TOKYO J. MATH.
VOL. 27, NO. 2, 2004

On a Theorem of Kawamoto on Normal Bases of Rings of Integers

Humio ICHIMURA

Yokohama City University

(Communicated by T. Kawasaki)

1. Introduction

A finite Galois extension L/K over a number field K has a relative normal integral basis (NIB for short) when $\mathcal{O}_L$ is free over the group ring $\mathcal{O}_K[\mathrm{Gal}(L/K)]$. Here, $\mathcal{O}_L$ (resp. $\mathcal{O}_K$) is the ring of integers of L (resp. K). It is well known by Noether that if L/K has a NIB, then L/K is tame (i.e., at most tamely ramified at all finite prime divisors). It is also well known by Hilbert and Speiser that when the base field K equals the rationals $\mathbf{Q}$, all tame abelian extensions $L/\mathbf{Q}$ have a NIB. Recently, Greither et al. [3] proved that there exists no Hilbert-Speiser number field other than $\mathbf{Q}$. Namely, they proved that when $K \neq \mathbf{Q}$, there exist a prime number p and a tame cyclic extension L/K of degree p having no NIB.

On the other hand, Kawamoto [7, 8] obtained the following result. For a prime number p, let ζ_p be a fixed primitive p-th root of unity.

THEOREM 1 (Kawamoto). *For a prime number p and a rational number $a \in \mathbf{Q}^\times$, the cyclic extension $\mathbf{Q}(\zeta_p,\ a^{1/p})/\mathbf{Q}(\zeta_p)$ has a NIB if it is tame.*

In [2, Theorem 2.1], Gómez Ayala gave a necessary and sufficient condition for a tame Kummer extension of prime degree to have a NIB, and deduced Theorem 1 from this criterion. For a prime number p, we say that a number field F enjoys the property (H_p) when for any element $a \in F^\times$, the cyclic extension $F(\zeta_p,\ a^{1/p})/F(\zeta_p)$ has a NIB if it is tame. Theorem 1 says that the rationals $\mathbf{Q}$ satisfies the property (H_p) for all p. Analogous to the result of Greither et al., it is shown in [5, IV] that when $F \neq \mathbf{Q}$, there exists a prime number p for which F does not satisfy (H_p). For a prime number p and a number field F with $\zeta_p \in F^\times$, we gave, in [5, V, Propositions 1, 2], a necessary and sufficient condition for (H_p) to be satisfied.

Received August 5, 2003; revised November 20, 2003
The author was partially supported by Grant-in-Aid for Scientific Research (C), (No. 16540033), the Ministry of Education, Culture, Sports, Science and Technology of Japan.

In this paper, we fix a prime number $p \geq 3$, and give some sufficient (resp. necessary) conditions for a number field F to satisfy (H_p) in the general case where F does not necessarily contain ζ_p. The conditions are obtained by using [2, Theorem 2.1], and similarly to [5, V, Propositions 1, 2], they are given in terms of the class number, the ideal class group of F and the group of units of $K = F(\zeta_p)$. Using these, we prove the following results when $p = 3$ and F is a quadratic field.

THEOREM 2. *Let $p = 3$ and $F = \mathbf{Q}(\sqrt{d})$ be an imaginary quadratic field with d a square free negative integer. Then, F enjoys the property (H_3) if and only if $d = -1, -2, -3$, or -11.*

Let $F = \mathbf{Q}(\sqrt{d})$ be a real quadratic field with d a square free positive integer, and let h_F be the class number of F and $\varepsilon = (t + u\sqrt{d})/2$ a fundamental unit of F. We write $t = t_F$ and $u = u_F$. We denote by λ (resp. μ) a prime number ≥ 5 with $\lambda \equiv 1 \bmod 4$ (resp. $\mu \equiv 3 \bmod 4$). When we write μ_1 and μ_2 (for example), we mean that μ_1, μ_2 are different prime numbers ≥ 5 with $\mu_1 \equiv \mu_2 \equiv 3 \bmod 4$.

THEOREM 3. *Let $p = 3$ and $F = \mathbf{Q}(\sqrt{d})$ be a real quadratic field with d a square free positive integer. Then, F enjoys the property (H_3) if and only if F satisfies the following three conditions;*

i) *d is of the form; $d = 2, 3, 6, \lambda, \mu, 2\mu, 3\mu$, or $\mu_1\mu_2$.*
ii) *$h_F = 1$,*
iii) *$3 \nmid u_F$, and further $3 \nmid t_F$ when $d \equiv -1 \bmod 3$.*

QUESTION. By Theorems 2 and 3, we have $h_F = 1$ for any quadratic field F satisfying (H_3). Does there exist a number field F with $h_F > 1$ satisfying (H_p) for some prime number $p \geq 3$?

This paper is organized as follows. In Section 2, we give a sufficient condition (resp. two necessary conditions) for a number field to satisfy (H_p). In Section 3, we show the results in Section 2. We prove Theorems 2 and 3 in Section 5 after preparing many lemmas in Section 4.

2. Conditions for (H_p)

For a number field K, let E_K (resp. h_K) be the group of units (resp. class number) of K. For an integral ideal $\mathfrak{A}$ of K, let $[E_K]_{\mathfrak{A}}$ be the subgroup of the multiplicative group $(\mathcal{O}_K/\mathfrak{A})^\times$ consisting of classes containing units of K. For an integer $a \in \mathcal{O}_K$, we simply write $\mathcal{O}_K/a = \mathcal{O}_K/a\mathcal{O}_K$ and $[E_K]_a = [E_K]_{a\mathcal{O}_K}$. Let $p \geq 3$ be a fixed prime number, F a number field, and $K = F(\zeta_p)$. Then, we can naturally regard $(\mathcal{O}_F/p)^\times$ as a subgroup of $(\mathcal{O}_K/p)^\times$. The following sufficient condition for (H_p) is an immediate consequence of [2, Theorem 2.1].

PROPOSITION 1. *Let $p \geq 3$ be a prime number, F a number field, and $K = F(\zeta_p)$. Assume that* (i) $h_F = 1$ *and that* (ii) $(\mathcal{O}_F/p)^\times \subseteq [E_K]_p$. *Then, F satisfies the condition* (H_p).

We give a criterion which assures the condition $(\mathcal{O}_F/p)^\times \subseteq [E_K]_p$. For a prime number p, let $\pi_p = \zeta_p - 1$. When p is unramified in F, we can naturally regard $(\mathcal{O}_F/p)^\times$ as a subgroup of $(\mathcal{O}_K/\pi_p)^\times$.

PROPOSITION 2. *Let p, F, K be as in Proposition* 1. *Assume that* (a) *p is unramified in F and that* (b) $(\mathcal{O}_F/p)^\times \subseteq [E_K]_{\pi_p}$. *Then, we have* $(\mathcal{O}_F/p)^\times \subseteq [E_K]_p$.

