as follows:

Let $D = (1+T)(d/dT)$. For each $u \in \mathfrak{o}_0^\times$, take a power series $f(T) \in \mathfrak{o}[[T]]$ such that $f(\pi_0) = u$. Put $\psi_k(u) = D^k \log f(T)|_{T=0} \bmod \mathfrak{p}$. This does not depend on a choice of $f(T)$. Hence ψ_k is a well-defined homomorphism.

Note that $U_0(\chi)$ is a free Z_p-module of rank one. If $\chi = \chi_{i,j}$, $1 \leqq j \leqq p-2$, then we can check $\psi_j(v_0^{e(\chi)}) \neq 0$ for some $\lambda \in V$ by the same argument as in §3, Chapter 7 of [7]. If $\chi = \chi_{i,0}$, we can check $\delta_{p-1}(v^{e(\chi)}) \not\equiv 0 \bmod \mathfrak{p}$ for some λ similarly, where δ_{p-1} is the Coates-Wiles homomorphism defined in the next section. Then $v_0^{e(\chi)}$ generates $U_0(\chi)/U_0(\chi)^p$, hence generates $U_0(\chi)$ over Z_p by Nakayama's lemma. By Proposition 2.1 and Nakayama's lemma, this implies that $v^{e(\chi)}$ is a basis for $U_\infty(\chi)$ over Λ. Hence we obtain

PROPOSITION 2.2. *Let $\chi \in \hat{\Delta}$, $\chi \neq \chi_{0,0}$, $\chi_{0,1}$. Then $v^{e(\chi)} = (v_n^{e(\chi)})_{n \geqq 0}$ is a basis for $U_\infty(\chi)$ over Λ for a suitable choice of $\lambda \in V$ (depending on χ).*

3. Logarithmic derivatives. We use the same notation as in the previous section. First, we recall the following result of Coleman ([4]).

PROPOSITION 3.1. *Let $u = (u_n) \in U_\infty$. Then there is a unique power series $f_u(T) \in \mathfrak{o}[[T]]$ such that*

$$f_u^{\phi^{-n}}(\pi_n) = u_n \qquad \text{for all} \quad n \geqq 0$$

(for $f(T) = \sum a_m T^m$ $(a_m \in \mathfrak{o})$, $f^{\phi^{-n}}(T) = \sum a_m^{\phi^{-n}} T^m$).

Let $u = (u_n) \in U_\infty$, and let $f_u(T)$ be the power series associated to u by Proposition 3.1. Let $D = (1+T)(d/dT)$. For each integer $k \geqq 1$, we define the Coates-Wiles homomorphism $\delta_k: U_\infty \to \mathfrak{o}$ by

$$(7) \qquad \begin{aligned} \delta_k(u) &= D^k \log f_u(T)|_{T=0} \\ &= D^{k-1}((1+T)f_u'(T)/f_u(T))|_{T=0}\,. \end{aligned}$$

Put $T = e^Z - 1 = \sum_{m \geqq 1}(Z^m/m!)$. Then $(dT/dZ) = e^Z = 1 + T$ and $D = (d/dZ)$, hence

$$(8) \qquad \delta_k(u) = \left(\frac{d}{dZ}\right)^k \log f_u(e^Z - 1)|_{Z=0}\,.$$

It is easy to see that the map δ_k has the following properties (cf. §13.7 of [15]).

PROPOSITION 3.2. *The map* $\delta_k\colon U_\infty \to \mathfrak{o}$ *is a continuous* $\boldsymbol{Z}_p$*-homomorphism satisfying*

(i) $\delta_k(u^g) = \kappa(g)^k \delta_k(u)$ *for* $\forall g \in \Gamma \times \langle\tau\rangle$, $\forall u \in U_\infty$,

(ii) $\delta_k(u^\phi) = \delta_k(u)^\phi$ *for* $\forall u \in U_\infty$.

In particular, if $u \in U_\infty(\chi_{i,j})$ *with* $j \not\equiv k \bmod (p-1)$, *then* $\delta_k(u) = 0$. *Further,* $\delta_k(h(T)u) = h(\kappa(\gamma)^k - 1)\delta_k(u)$ *for* $\forall h(T) \in \Lambda$, $\forall u \in U_\infty$.

