ACTA ARITHMETICA
114.1 (2004)

Normal integral bases and ray class groups

by

Humio Ichimura (Yokohama)

1. Introduction. A finite Galois extension N/F over a number field F with group G has a *normal integral basis* (NIB for short) when $\mathcal{O}_N$ is cyclic over the group ring $\mathcal{O}_F[G]$. Here, $\mathcal{O}_F$ denotes the ring of integers of a number field F. For a prime number p, we say that a number field F has *property* (A_p) when any tame cyclic extension N/F of degree p has a NIB. It is well known by Hilbert and Speiser that the rationals $\mathbb{Q}$ satisfy (A_p) for all primes p. On the other hand, Greither *et al.* [6] proved that any number field F with $F \neq \mathbb{Q}$ does not satisfy (A_p) for some p. For an integer $a \in \mathcal{O}_F$, let $\mathrm{Cl}_F(a)$ be the ray ideal class group of F defined modulo the principal ideal $a\mathcal{O}_F$. Using [6, Corollary 7], we showed in [8, V] that if $\zeta_p \in F^\times$, then F satisfies (A_p) if and only if the ray class group $\mathrm{Cl}_F(p)$ is trivial. Here, ζ_p is a primitive pth root of unity.

Let $p \geq 3$ be a prime number, F a number field, $K = F(\zeta_p)$, and $\Delta_F = \mathrm{Gal}(K/F)$. In this paper, we study property (A_p) when $\zeta_p \notin F^\times$ but $[K : F] = 2$ in connection with the ray class groups $\mathrm{Cl}_K(\pi)$ and $\mathrm{Cl}_K(p)$. Here, $\pi = \pi_p = \zeta_p - 1$. For a set X on which Δ_F acts, X^{Δ_F} denotes the invariant part. First, we prove the following:

Theorem 1. *Let $p \geq 3$ be a prime number, F a number field such that $\zeta_p \notin F^\times$, and $K = F(\zeta_p)$. Assume that $[K : F] = 2$. If F satisfies (A_p), then the ray class groups $\mathrm{Cl}_K(\pi)$ and $\mathrm{Cl}_K(p)^{\Delta_F}$ are trivial.*

We say that a number field F has *property* (B_p) when for any $a \in F^\times$, the cyclic extension $K(a^{1/p})/K$ has a NIB if it is tame, where $K = F(\zeta_p)$. A theorem of Kawamoto [12, 13] asserts that $\mathbb{Q}$ satisfies (B_p) for all primes p. Analogously to the result of Greither *et al.*, it is known by [8, IV] that any number field $F \neq \mathbb{Q}$ does not satisfy (B_p) for some p. In [11], we studied this property in some more detail. Using Theorem 1, we prove the following "duality" between properties (A_p) and (B_p).

2000 *Mathematics Subject Classification*: Primary 11R33.

THEOREM 2. *Under the setting and assumptions of Theorem* 1, *assume further that K/F is ramified at least for one prime divisor* (*including the infinite one*). *Then F satisfies* (A_p) *only when it satisfies* (B_p).

When $p = 3$, we can prove the following assertion stronger than Theorem 1.

THEOREM 3. *Let $p = 3$, F be a number field with $\zeta_3 \notin F^\times$, and $K = F(\zeta_3)$. Then F satisfies* (A_3) *if and only if the ray class groups $\mathrm{Cl}_K(\pi_3)$ and $\mathrm{Cl}_K(3)^{\Delta_F}$ are trivial.*

To prove this, we need the following descent property on NIB.

THEOREM 4. *Let $p = 3$, and F, K be as in Theorem* 3. *Then a tame cyclic cubic extension N/F has a NIB if and only if NK/K has a NIB.*

When $p = 3$ is unramified at F, this assertion is already known, by a result of Greither [5, Theorem 2.2].

The following is a consequence of Theorem 3.

PROPOSITION. *Let $p = 3$ and $F = \mathbb{Q}(\sqrt{d})$ be a quadratic field with d a square free integer. Then F satisfies* (A_3) *if and only if*

$$d = -1, -2, -3, -11, 2, 3, 5, 6, 17, 33, 41, 89.$$

REMARK 1. Let $p = 2$ and K be a number field. It is shown in [8, V] that the following three conditions are equivalent:

(i) any tame abelian extension over K of exponent 2 has a NIB,
(ii) any tame $(2, 2)$-extension over K has a NIB,
(iii) the ray class group $\mathrm{Cl}_K(4)$ of K defined modulo 4 is trivial.

REMARK 2. Let h_p (resp. h_p^+) be the class number of the p-cyclotomic field $\mathbb{Q}(\zeta_p)$ (resp. $\mathbb{Q}(\cos(2\pi/p))$), and let $h_p^- = h_p/h_p^+$. It is well known by Kummer that if $p \nmid h_p^-$, then $p \nmid h_p^+$ (cf. Washington [15, Theorems 5.34, 10.9]). Under the setting of Theorem 1, let X be the subgroup of $K^\times/(K^\times)^p$ consisting of classes $[x]$ with $x \in K^\times$ such that the cyclic extension $K(x^{1/p})/K$ is tame. Namely,

$$X = \{[x] \in K^\times/(K^\times)^p \mid (x, p) = 1,\ x \equiv u^p \bmod \pi^p \text{ for some } u \in \mathcal{O}_K\}.$$

By the action of Δ_F, we can decompose X as $X = X^+ \oplus X^-$, where $X^+ = X^{\Delta_F}$. Property (A_p) (resp. (B_p)) is a property on X^- (resp. X^+). Hence, Theorem 2 may be regarded as a Galois module analogue of the above classical duality.