COROLLARY 1. *Let p, F, K be as in Proposition* 1. *Assume that $h_F = 1$ and that the conditions of Proposition* 2 *are satisfied. Then, F satisfies the condition* (H_p).

Let us give necessary conditions for (H_p). For a number field F, let Cl_F be the ideal class group in the usual sense.

PROPOSITION 3. *Let p, F, K be as in Proposition* 1, *and let $\ell = [K : F]$. Assume that F satisfies (H_p). Then, all ideal classes of F capitulate in K. In particular, the exponent of Cl_F divides ℓ.*

PROPOSITION 4. *Let p, F, K be as in Proposition* 1. *Assume that F satisfies (H_p). Then, for any integer u of F relatively prime to p, we have $u \equiv \varepsilon \bmod \pi_p$ for some unit $\varepsilon \in E_K$.*

The following is immediate from Corollary 1 and Proposition 4.

COROLLARY 2. *Let p, F, K be as in Proposition* 1. *Assume that $h_F = 1$ and that p is unramified in F. Then, F satisfies (H_p) if and only if* $(\mathcal{O}_F/p)^\times \subseteq [E_K]_{\pi_p}$.

REMARK 1. Let $p \geq 3$ be a prime number, $F = \mathbf{Q}$, and $K = \mathbf{Q}(\zeta_p)$. Then, the conditions of Proposition 2 are satisfied. Actually, for a rational integer $a \in \mathbf{Z}$ relatively prime to p, the cyclotomic unit $c_a = (\zeta_p^a - 1)/(\zeta_p - 1)$ satisfies the congruence $c_a \equiv a \bmod \pi_p$. Hence, Theorem 1 of Kawamoto follows form Corollary 1. Further, by Proposition 2, we have $\mathbf{F}_p^\times = (\mathbf{Z}/p)^\times \subseteq [E_K]_p$, which we use in an argument in Section 4.

REMARK 2. Let F be a totally real number field and $K = F(\sqrt{-1})$. In [6, Corollary 4], a result corresponding to Proposition 1 is given for cyclic quartic extensions $K(a^{1/4})/K$ with $a \in F^\times$.

3. Proofs of Propositions

3.1. A theorem of Gómez Ayala. Let us first recall a theorem of Gómez Ayala [2, Theorem 2.1] mentioned in Sections 1 and 2. Let p be a prime number, and K a number field. Let $\mathfrak{A}$ be an integral ideal of K which is p-th power free in the semi-group of integral ideals of K. Then, we can uniquely write

$$\mathfrak{A} = \prod_{i=1}^{p-1} \mathfrak{A}_i{}^i \tag{1}$$

for some square free integral ideals $\mathfrak{A}_i$ of K relatively prime to each other. The associated ideals $\mathfrak{B}_j$ of $\mathfrak{A}$ are defined by

$$\mathfrak{B}_j = \prod_{i=1}^{p-1} \mathfrak{A}_i{}^{[ij/p]} \quad (0 \leq j \leq p-1)\,. \tag{2}$$

Here, for a real number x, $[x]$ denotes the largest integer with $[x] \leq x$. By the definition, we have $\mathfrak{B}_0 = \mathfrak{B}_1 = \mathcal{O}_K$.

THEOREM 4 (Gómez Ayala). *Let p be a prime number and K a number field with $\zeta_p \in K^\times$. Then, a cyclic extension L/K of degree p is tame and has a NIB if and only if there exists an integer a of K relatively prime to p satisfying the following four conditions*;

i) $L = K(a^{1/p})$,

ii) *the integral ideal $a\mathcal{O}_K$ is p-th power free*,

iii) *the associated ideals $\mathfrak{B}_j$ of $a\mathcal{O}_K$ defined by* (1) *and* (2) *are principal*, *and finally*,

iv) *letting $\alpha = a^{1/p}$, the congruence*

$$A = \sum_{j=0}^{p-1} \frac{\alpha^j}{x_j} \equiv 0 \bmod p$$

holds for some generators x_j of the principal ideals $\mathfrak{B}_j$.

Further, *when this is the case*, *the integer $\omega = A/p$ is a generator of a NIB of L/K*; *namely*, $\mathcal{O}_L = \mathcal{O}_K[\mathrm{Gal}(L/K)] \cdot \omega$.

The following assertion is a special case of this theorem. (For this, see [5, I, Theorem 2].)

LEMMA 1. *Let p, K be as in Theorem* 4. *Let a be an integer of K relatively prime to p such that the integral principal ideal $a\mathcal{O}_K$ is square free. Then, the cyclic extension $K(a^{1/p})/K$ has a NIB if and only if a satisfies the congruence $a \equiv \varepsilon^p \bmod \pi_p^p$ for some unit $\varepsilon \in E_K$.*

The following lemma is well known (cf. Washington [14, Exercises 9.2, 9.3]).

LEMMA 2. *Let p, K be as in Theorem* 4. *For an element $a \in K^\times$ relatively prime to p, the cyclic extension $K(a^{1/p})/K$ is tame if and only if the congruence $a \equiv u^p \bmod \pi_p^p$ holds for some integer $u \in \mathcal{O}_K$.*

3.2. Proofs of Propositions 1 and 2

PROOF OF PROPOSITION 1. Let a be an element of $F^\times$ such that $K(a^{1/p})/K$ is tame. Then, as $h_F = 1$, we may as well assume that a is an integer of F relatively prime to p and that the integral ideal $a\mathcal{O}_F$ is p-th power free. Let $\mathfrak{B}_j$ be the ideals of F associated to $a\mathcal{O}_F$ by (1) and (2). Since K/F is unramified outside p, the integral ideal $a\mathcal{O}_K$ of K is also p-th power free and the ideals $\mathfrak{B}'_j = \mathfrak{B}_j\mathcal{O}_K$ are associated to $a\mathcal{O}_K$.