Let $\chi = \chi_{i,j}$, $(i, j) \neq (0, 0)$, $(0, 1)$ $(0 \leqq i \leqq d-1, 1 \leqq j \leqq p-1)$. Let $v^{e(\chi)}$ be the basis for $U_\infty(\chi)$ over Λ constructed in §2. If $k \not\equiv j \bmod (p-1)$, then $\delta_k(v^{e(\chi)}) = 0$ by Proposition 3.2. So we assume $k \equiv j \bmod (p-1)$, $k \geqq 1$. By Proposition 3.2, we have

$$\delta_k(v^{e(\chi)}) = \frac{1}{\# \Delta} \sum_{s=0}^{d-1} \sum_{t=1}^{p-1} \chi_{i,j}^{-1}(\phi^s \tau^t) \kappa(\tau^t)^k \delta_k(v)^{\phi^s} = d^{-1} \sum_{s=0}^{d-1} \mu_d^{-is} \delta_k(v)^{\phi^s} . \tag{9}$$

Let $|\ |$ be a p-adic valuation of Φ. Let Q be the set of power series $\sum_{n\geqq 0} a_n T^n$ in $\Phi[[T]]$ such that $|a_n n!| \to 0$ as $n \to \infty$. Let C be the set of continuous functions from $\boldsymbol{Z}_p$ to Φ. Then Q and C are Banach algebras over Φ with norms $\sup |a_n n!|$ and $\max_{s \in \boldsymbol{Z}_p} |f(s)|$, respectively. To calculate $\delta_k(v)$, we need the following two facts on a slight generalization of Leopoldt's Γ-transform (see §1 of Lichtenbaum [8]).

LEMMA 3.3. *For each* $j \in \boldsymbol{Z}/(p-1)\boldsymbol{Z}$, *there is a unique bounded linear map* $\Gamma_j\colon Q \to C$ *such that*

$$\Gamma_j(h)(k) = \left(\frac{d}{dZ}\right)^k \tilde{h}(e^Z - 1)|_{Z=0} \qquad (k \geqq 0,\ k \equiv j \bmod (p-1)) ,$$

where $\tilde{h}(T) = h(T) - p^{-1} \sum_{i=0}^{p-1} h(\zeta_0^i(1+T) - 1)$ $(h \in Q)$.

LEMMA 3.4. *For any* $h \in \mathfrak{o}[[T]]$, $\Gamma_j(h)$ *is an Iwasawa function i.e. there is a power series* $g \in \mathfrak{o}[[T]]$ *such that*

$$\Gamma_j(h)(s) = g(\kappa(\gamma)^s - 1) \qquad (\forall s \in \boldsymbol{Z}_p) .$$

We return to the calculation of $\delta_k(v)$. We recall that $v = (v_n)$, $v_n = \omega(b)^{-\phi^{-n}}(b^{\phi^{-n}} - \pi_n)$, $b = \lambda - 1$ for some $\lambda \in V$, $\lambda \neq 1$. Then the power series associated to v is given by

$$f_v(T) = \omega(b)^{-1}(b - T) .$$

Put $h(T) = (1+T)f_v'(T)/f_v(T) = (1+T)/(1+T-\lambda)$. Then $\delta_k(v) = (d/dZ)^{k-1} h(e^Z - 1)|_{Z=0}$, and $\tilde{h}(T) = (1+T)/(1+T-\lambda) - p^{-1} \sum_{i=0}^{p-1} \zeta_0^i(1+T)/(\zeta_0^i(1+T) - \lambda)$. Taking the logarithmic derivatives of $X^p - \lambda^p = \prod_{i=0}^{p-1} (\zeta_0^i X - \lambda)$, we obtain

$$pX^{p-1}/(X^p - \lambda^p) = \sum_{i=0}^{p-1} \zeta_0^i/(\zeta_0^i X - \lambda)\,, \quad \text{where} \quad X = 1 + T\,.$$

Hence $\tilde{h}(T) = h(\mathrm{T}) - h^\phi((1 + T)^p - 1)$, and

$$\left(\frac{d}{dZ}\right)^{k-1} \tilde{h}(e^Z - 1)|_{Z=0} = \left(\frac{d}{dZ}\right)^{k-1} \{h(e^Z - 1) - h^\phi(e^{pZ} - 1)\}|_{Z=0}$$
$$= \delta_k(v) - p^{k-1}\delta_k(v)^\phi\,.$$