REMARK 3. In [11, Theorem 2], we proved that an imaginary quadratic field $F = \mathbb{Q}(\sqrt{d})$ with d a square free negative integer satisfies (B_3) if and only if $d = -1$, -2, -3, or -11. Hence, by the Proposition, (A_3) and (B_3) are equivalent for imaginary quadratic fields. However, in general, (A_p) is stronger than (B_p). Actually, we see from [11, Theorem 3] and the Proposition that there are many real quadratic fields satisfying (B_3) but not (A_3).

REMARK 4. On the descent property on NIB, the following general fact is known for the unramified case. Let $p \geq 3$ be a prime number, F a number field with $\zeta_p \notin F^\times$, and $K = F(\zeta_p)$. Then an unramified cyclic extension N/F of degree p has a NIB if and only if NK/K has a NIB. This was first shown by Brinkhuis [1] when $p = 3$ and F is an imaginary quadratic field, and then by the author [9] for the general case.

This paper is organized as follows. In Section 2, we recall a theorem of Gómez Ayala on NIB, and give some of its versions. In Section 3, we show several lemmas related to the theorem. In Section 4, we prove Theorems 1 and 2. In Section 5, we deal with the case $p = 3$, and prove Theorems 3, 4 and the Proposition.

2. A theorem of Gómez Ayala. In this section, we recall a theorem of Gómez Ayala on NIB and give some of its versions. Let p be a prime number, K a number field with $\zeta_p \in K^\times$, L/K a cyclic extension of degree p, and $G = \mathrm{Gal}(L/K)$. Let g be a fixed generator of G and ζ_p a fixed primitive pth root of unity. For $0 \leq i \leq p-1$, let $\mathcal{O}_L^{(i)}$ be the additive group of integers $x \in \mathcal{O}_L$ such that $x^g = \zeta_p^i x$. For an integer $\omega \in \mathcal{O}_L$, the resolvent ω_i is defined by

$$\omega_i = \sum_{r=0}^{p-1} \zeta_p^{-ir} \omega^{g^r} \qquad (0 \leq i \leq p-1).$$

As is easily seen, we have $\omega_i \in \mathcal{O}_L^{(i)}$. The following lemma is easily shown and well known to specialists. Let $E_K = \mathcal{O}_K^\times$ be the group of units of K.

LEMMA 1. *Under the above setting, the following assertions hold. If L/K has a NIB, then $\mathcal{O}_L^{(i)}$ is cyclic over $\mathcal{O}_K$ for each i. More precisely, if an integer ω of L generates $\mathcal{O}_L$ over $\mathcal{O}_K[G]$, then the resolvent ω_i generates $\mathcal{O}_L^{(i)}$ over $\mathcal{O}_K$ and*

$$\omega_0 \in E_K \quad \textit{and} \quad \sum_{i=0}^{p-1} \omega_i \equiv 0 \bmod p.$$

In [4, Theorem 2.1], Gómez Ayala gave the following necessary and sufficient condition for a tame Kummer extension of prime degree to have a NIB in terms of a Kummer generator. Let $\mathfrak{A}$ be a pth power free integral ideal of a number field K. Namely, $\wp^p \nmid \mathfrak{A}$ for any prime ideal $\wp$ 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

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

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

THEOREM 5 (Gómez Ayala). *Let p be a prime number and K a number field with $\zeta_p \in K^\times$. Let L/K be a tame cyclic extension of degree p with group G. Then L/K has a NIB if and only if there exists an integer $a \in \mathcal{O}_L$ with $L = K(a^{1/p})$ satisfying the following three conditions*:

(i) *the integral ideal $a\mathcal{O}_K$ is pth power free*,

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

(iii) *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, $\omega = A/p$ generates $\mathcal{O}_L$ over $\mathcal{O}_K[G]$.

The following is a consequence of this theorem.

LEMMA 2. *Let p, K, L/K, G be as in Theorem* 5. *Then L/K has a NIB if and only if the following conditions are satisfied*:

(i) *$\mathcal{O}_L^{(i)}$ is cyclic over $\mathcal{O}_K$ for each i with $0 \le i \le p-1$*,

(ii) *there exists a generator α_i of $\mathcal{O}_L^{(i)}$ over $\mathcal{O}_K$ such that the principal ideal $\alpha_i^p\mathcal{O}_K$ of K is pth power free and*

$$A = \sum_{i=0}^{p-1} \alpha_i \equiv 0 \bmod p.$$

Further, when this is the case, $\omega = A/p$ generates $\mathcal{O}_L$ over $\mathcal{O}_K[G]$.