As $K(a^{1/p})/K$ is tame, we have $a \equiv u^p \bmod \pi_p^p$ for some $u \in \mathcal{O}_K$ by Lemma 2. Taking the norm from K to F, we see that $a \equiv v^p \bmod \pi_p^p$ for some $v \in \mathcal{O}_F$. By the condition (ii) of Proposition 1, $v \equiv \varepsilon \bmod p$ for some unit $\varepsilon \in E_K$. Hence, we obtain

$$a \equiv \varepsilon^p \bmod \pi_p^p \quad \text{with } \varepsilon \in E_K\,. \tag{3}$$

As $h_F = 1$, we have $\mathfrak{B}_j = x_j\mathcal{O}_F$ for some $x_j \in \mathcal{O}_F$. By (ii), $x_j \equiv \eta_j \bmod p$ for some unit $\eta_j \in E_K$. Letting $y_j = x_j\eta_j^{-1} \in \mathcal{O}_K$, we have $\mathfrak{B}'_j = y_j\mathcal{O}_K$ and $y_j \equiv 1 \bmod p$. Now, letting $\alpha = a^{1/p}$, we see that

$$\sum_{j=0}^{p-1} \frac{\alpha^j}{y_j\varepsilon^j} \equiv \sum_j \left(\frac{\alpha}{\varepsilon}\right)^j \equiv 0 \bmod p\,.$$

Here, the second congruence holds by (3). Therefore, $K(a^{1/p})/K$ has a NIB by Theorem 4. □

PROOF OF PROPOSITION 2. Let $\wp_1, \cdots, \wp_r$ be the prime ideals of F over p, and f_i the degree of $\wp_i$. Let f be the least common multiple of $f_1, \cdots, f_r$, and $q = p^f$. Then, for any $x \in \mathcal{O}_F$, we have $x^q \equiv x \bmod \wp_i$. This implies $x^q \equiv x \bmod p$ as p is unramified in F (the condition (a)). Let $x \in \mathcal{O}_F$ be an integer relatively prime to p. By (b), we have $x \equiv \varepsilon \bmod \pi_p$ for some unit $\varepsilon \in E_K$. Then, it follows that $x^p \equiv \varepsilon^p \bmod p$. Raising to the q/p-th power, we obtain $x \equiv x^q \equiv \varepsilon^q \bmod p$. □

3.3. Proofs of Propositions 3 and 4

PROOF OF PROPOSITION 3. Let $\wp$ be a prime ideal of F with $\wp \nmid p$, and e the order of the ideal class of F containing $\wp$. Then, $\wp^e = b_1\mathcal{O}_F$ for some $b_1 \in \mathcal{O}_F$. By the Chebotarev density theorem, there exists a principal prime ideal $\mathfrak{L} = b_2\mathcal{O}_F$ such that $b = b_1b_2 \equiv 1 \bmod \pi_p^p$. As $K(b^{1/p})/K$ is tame, it has a NIB by the assumption of Proposition 3. Hence, there exists an integer a of K relatively prime to p such that $K(a^{1/p}) = K(b^{1/p})$ and the principal ideal $a\mathcal{O}_K$ satisfies the conditions (ii) and (iii) of Theorem 4. Let $\mathfrak{B}_j$ be the ideals of K associated to $a\mathcal{O}_K$ by (1) and (2). By the condition (iii), they are principal ideals. As $K(a^{1/p}) = K(b^{1/p})$, we have $a = b^sx^p$ for some $1 \le s \le p-1$ and $x \in K^\times$. Writing $es = pf + t$ with $0 \le t \le p-1$, we obtain

$$a\mathcal{O}_K = (\wp\mathcal{O}_K)^t(\mathfrak{L}\mathcal{O}_K)^s(x\wp^f\mathcal{O}_K)^p\,.$$

By (ii), the integral ideal $a\mathcal{O}_K$ is p-th power free. Then, we must have $x\wp^f\mathcal{O}_K = \mathcal{O}_K$ in the above equality. Hence, we obtain

$$a\mathcal{O}_K = (\wp\mathcal{O}_K)^t(b_2\mathcal{O}_K)^s\,. \tag{4}$$

From $x\wp^f\mathcal{O}_K=\mathcal{O}_K$, it follows that $\wp^{\ell f}=(N_{K/F}x^{-1})\mathcal{O}_F$ where $\ell=[K:F]$. Hence, we obtain $e|\ell f$. The condition $t=0$ (namely, $es=pf$ and $f\neq 0$) contradicts this divisibility as $p\nmid \ell s$. Thus, we obtain $1\le t\le p-1$. When $t=1$, it is clear from (4) that $\wp\mathcal{O}_K$ is principal. When $2\le t\le p-1$, we can choose an integer j with $2\le j\le p-1$ so that $[jt/p]=1$. Then, from (2) and (4), we see that $\mathfrak{B}_j$ equals $\wp\mathcal{O}_K$ times a principal ideal. Therefore, $\wp\mathcal{O}_K$ is a principal ideal as so is $\mathfrak{B}_j$. $\square$

PROOF OF PROPOSITION 4. Let u be an integer of F relatively prime to p. By the Chebotarev density theorem, there exists a principal prime ideal $\mathfrak{L}=a\mathcal{O}_F$ of F such that $a\equiv u^p \bmod \pi_p^p$. By the assumption, $K(a^{1/p})/K$ has a NIB as it is tame. Then, by Lemma 1, we have $a\equiv\varepsilon^p \bmod \pi_p^p$ for some unit $\varepsilon\in E_K$. Hence, we obtain $u\equiv\varepsilon \bmod \pi_p$. $\square$

4. Lemmas

In this section, we prepare many lemmas which are necessary for proving Theorems 2 and 3. For a finite abelian group A and integers $n_i\in\mathbf{Z}$ $(1\le i\le r)$, we write $A=(n_1,\cdots,n_r)$ when A is isomorphic to the additive group $\mathbf{Z}/n_1\oplus\cdots\oplus\mathbf{Z}/n_r$. For a number field F and an integer $a\in\mathcal{O}_F$, we denote by $\langle a_1,\cdots,a_s\rangle_a$ the subgroup of $(\mathcal{O}_F/a)^\times$ generated by the classes containing integers $a_1,\cdots,a_s\in\mathcal{O}_F$ relatively prime to a. For an element α of a quadratic field, let $N\alpha$ denote the norm of α to $\mathbf{Q}$. First, we show the following:

LEMMA 3. *Let $p\ge 3$ be a prime number. Let $F=\mathbf{Q}(\sqrt{d})$ be a real quadratic field with a square free positive integer d, and $\varepsilon=(t+u\sqrt{d})/2$ a fundamental unit of F. If $p|d$ and $p\nmid u$, then we have $(\mathcal{O}_F/p)^\times\subseteq[E_K]_p$. Here, $K=F(\zeta_p)$.*

PROOF. We have $(\mathcal{O}_F/p)^\times=(p-1,\ p)$ as $p|d$. We naturally have $\mathbf{F}_p^\times=(\mathbf{Z}/p)^\times\subseteq(\mathcal{O}_F/p)^\times$. We have seen in Remark 1 that $\mathbf{F}_p^\times$ is contained in $[E_K]_p$. As $p\nmid u$, we see that $\varepsilon^4\not\equiv 1 \bmod p$. On the other hand, we see that

$$\varepsilon^{4p}\equiv(t/2)^4\equiv 1 \bmod p$$

since $p|d$ and $1=N\varepsilon^2\equiv(t/2)^4 \bmod p$. Hence, the order of the class containing ε^4 is of order p. Therefore, we obtain $(\mathcal{O}_F/p)^\times\subseteq[E_K]_p$. $\square$

Secondly, we recall a result of Hasse [4, Section 26] on unit index of imaginary abelian fields. Let $K/\mathbf{Q}$ be an imaginary $(2,\ 2)$-extension with $\zeta_3\in K^\times$, and Q_K the unit index of K. Let $K^+=\mathbf{Q}(\sqrt{d_0})$ be the maximal real subfield of K, and $\mathbf{Q}(\sqrt{-d_1})$ the imaginary quadratic subfield different from $\mathbf{Q}(\sqrt{-3})$. Here, $d_0,\ d_1$ are square free positive integers. Let ε_0 be the fundamental unit of K^+ with $\varepsilon_0>1$. The following lemma is an immediate consequence of the formulas (assertions) (8), (10), (11) and (12) in [4, Section 26].