Replacing v by v^{ϕ^s} in the above equality, we obtain

$$\text{(10)} \qquad \delta_k(v)^{\phi^s} - p^{k-1}\delta_k(v)^{\phi^{s+1}} = \left(\frac{d}{dZ}\right)^{k-1} \tilde{h}^{\phi^s}(e^Z - 1)|_{Z=0}$$
$$(0 \leqq s \leqq d - 1)\,.$$

By Lemma 3.3, the right side of (10) is $\Gamma_{j-1}(h^{\phi^s})(k - 1)$. If $k \geqq 2$, then we can solve the liner equations (10) with respect to $\delta_k(v)^{\phi^s}$:

$$\text{(11)} \qquad \delta_k(v)^{\phi^s} = (1 - p^{d(k-1)})^{-1} \sum_{t=0}^{d-1} p^{t(k-1)} \Gamma_{j-1}(h^{\phi^{s+t}})(k - 1)$$
$$(0 \leqq s \leqq d - 1)\,.$$

It follows from (9) and (11) that

$$\text{(12)} \qquad (1 - \mu_d^i p^{k-1})\delta_k(v^{e(\chi)}) = d^{-1} \sum_{t=0}^{d-1} \mu_d^{-it} \Gamma_{j-1}(h^{\phi^t})(k - 1)\,.$$

If $k = 1$, then $j = 1$ and $i \not\equiv 0 \bmod d$. It is easy to check that the equality (12) is also valid for $k = 1$. Since $h^{\phi^t} \in \mathfrak{o}[[T]]$, $\Gamma_{j-1}(h^{\phi^t})$ is an Iwasawa function by Lemma 3.4. Hence there is a power series $a_\chi(T) \in \mathfrak{o}[[T]]$ such that

$$\text{(13)} \qquad (1 - \mu_d^i p^{k-1})\delta_k(v^{e(\chi)}) = a_\chi(\kappa(\gamma)^{k-1} - 1)$$
$$\text{for any} \quad k \geqq 1,\ k \equiv j \bmod (p - 1)\,.$$

Put $b_\chi(T) = a_\chi(\kappa(\gamma)^{-1}(1 + T) - 1)$, then $b_\chi(T) \in \mathfrak{o}[[T]]$ and $b_\chi(\kappa(\gamma)^k - 1) = a_\chi(\kappa(\gamma)^{k-1} - 1)$. It follows from the proof of Proposition 2.2 that $\delta_j(v^{e(\chi)}) \bmod \mathfrak{p} = \psi_j(v_0^{e(\chi)}) \neq 0$. This implies that $b_\chi(T)$ is a unit in $\mathfrak{o}[[T]]$. Note $\mu_d^i = \chi(\phi)$. Thus we have proved

PROPOSITION 3.5. *Let $\chi = \chi_{i,j}$, $\chi \neq \chi_{0,0}$, $\chi_{0,1}$, and let $v^{e(\chi)}$ be the basis for $U_\infty(\chi)$ over Λ constructed in* §2. *Then there is a unit power series $b_\chi(T)$ in $\mathfrak{o}[[T]]$ such that*

$$(1 - \chi(\phi)p^{k-1})\delta_k(v^{e(\chi)}) = b_\chi(\kappa(\gamma)^k - 1)$$

for any $k \geqq 1$, $k \equiv j \bmod (p - 1)$.

4. The closure of the Stark-Shintani units. Let F be a real quadratic field embedded in $\boldsymbol{R}$, and let p be an odd prime number which splits in F ($p = \mathfrak{p}\mathfrak{p}'$). Further assume $p \not\equiv 1 \bmod 8$. Take an integer α of F such that $\alpha > 0$, $\alpha' < 0$, $\alpha \in \mathfrak{p}$, $\alpha \notin \mathfrak{p}^2$ and $\alpha \notin \mathfrak{p}'$. Put $\alpha\alpha' = -ap$, and assume that a is a quadratic residue modulo p and $T_{F/Q}(\alpha)$ is not. Put $M = F(\sqrt{\alpha})$, $N = F(\sqrt{p^*\alpha})$, where $p^* = (-1)^{(p-1)/2}p$. Then it is easy to see that $\mathfrak{p}$ ramifies in M and remains prime in N, and $\mathfrak{p}'$ ramifies in N and remains prime in M. Put $M_0 = M\boldsymbol{Q}(\zeta_0)^+$ (ζ_0 is a primitive p-th root of unity). Then M_0 satisfies the condition (D). Further, M_0 has the property (P) by the results of [9] (see Theorem 1, Proposition 10 and Remark after Proposition 13 of [9]). Hence we can apply Theorem 1 to the cyclotomic $\boldsymbol{Z}_p$-extension $M_\infty = \bigcup_{n\geq 0} M_n$ of M_0.

Let $\mathfrak{f}_n$ be the conductor of M_n/F and let G_n be the subgroup of $H_F(\mathfrak{f}_n)$ corresponding to M_n. Put $\eta_n = X_{\mathfrak{f}_n}(1, G_n)$. We have seen in the proof of Theorem 1 that

(14) $$N_{n,m}(\eta_m) = \pm\eta_n \qquad \text{for any} \quad m \geqq n \geqq 0\,.$$

Put $K_n = M(\zeta_n)$, and put $K_\infty = \bigcup_{n\geq 0} K_n$. Since $\boldsymbol{Q}(\sqrt{p^*})$ is contained in $\boldsymbol{Q}(\zeta_0)$, N is contained in K_0. Since $\mathfrak{p}$ is totally ramified in $F(\zeta_n)$ and remains prime in N, there is a unique prime $\mathfrak{p}_n$ of $K_n = NF(\zeta_n)$ lying over $\mathfrak{p}$. Since p splits in F, the completion of F at $\mathfrak{p}$ is identified with $\boldsymbol{Q}_p$. Let Φ be the completion of N at $\mathfrak{p}$, and let Φ_n be the completion of K_n at $\mathfrak{p}_n$. Then Φ is the unramified extension of $\boldsymbol{Q}_p$ of degree 2 and $\Phi_n = \Phi(\zeta_n)$. Hence we are in the situation of §§2-3 with $d = 2$. So we use the same notation as in §§2-3 without further comment. Note that $\mathrm{Gal}(K_\infty/F)$ is naturally isomorphic to $H = \mathrm{Gal}(\Phi_\infty/\boldsymbol{Q}_p)$.

We can view the unit $X_{\mathfrak{f}_n}(c, G_n)$ of M_n as a unit of Φ_n by the inclusions $M_n \subset K_n \subset \Phi_n$. Put $\xi_n = \eta_n^{p^2-1}$. Then $\xi_n \equiv 1 \bmod \mathfrak{p}_n$. Let $\mathscr{C}_n$ be the subgroup of $E(M_n)^-$ generated by $(\xi_n)^{\gamma^s\tau^t}$ $(0 \leqq s \leqq p^n - 1, 1 \leqq t \leqq (p-1)/2)$. Then $\mathscr{C}_n$ is a subgroup of U_n. Let $\bar{\mathscr{C}}_n$ be the closure of $\mathscr{C}_n$ in U_n. Since $\mathscr{C}_n$ is stable under the action of H, $\bar{\mathscr{C}}_n$ is a $\boldsymbol{Z}_p[H]$-module. Hence we have a decomposition $\bar{\mathscr{C}}_n = \bigoplus_\chi \bar{\mathscr{C}}_n(\chi)$. It follows from the definition of τ and ϕ that $\phi|M_n$ is the generator of $\mathrm{Gal}(M_n/M_n^+)$ and $(\tau\phi)^{(p-1)/2}$ induces the identity mapping on M_n. Hence $(\xi_n)^\phi = \xi_n^{-1}$ and $(\xi_n)^{(\tau\phi)(p-1)/2} = \xi_n$. This implies that $\bar{\mathscr{C}}_n(\chi_{i,j}) = 1$ for $i = 0$ or $j \not\equiv (p-1)/2 \bmod 2$.