LEMMA 4. *Under the above setting, the following assertions on Q_K hold.*

(I) *When $d_1=1$, we have $Q_K=2$, and a fundamental unit ε of K satisfies $\varepsilon^2=\sqrt{-1}\cdot\varepsilon_0$.*

(II) *When* $3|d_1$, *we have* $Q_K = 1$.

(III) *When* $d_1 > 1$ *and* $3 \nmid d_1$, *we have* $Q_K = 2$ *if and only if there exists an integer* γ_0 *of* K^+ *such that* $N\gamma_0 = \pm 3$. *Further, when this is the case, we can choose a fundamental unit* ε *of* K *so that* $\varepsilon^2 = -\varepsilon_0$.

In the following, we let $p = 3$ and let $F = \mathbf{Q}(\sqrt{d})$ be a quadratic field (real or imaginary) with $F \neq \mathbf{Q}(\sqrt{-3})$, and $K = F(\sqrt{-3})$. Here, d is a square free integer. Let $F^* = \mathbf{Q}(\sqrt{-3d})$ be the quadratic field associated to F.

LEMMA 5. *Let* $F = \mathbf{Q}(\sqrt{d})$ *be an imaginary quadratic field with* $d \neq -1, -3$. *If the prime number* 3 *is unramified in* F *and* $Q_K = 1$, *then* F *does not satisfy* (H_3).

PROOF. Let ε be a fundamental unit of the real quadratic field F^*. We have $\varepsilon \equiv \pm 1 \mod \pi_3$ as 3 is ramified in F^*. Then, as $Q_K = 1$, it follows that $[E_K]_{\pi_3} = \langle -1 \rangle_{\pi_3}$. Therefore, we obtain $(\mathcal{O}_F/3)^\times \not\subseteq [E_K]_{\pi_3}$, and hence F does not satisfy (H_3) by Proposition 4. □

LEMMA 6. *Let* $F = \mathbf{Q}(\sqrt{d})$ *be a real quadratic field with a fundamental unit* $\varepsilon = (t + u\sqrt{d})/2$. *Assume that* 3 *is unramified in* F *and* $Q_K = 1$. *Then, the following assertions hold*:

(I) *When* $d \equiv 1 \bmod 3$, *we have* $(\mathcal{O}_F/3)^\times \subseteq [E_K]_{\pi_3}$ *if and only if* $3 \nmid u$.

(II) *When* $d \equiv -1 \bmod 3$, *we have* $(\mathcal{O}_F/3)^\times \subseteq [E_K]_{\pi_3}$ *if and only if* $3 \nmid tu$.

Namely, the inclusion $(\mathcal{O}_F/3)^\times \subseteq [E_K]_{\pi_3}$ *holds if and only if the condition* (iii) *of Theorem* 3 *is satisfied.*

PROOF. We have $(\mathcal{O}_F/3)^\times = (\mathcal{O}_K/\pi_3)^\times = (2, 2)$ or (8) according to whether $d \equiv 1 \bmod 3$ or $d \equiv -1 \bmod 3$. As $Q_K = 1$, we have $[E_K]_{\pi_3} = \langle -1, \varepsilon \rangle_{\pi_3}$.

First, let $d \equiv 1 \bmod 3$. If $3|u$, then $(\mathcal{O}_F/3)^\times \not\subseteq [E_K]_{\pi_3}$ as $\varepsilon \equiv \pm 1 \bmod 3$. Assume that $3 \nmid u$. Then, as $N\varepsilon = \pm 1$, it follows that $3|t$ and hence $\varepsilon \equiv \pm\sqrt{d} \mod \pi_3$. However, we see that $\sqrt{d} \not\equiv \pm 1 \mod \pi_3$ as 3 is unramified in F. Hence, we obtain $(\mathcal{O}_F/3)^\times \subseteq [E_K]_{\pi_3}$.

Next, let $d \equiv -1 \bmod 3$. If $3|tu$, we easily see that $\varepsilon^4 \equiv 1 \mod \pi_3$, and hence $(\mathcal{O}_F/3)^\times \not\subseteq [E_K]_{\pi_3}$. Assume that $3 \nmid tu$. Then, we may as well assume that $\varepsilon \equiv 1 + \sqrt{d} \mod \pi_3$. We see that $\varepsilon^4 \equiv d \equiv -1 \mod \pi_3$, and hence $(\mathcal{O}_F/3)^\times \subseteq [E_K]_{\pi_3}$. □

We recall some lemmas from Kubota [9]. An ideal $\mathfrak{A}$ of F is called an ambiguous ideal when $\mathfrak{A}^s = \mathfrak{A}$, s being the nontrivial automorphism of F.

LEMMA 7 ([9, Hilfsatz 15]). *Let* $c \in Cl_F$ *be an ideal class of* F. *If* c *capitulates in* K, *then* $c^2 = 1$ *and* c *contains an ambiguous ideal of* F.

Let A_F be the group of ambiguous ideals of F, and $\tilde{A}_F$ its lift to K. Let $k = \mathbf{Q}(\sqrt{-3})$ $(\subseteq K)$. Let A_{F^*}, $\tilde{A}_{F^*}$ and A_k, $\tilde{A}_k$ be the corresponding objects for F^* and k, respectively. In the group of ideals of K, let A be the subgroup generated by $\tilde{A}_F$, $\tilde{A}_{F^*}$ and $\tilde{A}_k$. Let B be the group of principal ideals $x\mathcal{O}_K$ of K such that $(x\mathcal{O}_K)^2 = y\mathcal{O}_K$ for some $y \in \mathbf{Q}^\times$. Clearly, we have $B \subseteq A$. Let t be the number of prime numbers which ramify in K. Let E_K^* be the subgroup of E_K generated by all units of the intermediate fields F, F^* and k whose norm to $\mathbf{Q}$ are 1.

LEMMA 8 ([9, Hilfsatz 16]). *Under the above setting, we have* $[A : B] = 2^{t-3}[E_K : E_K^*]$.

We easily see that $\tilde{A}_F\tilde{A}_k = \tilde{A}_{F^*}\tilde{A}_k = A$ and $\tilde{A}_k \subseteq B$. Therefore, from the above lemma, we obtain the following assertion.

LEMMA 9. (I) *If all ideal classes of F capitulate in K, then we have* $2^{t-3}[E_K : E_K^*] = 1$.

(II) *Assume that the exponent of Cl_F divides 2 and that each ideal class of F contains an ambiguous ideal. Then, all ideal classes of F capitulate in K if and only if* $2^{t-3}[E_K : E_K^*] = 1$.

REMARK 3. It is known that any ideal class of F of order 2 contains an ambiguous ideal when F is imaginary or when F is real and $N\varepsilon = -1$, ε being a fundamental unit of F.

Finally, we prepare some lemmas to deal with the case where $d = 3\ell$ is a square free integer divisible by 3 and $\ell \neq 1$. Let $d = 3\ell$ be such an integer. Then, $(\mathcal{O}_F/3)^\times = (2, 3)$. Further, $(\mathcal{O}_K/3)^\times = (3, 3, 8)$ when $\ell \equiv 1 \bmod 3$, and $(\mathcal{O}_K/3)^\times = (6, 6)$ when $\ell \equiv -1 \bmod 3$. Let ε be a fundamental unit of K. Note that $\sqrt{-1} \notin K^\times$ as $\ell \neq 1$. Then, we have $E_K = \langle -1, \zeta_3, \varepsilon \rangle$, and we may as well assume that ε^2 is a real unit by Lemma 4.

LEMMA 10. *Under the above setting, assume that the order of the class $\bar{\varepsilon} \in (\mathcal{O}_K/3)^\times$ is a power of 2. Let x be an integer of F with $(x, 3) = 1$ such that the class $\bar{x}$ in $(\mathcal{O}_F/3)^\times$ is of order 3. Then, there exist no units $\delta, \eta \in E_K$ such that*

$$x \equiv \delta + \eta \bmod 3 \quad \text{and} \quad \delta \equiv \eta \bmod \pi_3 .$$

PROOF. We may as well assume that $\varepsilon \not\equiv 1 \bmod 3$ replacing ε with $-\varepsilon$ if necessary. Then, as the order of $\bar{\varepsilon}$ is a power of 2, we see that $[E_K]_3 = \langle \varepsilon, \zeta_3 \rangle_3 = (2^\alpha, 3)$ for some $\alpha \geq 1$ or $[E_K]_3 = \langle -1, \varepsilon, \zeta_3 \rangle_3 = (2, 2, 3)$. The second case can occur only when $\ell \equiv -1 \bmod 3$. To show the assertion, let us assume, to the contrary, that x satisfies the above congruence. Then, we see from the above that

$$x \equiv \pm(\zeta_3^a + \zeta_3^b)\varepsilon^c \bmod 3$$

for some $a, b, c \in \mathbf{Z}$. Here, the $-$ sign is necessary only when $[E_K]_3 = (2, 2, 3)$. Note that $\zeta_3^a + \zeta_3^b \equiv -1, -\zeta_3, -\zeta_3^2 \bmod 3$. Then, it follows from the above congruence that $x \equiv \zeta_3^r \bmod 3$ for some r because of the assumptions on the orders of $\bar{\varepsilon}$ and $\bar{x}$. As $(\mathcal{O}_F/3)^\times = (2, 3)$, we may as well assume that $x = 1 + \sqrt{3\ell}$. Then, from $x \equiv \zeta_3^r \bmod 3$, we obtain $\sqrt{3\ell} \equiv 0 \bmod 3$ or $\sqrt{-\ell} \equiv \pm 1 \bmod \pi_3$. However, we easily see that this is impossible. □

REMARK 4. Let $K^+ = \mathbf{Q}(\sqrt{d_0})$ be the maximal real subfield of K, and $\varepsilon_0 = (t + u\sqrt{d_0})/2$ a fundamental unit of K^+. When the prime 3 is unramified in K^+, the assumption on ε in Lemma 10 is satisfied. This is because of $\varepsilon_0^8 \equiv 1 \bmod 3$ and Lemma 4. When 3 is ramified in K^+ and $3|u$, the assumption is satisfied by Lemma 4 since $\varepsilon_0 \equiv \pm 1 \bmod 3$.

LEMMA 11. *Under the setting and the assumption of Lemma* 10, *let* $a \in \mathcal{O}_K$ *be an integer of* K *with* $a \notin (K^\times)^3$ *and* $a \equiv 1 \bmod \pi_3^3$. *Let* $\alpha = a^{1/3}$ $(\equiv 1 \bmod \pi_3)$. *Then, for an integer* $x \in \mathcal{O}_F$ *with* $(x, 3) = 1$, *the congruence*

$$\delta_0 + \delta_1\alpha + \frac{\delta_2\alpha^2}{x} \equiv 0 \bmod 3 \tag{5}$$

holds for some units $\delta_0, \delta_1, \delta_2 \in E_K$ *if and only if* $x \equiv \pm 1 \bmod 3$.

PROOF. As $\alpha \equiv 1 \bmod \pi_3$, we have $1 + \alpha + \alpha^2 \equiv 0 \bmod 3$. Hence, the"if" part holds with $\delta_0 = \delta_1 = 1$ and $\delta_2 = \pm 1$. Let us show the "only if" part. Let $x \in \mathcal{O}_F$ be an integer with $(x, 3) = 1$ satisfying the congruence (5). To show $x \equiv \pm 1 \bmod 3$, let us assume, to the contrary, that $x \not\equiv \pm 1 \bmod 3$. As $(\mathcal{O}_F/3)^\times = (2, 3)$, we may as well assume that the class $\bar{x} \in (\mathcal{O}_F/3)^\times$ is of order 3 replacing x with $-x$ if necessary. It follows from (5) and $1 + \alpha + \alpha^2 \equiv 0 \bmod 3$ that

$$(\delta_0 - \delta_2/x) + (\delta_1 - \delta_2/x)\alpha \equiv 0 \bmod 3\,.$$

Replacing α with $\zeta_3\alpha$, we have

$$(\delta_0 - \delta_2/x) + (\delta_1 - \delta_2/x)\zeta_3\alpha \equiv 0 \bmod 3\,.$$

Subtracting the second congruence from the first one, we obtain

$$\delta_0/\delta_2 \equiv \delta_1/\delta_2 \equiv 1/x \bmod \pi_3\,. \tag{6}$$

Then, it also follows that

$$\frac{\delta_0 - \delta_2/x}{\pi_3} + \frac{\delta_1 - \delta_2/x}{\pi_3}\alpha \equiv 0 \bmod \pi_3\,.$$

As $\alpha \equiv 1 \bmod \pi_3$, it follows from the last congruence that

$$1/x \equiv (-\delta_0/\delta_2) + (-\delta_1/\delta_2) \bmod 3\,. \tag{7}$$

However, the congruences (6) and (7) can not simultaneously hold by Lemma 10. $\square$

LEMMA 12. *Under the setting and the assumption of Lemma* 10, *there exist infinitely many classes* $\bar{a} \in F^\times/(F^\times)^3$ *for which the cyclic extension* $K(a^{1/3})/K$ *is tame but has no NIB. Namely*, F *does not satisfy* (H_3).