LEMMA 4.1. *Let $\chi = \chi_{1,j}$, $j \equiv (p-1)/2 \bmod 2$. Then the elements $\xi_n^{e(\chi)\gamma^s}$ $(0 \leqq s \leqq p^n - 1)$ of $\bar{\mathscr{C}}_n(\chi)$ are multiplicatively independent over $\boldsymbol{Z}_p$.*

PROOF. Put $r = (p-1)/2$. We have observed that $\bar{\mathscr{C}}_n = \bigoplus_j \bar{\mathscr{C}}_n(\chi_{1,j})$, where j runs over the r integers satisfying $1 \leqq j \leqq 2r$, $j \equiv r \bmod 2$.

Since $(\xi_n^{\gamma^s\tau^t})^{e(\chi)} = (\xi_n^{e(\chi)\gamma^s})^{\chi(\tau^t)}$, $\bar{\mathscr{E}}_n(\chi)$ is generated by $\xi_n^{e(\chi)\gamma^s}$ $(0 \leqq s \leqq p^n - 1)$ over $\boldsymbol{Z}_p$ and the $\boldsymbol{Z}_p$-rank of $\bar{\mathscr{E}}_n(\chi)$ is at most p^n. So it suffices to show that the $\boldsymbol{Z}_p$-rank of $\bar{\mathscr{E}}_n$ equals to rp^n. But $\xi_n^{\gamma^s\tau^t}$ $(0 \leqq s \leqq p^n - 1, 1 \leqq t \leqq r)$ are independent units of M_n by Theorem 1. Hence they are multiplicatively independent over $\boldsymbol{Z}_p$ by a theorem of Brumer ([2]). Then the $\boldsymbol{Z}_p$-rank of $\bar{\mathscr{E}}_n$ is rp^n. q.e.d.

Let $\bar{\mathscr{E}}_\infty = \text{proj lim}\, \bar{\mathscr{E}}_n$ (with respect to $N_{n,m}$). Then $\bar{\mathscr{E}}_\infty$ is a compact H-module. For each χ, $\bar{\mathscr{E}}_\infty(\chi) = \text{proj lim}\, \bar{\mathscr{E}}_n(\chi)$ and $\bar{\mathscr{E}}_\infty(\chi)$ is a compact Γ-module, hence a compact Λ-module. Note that $\xi = (\xi_n)_{n \geqq 0}$ is an element of $\bar{\mathscr{E}}_\infty$ by (14). Our purpose is to relate the Λ-module structure of $U_\infty(\chi)/\bar{\mathscr{E}}_\infty(\chi)$ to the values of δ_k at ξ.

LEMMA 4.2. *$\bar{\mathscr{E}}_\infty(\chi) = \Lambda\xi^{e(\chi)}$ for any $\chi \in \hat{\Delta}$.*

This lemma is proved by the same argument as in p. 314 of [15]. Now we are ready to prove the following proposition.

PROPOSITION 4.3. *Let χ be as in Lemma 4.1.*

(i) *The natural projection $\bar{\mathscr{E}}_\infty(\chi) \to \bar{\mathscr{E}}_n(\chi)$ induces an isomorphism $\bar{\mathscr{E}}_\infty(\chi)/\omega_n\bar{\mathscr{E}}_\infty(\chi) \xrightarrow{\sim} \bar{\mathscr{E}}_n(\chi)$ for any $n \geqq 0$.*

(ii) *$\Lambda \cong \bar{\mathscr{E}}_\infty(\chi)$ by $f(T) \mapsto f(T)\xi^{e(\chi)}$.*

(iii) *$(U_\infty(\chi)/\bar{\mathscr{E}}_\infty(\chi))^{(n)} \xrightarrow{\sim} U_n(\chi)/\bar{\mathscr{E}}_n(\chi)$ for any $n \geqq 0$, where $A^{(n)} = A/\omega_n A$ for any compact Λ-module A.*