PROOF. By the Chebotarev density theorem, there exist infinitely many couples $(\mathfrak{L}_1, \mathfrak{L}_2)$ of principal prime ideals $\mathfrak{L}_1 = b_1\mathcal{O}_F$ and $\mathfrak{L}_2 = b_2\mathcal{O}_F$ of F such that $b_1 \equiv b_2 \equiv 1 + \sqrt{3\ell} \bmod \pi_3^3$. Put $b = b_1b_2^2$ and $b' = b_2b_1^2$. Then, $b \equiv b' \equiv 1 \bmod \pi_3^3$ and the cyclic cubic extension $K(b^{1/3}) = K(b'^{1/3})$ over K is tame. Assume that this extension has a NIB.

Then, there exists an integer $a \in \mathcal{O}_K$ with $K(a^{1/3}) = K(b^{1/3})$ satisfying the conditions of Theorem 4. We have $a = b^s y^3$ for $s \in \{1, 2\}$ and some $y \in K^\times$. When $s = 1$, $\eta = y$ is a unit of K as the ideal $a\mathcal{O}_K$ is cubic power free, and $a = b\eta^3$. When $s = 2$, $\eta = b_2 y$ is a unit of K, and $a = b'\eta^3$. Therefore, replacing a with $a\eta^{-3}$, we may as well assume that $a \equiv 1 \bmod \pi_3^3$ (as in Lemma 11). Let $\mathfrak{B}_j$ be the ideals of K associated to $a\mathcal{O}_K$ by (1) and (2). By the definition, $\mathfrak{B}_0 = \mathfrak{B}_1 = \mathcal{O}_K$, and $\mathfrak{B}_2 = \mathfrak{L}_2\mathcal{O}_K = b_2\mathcal{O}_K$ or $\mathfrak{B}_2 = \mathfrak{L}_1\mathcal{O}_K = b_1\mathcal{O}_K$ according to whether $s = 1$ or 2. Therefore, by the condition (iv) of Theorem 4, letting $\alpha = a^{1/3}$ and $x = b_1$ or b_2, the congruence (5) holds for some units $\delta_0, \delta_1, \delta_2 \in E_K$. However, this is impossible by Lemma 11 since the class $\bar{x} \in (\mathcal{O}_F/3)^\times$ is of order 3. $\square$

LEMMA 13. *Let $d = 3\ell > 0$ be a square free positive integer divisible by 3 with $\ell \neq 1$, $F = \mathbf{Q}(\sqrt{d})$, and $\varepsilon_0 = (t + u\sqrt{d})/2$ a fundamental unit of F. Under the above setting, assume that $h_F = 2$, $3 \nmid u$ and $Q_K = 1$. Then, there exist infinitely many classes $\bar{a} \in F^\times/(F^\times)^3$ for which the cyclic extension $K(a^{1/3})/K$ is tame but has no NIB. Namely, F does not satisfy (H_3).*

PROOF. As $Q_K = 1$, the prime ideal $\wp_3$ of F over 3 is not principal by Lemma 4 (III). Let $\wp_\ell$ be the product of distinct prime ideals of F dividing ℓ. As $\wp_3\wp_\ell = \sqrt{d}\mathcal{O}_F$, the ideal class containing $\wp_\ell$ is of order 2. Let $Cl_F(\wp_3^3)$ be the ray class group of F defined modulo $\wp_3^3$. As $3 \nmid u$ and $3|d$, we see that the quotient group of $(\mathcal{O}_F/\wp_3^3)^\times$ modulo $[E_F]_{\wp_3^3}$ is a cyclic group of order 3. Hence, it follows that $Cl_F(\wp_3^3)$ is a cyclic group of order 6 as $h_F = 2$. Let $\mathfrak{L}_1$ and $\mathfrak{L}_2$ be prime ideals of F contained in one class $\in Cl_F(\wp_3^3)$ of order 6. Then, we have $\mathfrak{L}_1\mathfrak{L}_2^5 = c\mathcal{O}_F$ for some integer $c \in \mathcal{O}_F$ such that $c \equiv 1 \bmod \pi_3^3$. In the usual class group Cl_F, the ideals $\mathfrak{L}_1$, $\mathfrak{L}_2$ and $\wp_\ell$ are contained in the same class as $h_F = 2$. Then, as $\wp_\ell\mathcal{O}_K = \sqrt{-\ell}\mathcal{O}_K$, we see that $\mathfrak{L}_i\mathcal{O}_K = x_i\mathcal{O}_K$ for some $x_i \in \mathcal{O}_K$ such that

$$c = x_1x_2^5 \quad \text{and} \quad \frac{x_i}{\sqrt{-\ell}} \in E_K \cdot F^\times .$$

As $3 \nmid u$ and $3|d$, we have $(\mathcal{O}_F/3)^\times \subseteq [E_K]_3$ by Lemma 3. Therefore, we can write

$$x_i \equiv \varepsilon_i\sqrt{-\ell} \bmod 3 \tag{8}$$

for some unit $\varepsilon_i \in E_K$. Let $b = c/x_2^3 = x_1x_2^2$. Then, as $c \equiv 1 \bmod \pi_3^3$, the cyclic extension $K(b^{1/3}) = K(c^{1/3})$ over K is tame. To show that it has no NIB, we assume, to the contrary, that it has a NIB. Then, there exists an integer $a \in \mathcal{O}_K$ with $K(a^{1/3}) = K(b^{1/3})$ satisfying the conditions of Theorem 4. We have $a = b^s y^3$ for $s \in \{1, 2\}$ and some $y \in K^\times$. Similary as in the proof of Lemma 12, the ideal $\mathfrak{B}_2$ associated to $a\mathcal{O}_K$ by (1) and (2) equals the principal ideal $x_2\mathcal{O}_K$ or $x_1\mathcal{O}_K$ according to whether $s = 1$ or 2. Let $\alpha = a^{1/3}$. Then, by the condition (iv) of Theorem 4 and (8), we see that the congruence

$$\delta_0 + \delta_1\alpha + \frac{\delta_2\alpha^2}{\sqrt{-\ell}} \equiv 0 \bmod 3$$

holds for some units $\delta_0,\ \delta_1,\ \delta_2 \in E_K$. As $K(a^{1/3})/K$ is tame, we can take an integer $v \in \mathcal{O}_K$ such that $\alpha \equiv v \bmod \pi_3$ by Lemma 2. Then, $1+\alpha/v+(\alpha/v)^2 \equiv 0 \bmod 3$. Hence, it follows from the above congruence that

$$\left(\delta_0 - \frac{\delta_2 v^2}{\sqrt{-\ell}}\right) + \left(\delta_1 - \frac{\delta_2 v}{\sqrt{-\ell}}\right)\alpha \equiv 0 \bmod 3\,.$$