PROOF. It follows from (14) that the natural projection $\bar{\mathscr{E}}_\infty(\chi) \to \bar{\mathscr{E}}_n(\chi)$ is surjective. Obviously $\omega_n\bar{\mathscr{E}}_\infty(\chi)$ is contained in the kernel. Let $u = (u_m)$ be in the kernel. Hence $u_n = 1$. By Lemma 4.2, $u = f(T)\xi^{e(\chi)}$ for some $f(T) \in \Lambda$. Then $f(T)\xi_n^{e(\chi)} = u_n = 1$ and $\omega_n\xi_n^{e(\chi)} = 1$. By Lemma 4.1, this implies that $f(T) \equiv 0 \bmod \omega_n\Lambda$. Hence $u \in \omega_n\bar{\mathscr{E}}_\infty(\chi)$. This proves the first statement. The second statement follows immediately from Proposition 2.1 and Lemma 4.2. The natural projection $U_\infty(\chi) \to U_n(\chi)$ is surjective and its kernel is $\omega_n U_\infty(\chi)$ by Proposition 2.1. Further it maps $\bar{\mathscr{E}}_\infty(\chi)$ onto $\bar{\mathscr{E}}_n(\chi)$ by (i). Hence the natural homomorphism $U_\infty(\chi) \to U_n(\chi)/\bar{\mathscr{E}}_n(\chi)$ is surjective and its kernel is $\omega_n U_\infty(\chi)\bar{\mathscr{E}}_\infty(\chi)$. This proves the third statement. q.e.d.

The following theorem is the main result of this section.

THEOREM 3. *Let $\chi = \chi_{1,j}$, $1 \leqq j \leqq p - 1$, $j \equiv (p-1)/2 \bmod 2$. Then there are two power series $f_\chi(T) \in \Lambda$, $g_\chi(T) \in \mathfrak{o}[[T]]$ with the following properties:*

(i) *$U_\infty(\chi)/\bar{\mathscr{E}}_\infty(\chi) \cong \Lambda/f_\chi(T)\Lambda$ as Λ-modules.*

(ii) $(1+p^{k-1})\delta_k(\xi)=g_\chi(\kappa(\gamma)^k-1)$ *for any* $k\geqq 1$, $k\equiv j \bmod (p-1)$.
(iii) $f_\chi(T)\mathfrak{o}[[T]]=g_\chi(T)\mathfrak{o}[[T]]$.

PROOF. Let $v^{e(\chi)}$ be the basis for $U_\infty(\chi)$ over Λ in §2. Since $\overline{\mathscr{C}}_\infty(\chi)=\Lambda\xi^{e(\chi)}\subset U_\infty(\chi)=\Lambda v^{e(\chi)}$, there is a power series $f_\chi(T)\in\Lambda$ such that $\xi^{e(\chi)}=f_\chi(T)v^{e(\chi)}$. Then $U_\infty(\chi)/\overline{\mathscr{C}}_\infty(\chi)\cong\Lambda/f_\chi(T)\Lambda$ as Λ-modules. Let $b_\chi(T)$ be the unit power series in Proposition 3.5, and put $g_\chi(T)=b_\chi(T)f_\chi(T)$. Since $\xi^\phi=\xi^{-1}$ and $\chi(\phi)=-1$, Proposition 3.2 implies that $\delta_k(\xi)=\delta_k(\xi^{e(\chi)})$ for $k\geqq 1$, $k\equiv j \bmod (p-1)$ (cf. (9)). Then it follows from Propositions 3.2 and 3.5 that

$$\begin{aligned}(1+p^{k-1})\delta_k(\xi)&=(1+p^{k-1})f_\chi(\kappa(\gamma)^k-1)\delta_k(v^{e(\chi)})\\&=f_\chi(\kappa(\gamma)^k-1)b_\chi(\kappa(\gamma)^k-1)\\&=g_\chi(\kappa(\gamma)^k-1)\end{aligned}$$

for any $k\geqq 1$, $k\equiv j \bmod (p-1)$. q.e.d.

We may view the above theorem as a weak analogue of a result of Iwasawa on cyclotomic units and a result of Coates-Wiles on elliptic units. It is known that the values of δ_k at the limit of cyclotomic units (resp. elliptic units) are essentially the values of the corresponding L-function at integers and the p-adic analytic function $\boldsymbol{Z}_p\ni s\mapsto g_\chi(\kappa(\gamma)^s-1)$ is essentially the p-adic L-function of Kubota-Leopoldt (resp. the p-adic L-function associated to an elliptic curve) (cf. [3], [5]).

COROLLARY. *Let* $p\equiv 3 \bmod 4$. *Put* $h_n^-=h(M_n)/h(M_n^+)$, $\eta_0=X_{\mathfrak{f}_0}(1, G_0)$. *If* $\psi_j(\eta_0)\neq 0$ *for any odd integer* j *with* $1\leqq j\leqq p-1$, *then* h_n^- *is prime to* p *for any* $n\geqq 0$.

PROOF. Since $\delta_j(\xi) \bmod \mathfrak{p}=\psi_j(\xi_0)=(p^2-1)\psi_j(\eta_0)$, $\psi_j(\eta_0)\neq 0$ implies $\delta_j(\xi)\not\equiv 0 \bmod \mathfrak{p}$. Hence $g_\chi(T)$ and $f_\chi(T)$ are unit power series and $U_\infty(\chi)/\overline{\mathscr{C}}_\infty(\chi)$ is trivial for $\chi=\chi_{1,j}$, $1\leqq j\leqq (p-1)$, $j\equiv 1 \bmod 2$ by Theorem 3. Then it follows from (iii) of Proposition 4.3 that $U_n(\chi_{1,j})=\overline{\mathscr{C}}_n(\chi_{1,j})$ for odd j with $1\leqq j\leqq (p-1)$. Since $\overline{\mathscr{C}}_n=\bigoplus_{j\text{ odd}}\overline{\mathscr{C}}_n(\chi_{1,j})$ and the $\boldsymbol{Z}_p$-rank of $\overline{\mathscr{C}}_n$ equals to the $\boldsymbol{Z}$-rank of $E(M_n)^-$ $(=p^n(p-1)/2)$, this implies that $[E(M_n)^-:\mathscr{C}_n]$ is prime to p. Hence h_n^- is prime to p by Theorem 1. q.e.d.

REMARK. The above corollary gives a sufficient condition for $p\nmid h_n^-$ $(\forall n\geqq 0)$ in terms of certain congruences which can be calculated by knowing a special unit η_0 of M_0.

Now we prove Theorem 2 stated in the introduction. Note that the assumption on M and p in Theorem 2 is the same as in the beginning of this section except that we need not assume $p \not\equiv 1 \bmod 8$ in Theorem 2. We keep the notations Φ_n, U_n, γ, ϕ, τ and $\chi_{i,j}$ as before. But in this time, let $M_0 = M$ and let $M_\infty = \bigcup_{n\geq 0} M_n$ be the cyclotomic $\boldsymbol{Z}_p$-extension of M. Then $[M_n: F] = 2p^n$ and $M_n \subset MQ(\zeta_n)^+ \subset \Phi_n$. Further the condition (D) is trivial since M/F is a quadratic extension, and M has the property (P) by Theorem 1 of [9]. Hence we can define η_n, ξ_n, $\bar{\mathscr{C}}_n$ and $\bar{\mathscr{C}}_\infty$ similarly. Then it follows from the definition of ϕ (resp. τ) that $\phi|M_n$ (resp. $\tau|M_n$) is the generator of $\mathrm{Gal}(M_n/M_n^+)$. Hence $\xi_n^\phi = \xi_n^\tau = \xi_n^{-1}$. This implies that $\bar{\mathscr{C}}_n = \bar{\mathscr{C}}_n(\chi_{1,r})$ and $\bar{\mathscr{C}}_\infty = \bar{\mathscr{C}}_\infty(\chi_{1,r})$ for $r = (p-1)/2$. Then we can prove that the same statements as in Theorem 3 and its corollary also hold for this case. So it suffices to show that $\psi_r(\eta_0) \neq 0$ under the assumption of Theorem 2. Put $\eta_0 = (x + y\sqrt{\alpha})/2$ (x and y are integers of F). Then $x \not\equiv 0 \bmod \mathfrak{p}$, since η_0 is a unit of F and α is a prime element of $F_\mathfrak{p}$ ($F_\mathfrak{p}$ is the completion of F at $\mathfrak{p}$ and $F_\mathfrak{p}$ is identified with $\boldsymbol{Q}_p$). Since the ramification index for $\Phi_0/F_\mathfrak{p}$ is $(p-1)$ $(=2r)$ and $M \subset M(\xi_0) \subset \Phi_0$, there is a unit u of Φ_0 such that $\sqrt{\alpha} = \pi_0^r u$, $\pi_0 = \zeta_0 - 1$. Write $u = g(\pi_0)$, $g(T) = a_0 + a_1 T + \cdots \in \mathfrak{o}[[T]]$. Then a_0 is a unit of $\mathfrak{o}$. Put $f(T) = (1/2)(x + yT^r g(T))$. Then $f(T) \in \mathfrak{o}[[T]]$ and $\eta_0 = f(\pi_0)$. Recall that $D = (1+T)(d/dT)$. Then

$$D(\log f(T)) = \frac{(1+T)(ryT^{r-1}g(T) + yT^r g'(T))}{x + yT^r g(T)}$$
$$\equiv r a_0 x^{-1} y T^{r-1} \bmod T^r \mathfrak{o}[[T]] .$$