From this, we obtain

$$\sqrt{-\ell} \equiv \delta_2 v^2/\delta_0 \equiv \delta_2 v/\delta_1 \bmod \pi_3$$

similarly as in the proof of Lemma 11. As $Q_K = 1$ and $3|d$, we have $[E_K]_{\pi_3} = \langle -1\rangle_{\pi_3}$. Therefore, it follows that $\sqrt{-\ell} \equiv \pm\ell \equiv \pm 1 \bmod \pi_3$ from the above congruence. However, we easily see that this is impossible. $\square$

5. Proofs of Theorems 2 and 3

We use the same notation as in Section 4. In particular, $F = \mathbf{Q}(\sqrt{d})$ is a quadratic field with d a square free integer, and $K = F(\sqrt{-3})$. If F satisfies (H_3), then the exponent of Cl_F divides 2 and $2^{t-3}[E_K : E_K^*] = 1$ by Proposition 3 and Lemma 9 (I). In particular, $t \leq 3$ and hence $h_F|4$ by genus theory. Hence, we see that $h_F = 1$, 2 or $Cl_F = (2,\ 2)$ if (H_3) is satisfied.

PROOF OF THEOREM 2. Let $F = \mathbf{Q}(\sqrt{d})$ be an imaginary quadratic field. When $d \neq -3$, let ε_0 be the fundamental unit of the associated real quadratic field $F^* = \mathbf{Q}(\sqrt{-3d})$ with $\varepsilon_0 > 1$, and let ε be a fundamental unit of $K = F(\sqrt{-3})$. We let $\varepsilon = \varepsilon_0$ if $Q_K = 1$, and we may choose ε as in Lemma 4 if $Q_K = 2$.

The case $h_F = 1$. By Stark [12], there are exactly nine imaginary quadratic fields $F = \mathbf{Q}(\sqrt{d})$ with $h_F = 1$;

$$d = -1\,,\quad -2\,,\quad -3\,,\quad -7\,,\quad -11\,,\quad -19\,,\quad -43\,,\quad -67\,,\quad -163\,.$$

When $d = -3$, F satisfies $(\mathcal{O}_F/3)^\times = \langle -1,\ \zeta_3\rangle_3$, and hence it satisfies (H_3) by Proposition 1. For the other eight ones, we see from Lemma 4 (III) that $Q_K = 2$ by using the fact that 3 is ramified in F^* and h_{F^*} is odd. Further, (H_3) is satisfied if and only if $(\mathcal{O}_F/3)^\times \subseteq [E_K]_{\pi_3}$ by Corollary 2. Let $d = -2,\ -11$. Then, as $d \equiv 1 \bmod 3$, we see that $(\mathcal{O}_F/3)^\times = (\mathcal{O}_K/\pi_3)^\times = (2,\ 2)$ and $\sqrt{d} \not\equiv \pm 1 \bmod \pi_3$. Hence, it follows that $(\mathcal{O}_K/\pi_3)^\times = \langle -1,\ \sqrt{d}\rangle_{\pi_3}$. Using Lemma 4 (III), we see that

$$\varepsilon = \sqrt{-2}+\sqrt{-3} \quad \text{or} \quad \sqrt{-11}+2\sqrt{-3}$$

according to whether $d = -2$ or -11. Hence, (H_3) is satisfied for these d. Let d be the remaining six ones. Then, as $d \equiv -1 \bmod 3$, $(\mathcal{O}_F/3)^\times = (\mathcal{O}_K/\pi_3)^\times = (8)$. When $d = -1$, we see that the order of the class $\bar{\varepsilon} \in (\mathcal{O}_K/\pi_3)^\times$ equals 8, where ε is the fundamental unit of K given in Lemma 4 (I). Hence, (H_3) is satisfied for $d = -1$. For the other five ones, we have $\varepsilon_0 \equiv \pm 1 \bmod \pi_3$ as 3 is ramified in F^*. Then, it follows that $\varepsilon^4 = \varepsilon_0^2 \equiv 1 \bmod \pi_3$ by Lemma 4 (III), and hence (H_3) is not satisfied for these d.

The case $h_F = 2$. By Stark [13] and Montgomery and Weinberger [11], there are exactly 18 imaginary quadratic fields $F = \mathbf{Q}(\sqrt{d})$ with $h_F = 2$. Using Lemmas 4 and 9 (II) (and Remark 3), we see by some hand calculation that among these, there are exactly 13 ones for which all ideal classes capitulate in K;

$$d = -5\,,\quad -10\,,\quad -22\,,\quad -35\,,\quad -58\,,\quad -115\,,\quad -187\,,\quad -235$$

and

$$d = -3\ell \quad \text{with } \ell = 2\,,\quad 5\,,\quad 17\,,\quad 41\,,\quad 89\,.$$

For these 13 ones, we have $Q_K = 1$. Therefore, for the first 8 ones, (H_3) is not satisfied by Lemma 5. For the remaining 5 ones, (H_3) is not satisfied by Lemma 12 (and Remark 4).

The case $Cl_F = (2, 2)$. By Arno [1], there are exactly 54 imaginary quadratic fields $F = \mathbf{Q}(\sqrt{d})$ with $h_F = 4$. We see from genus theory that among them, there are exactly 15 ones for which $Cl_F = (2, 2)$ and $t \leq 3$. For these 15 ones, we have $3|d$, and hence (H_3) is not satisfied by Lemma 12 (and Remark 4). $\square$

PROOF OF THEOREM 3. As in Section 1, let λ (resp. μ) denote a prime number ≥ 5 with $\lambda \equiv 1 \bmod 4$ (resp. $\mu \equiv 3 \bmod 4$). Let $F = \mathbf{Q}(\sqrt{d})$ be a real quadratic field, and $\varepsilon = (t + u\sqrt{d})/2$ a fundamental unit of F. We distinguish the cases according to whether $N\varepsilon = -1$ or 1 and $Q_K = 1$ or 2. Let r $(\leq t)$ be the number of prime numbers which ramify in F. We see that $r = t - 1$ or t, and that $r = t$ if and only if 3 is ramified in F. For a prime number ν which ramify in F, let $\wp_\nu$ be the prime ideal of F over ν.

(I) The case $N\varepsilon = -1$ and $Q_K = 1$. In this case, we have $[E_K : E_K^*] = 2$. Then, by Proposition 3 and Lemma 9 (I), we have $t = 2$ and hence $r = 1,\ 2$ if (H_3) is satisfied.