Since $D^{r-1}(T^k)|_{T=0} = 0$ if $k \geqq r$ and $D^{r-1}(T^{r-1})|_{T=0} = (r-1)!$, we obtain

$$\psi_r(\eta_0) = D^r(\log f(T))|_{T=0} \bmod \mathfrak{p}$$
$$= r!\, a_0 x^{-1} y \bmod \mathfrak{p} .$$

Since $r!\, a_0 x^{-1}$ is a unit of $\mathfrak{o}$, $\psi_r(\eta_0) \neq 0$ is equivalent to $y \not\equiv 0 \bmod \mathfrak{p}$. This completes the proof of Theorem 2.

We conclude this paper by giving an example of Theorem 2.

EXAMPLE. Let $F = \boldsymbol{Q}(\sqrt{5})$. Put $\varepsilon = (3 + \sqrt{5})/2$. Let $p = 11$ and let $\alpha = (-1 + 3\sqrt{5})/2$. Then p splits in F and $\alpha\alpha' = -p$. Hence the assumption of Theorem 2 is satisfied. Let $M = F(\sqrt{\alpha})$. Then it was shown in pp. 191-192 of [10] that

$$X_\mathfrak{f}(1, G) = (\varepsilon + \sqrt{\alpha})/2 .$$

Hence $11 \nmid h_n^-$ for any $n \geqq 0$ by Theorem 2. This is also an example of the corollary to Theorem 1.

REFERENCES

[1] T. ARAKAWA, On the Stark-Shintani conjecture and certain relative class numbers, to appear.

[2] A. BRUMER, On the units of algebraic number fields, Mathematika, 14 (1967), 121–124.

[3] J. COATES AND A. WILES, On p-adic L-functions and elliptic units, J. Austral. Math. Soc., Ser. A, 26 (1978), 1–25.

[4] R. F. COLEMAN, Division values in local fields, Invent. Math. 53 (1979), 91–116.

[5] K. IWASAWA, On some modules in the theory of cyclotomic fields, J. Math. Soc. Japan, 16 (1964), 42–82.

[6] K. IWASAWA, On $\boldsymbol{Z}_l$-extensions of algebraic number fields, Ann. of Math. 98 (1973), 246–326.

[7] S. LANG, Cyclotomic Fields, Springer-Verlag, New York, 1978.

[8] S. LICHTENBAUM, On p-adic L-functions associated to elliptic curves, Invent. Math. 56 (1980), 19–55.

[9] J. NAKAGAWA, On the Stark-Shintani conjecture and cyclotomic $\boldsymbol{Z}_p$-extensions of class fields over real quadratic fields, to appear in J. Math. Soc. Japan.

[10] T. SHINTANI, On a Kronecker limit formula for real quadratic fields, J. Fac. Sci. Univ. Tokyo, Sec. IA, 24 (1977), 167–199.

[11] T. SHINTANI, On certain ray class invariants of real quadratic fields, J. Math. Soc. Japan, 30 (1978), 139–167.

[12] H. M. STARK, L-functions at $s=1$. III. Totally real fields and Hilbert's twelfth problem, Advances in Math. 22 (1976), 64–84.

[13] H. M. STARK, Class fields for real quadratic fields and L-series at $s=1$, Proc. Durham Conf., pp. 355–374, Academic Press, New York, 1977.

[14] H. M. STARK, L-functions at $s=1$. IV. First derivatives at $s=0$, Advances in Math. 35 (1980), 197–235.

[15] L. C. WASHINGTON, Introduction to Cyclotomic Fields, Springer-Verlag, New York, 1982.

MATHEMATICAL INSTITUTE
TÔHOKU UNIVERSITY
SENDAI 980
JAPAN