First, let $r = 1$. Then, $F = \mathbf{Q}(\sqrt{2})$ or $\mathbf{Q}(\sqrt{\lambda})$. For these F, we actually have $N\varepsilon = -1$, and $Q_K = 1$ by Lemma 4 (II). As h_F is odd, it follows from Proposition 3 and Corollary 2 that F satisfies (H_3) if and only if $h_F = 1$ and $(\mathcal{O}_F/3)^\times \subseteq [E_K]_{\pi_3}$. Therefore, by Lemma 6, (H_3) is satisfied if and only if the conditions (ii) and (iii) of Theorem 3 are satisfied.

Next, let $r = 2$. Then, as $t = 2$, we have $F = \mathbf{Q}(\sqrt{3})$, $\mathbf{Q}(\sqrt{6})$ or $\mathbf{Q}(\sqrt{3\mu})$. However, for these F, we have $N\varepsilon = 1$.

(II) The case $N\varepsilon = -1$ and $Q_K = 2$. In this case, we have $[E_K : E_K^*] = 4$. Then, by Proposition 3 and Lemma 9 (I), we have $t = r = 1$ if (H_3) is satisfied. Hence, F is unramified outside 3. However, there does not exist such a real quadratic field.

(III) The case $N\varepsilon = 1$ and $Q_K = 1$. In this case, we have $[E_K : E_K^*] = 1$. Hence, $t = 3$ and $r = 2,\ 3$ if (H_3) is satisfied.

First, let $r = 2$. Then, as $r < t$, we have (A) $F = \mathbf{Q}(\sqrt{\mu})$, $\mathbf{Q}(\sqrt{2\mu})$ or $\mathbf{Q}(\sqrt{\mu_1\mu_2})$, or (B) $F = \mathbf{Q}(\sqrt{2\lambda})$ or $\mathbf{Q}(\sqrt{\lambda_1\lambda_2})$. For these F, we actually have $Q_K = 1$ by Lemma 4 (II). For F of type (A), $N\varepsilon = 1$ and h_F is odd. Hence, for F of type (A), we see that (H_3) is satisfied if and only if the conditions (ii) and (iii) of Theorem 3 are satisfied by Proposition 3, Corollary

2 and Lemma 6. Let us deal with F of type (B). For these F, the 2-rank of Cl_F is one. We see that $N\varepsilon = 1$ if and only if $\wp_2$ and $\wp_\lambda$ (resp. $\wp_{\lambda_1}$ and $\wp_{\lambda_2}$) are principal (cf. Exercise 1.2.4 in Mollin [10, page 13]). However, when these ideals are principal, the (unique) ideal class c of F of order 2 does not contain an ambiguous ideal. Hence, the class c does not capitulate in K by Lemma 7. Therefore, by Proposition 3, (H_3) is not satisfied for F of type (B).

Next, let $r = 3$. As $t = r = 3$, we have $F = \mathbf{Q}(\sqrt{6\mu})$, $\mathbf{Q}(\sqrt{6\lambda})$, $\mathbf{Q}(\sqrt{3\lambda})$ or $\mathbf{Q}(\sqrt{3\lambda\mu})$. For these F, $N\varepsilon = 1$. As the 2-rank of Cl_F is one, we must have $h_F = 2$ if (H_3) is satisfied. When $3|u$, (H_3) is not satisfied by Lemma 12 (and Remark 4). When $3 \nmid u$ (and $h_F = 2$, $Q_K = 1$), (H_3) is not satisfied by Lemma 13.

(IV) The case $N\varepsilon = 1$ and $Q_K = 2$. In this case, we have $[E_K : E_K^*] = 2$. Hence, $t = 2$ and $r = 1,\ 2$ if (H_3) is satisfied. The case $r = 1$ can not occur as $N\varepsilon = 1$. Hence, we obtain $t = r = 2$, and hence $F = \mathbf{Q}(\sqrt{3})$, $\mathbf{Q}(\sqrt{6})$ or $\mathbf{Q}(\sqrt{3\mu})$. For these F, $N\varepsilon = 1$. As h_F is odd, the prime ideal $\wp_3$ is principal. Hence, $Q_K = 2$ by Lemma 4 (III). By Proposition 1 and Lemma 3, this type of F satisfies (H_3) if $h_F = 1$ and $3 \nmid u$. If $h_F > 1$, it does not satisfy (H_3) by Proposition 3. If $3|u$, it does not satisfy (H_3) by Lemma 12 (and Remark 4).

Now, Theorem 3 follows from the above argument. $\square$

ACKNOWLEDGEMENTS. The author thanks the referee for carefully reading the manuscript and in particular for pointing out that $d = 3$ was neglected in the statement and the proof of Theorem 3 of the old version.

References

[1] S. ARNO, The imaginary quadratic fields of class number 4, Acta Arith. **60** (1992), 321–334.
[2] E. GÓMEZ AYALA, Bases normales d'entiers dans les extensions de Kummer de degré premier, J. Théor. Nombres Bordeaux **6** (1994), 95–116.
[3] C. GREITHER, D. REPLOGLE, K. RUBIN and A. SRIVASTAV, Swan modules and Hilbert-Speiser number fields, J. Number Theory **79** (1999), 167–173.
[4] H. HASSE, *Über die Klassenzahl Abelscher Zahlkörper*, Akademie-Verlag, (1952).
[5] H. ICHIMURA, Note on the ring of integers of a Kummer extension of prime degree, I, Comment. Math. Univ. Sancti Pauli **52** (2003), 59–67; IV, Proc. Japan Acad. **77A** (2001), 92–94; V, Proc. Japan Acad. **78A** (2002), 76–79.
[6] H. ICHIMURA, On the ring of integers of a tame Kummer extension over a number field, J. Pure Applied Algebra **187** (2004), 169–182.
[7] F. KAWAMOTO, On normal integral basis, Tokyo J. Math. **7** (1985), 221–231.
[8] F. KAWAMOTO, Remark on "On normal integral basis", Tokyo J. Math. **8** (1985), 275.
[9] T. KUBOTA, Über den bizyklischen biquadratischen Zahlkörper, Nagoya Math. J. **10** (1956), 65–85.
[10] R. A. MOLLIN, *Quadratics*, CRC Press (1996).
[11] H. L. MONTGOMERY and P. T. WEINBERGER, Notes on small class numbers, Acta Arith. **24** (1973/74), 529–542.
[12] H. M. STARK, A complete determination of complex quadratic fields of class number one, Michigan J. Math. **14** (1967), 1–27.
[13] H. M. STARK, On complex quadratic fields of class number two, Math. Comp. **29** (1975), 289–302.
[14] L. C. WASHINGTON, *Introduction to Cyclotomic Fields (2nd edition)*, Springer (1996).

Present Address:
DEPARTMENT OF MATHEMATICS, YOKOHAMA CITY UNIVERSITY,
22–2, SETO, KANAZAWA-KU, YOKOHAMA 236–0027, JAPAN.
e-mail: ichimura@yokohama-cu.ac.jp