Proof. Assume that L/K has a NIB. Under the notation of Theorem 5, let g be a generator of G with $\alpha^g = \zeta_p\alpha$. By Lemma 1, $\mathcal{O}_L^{(i)}$ is cyclic over $\mathcal{O}_K$. Further, we see from (1) and (2) that $\alpha^i/x_i \in \mathcal{O}_L^{(i)}$ and $(\alpha^i/x_i^p)\mathcal{O}_K$ is pth power free. Therefore, $\alpha_i = \alpha^i/x_i$ generates $\mathcal{O}_L^{(i)}$ over $\mathcal{O}_K$. Hence, conditions (i) and (ii) of Lemma 2 are satisfied by Theorem 5. Conversely, assume that these two conditions are satisfied. Let $\alpha = \alpha_1$ and $a = \alpha^p$ ($\in \mathcal{O}_K$), and choose $g \in G$ so that $\alpha^g = \zeta_p\alpha$. Clearly, $L = K(a^{1/p})$, and condition (i) in Theorem 5 is satisfied. Let $\mathfrak{B}_j$ be the ideals associated to the pth power free integral ideal $a\mathcal{O}_K$. We have $\alpha_j = \alpha^j/y_j$ for some $y_j \in \mathcal{O}_K$ since $\alpha^j \in \mathcal{O}_L^{(j)}$ and α_j generates $\mathcal{O}_L^{(j)}$ over $\mathcal{O}_K$. However, as $\alpha_j^p\mathcal{O}_K$ is pth power free, we see that $y_j\mathcal{O}_K = \mathfrak{B}_j$ by (2). Therefore, all conditions in Theorem 5 are satisfied, and hence L/K has a NIB. ∎

The following is a version of this lemma.

LEMMA 3. *Let $p \geq 3$ be a prime number, F a number field with $\zeta_p \notin F^\times$, and $K = F(\zeta_p)$. Assume that $[K : F] = 2$. Let N/F be a tame cyclic extension of degree p with group G, and $L = NK$. Then N/F has a NIB if and only if the following two conditions are satisfied*:

(i) *$\mathcal{O}_L^{(i)}$ is cyclic over $\mathcal{O}_K$ for each i with $0 \leq i \leq (p-1)/2$,*

(ii) *for each $0 \leq i \leq (p-1)/2$, there exists a generator α_i of $\mathcal{O}_L^{(i)}$ over $\mathcal{O}_K$ such that the principal ideal $\alpha_i^p\mathcal{O}_K$ of K is pth power free and*

$$\alpha_0 \in E_F \quad \textit{and} \quad A = \alpha_0 + \sum_{i=1}^{(p-1)/2} (\alpha_i + \alpha_i') \equiv 0 \bmod p.$$

Here and in the proof of this lemma, for an element x (resp. a subset X) of L, x' (resp. X') denotes its conjugate over N.

Proof. Since $L = NK$ and $\zeta_p' = \zeta_p^{-1}$, we easily see that

$$(\mathcal{O}_L^{(i)})' = \mathcal{O}_L^{(p-i)}, \quad \omega_i' = \omega_{p-i} \quad (1 \leq i \leq (p-1)/2) \tag{3}$$

for any integer $\omega \in \mathcal{O}_N$. Assume that $\mathcal{O}_N = \mathcal{O}_F[G]\omega$ for some $\omega \in \mathcal{O}_N$. Then we see that $\mathcal{O}_L = \mathcal{O}_K[G]\omega$ by a classical result on rings of integers (cf. Fröhlich and Taylor [3, III, (2.13)]), and that

$$\omega_0 = \mathrm{Tr}_{L/K}\,\omega \in E_K \cap F = E_F$$

by Lemma 1. Here, $\mathrm{Tr}_{L/K}$ denotes the trace map. From the above and Lemmas 1, 2, we see that conditions (i) and (ii) of Lemma 3 are satisfied with $\alpha_i = \omega_i$. Conversely, assume that conditions (i) and (ii) are satisfied, and let $\omega = A/p$. Then $\omega \in \mathcal{O}_N$ by (ii). By (3) and the conditions of Lemma 3, we see from Lemma 2 that $\mathcal{O}_L = \mathcal{O}_K[G]\omega$. As $\omega \in \mathcal{O}_N$, this implies that $\mathcal{O}_N = \mathcal{O}_F[G]\omega$. ∎

REMARK 5. In [10], we gave a generalization of the theorem of Gómez Ayala (Theorem 5) and some of its applications. A function field analogue of the theorem is already given in Chapman [2].

3. Lemmas. In this section, we prepare some lemmas related to Theorem 5 which are necessary to prove our theorems. In what follows, we let $p \geq 3$ be a *fixed* odd prime number, ζ_p a *fixed* primitive pth root of unity, and $\pi = \pi_p = \zeta_p - 1$.

LEMMA 4. *Let s, t be integers with $1 \leq s < t \leq p-1$. Let K be a number field, and $\mathfrak{A}_1$, $\mathfrak{A}_2$ square free integral ideals of K relatively prime to each other. If the associated ideals $\mathfrak{B}_j$ of $\mathfrak{A} = \mathfrak{A}_1^s\mathfrak{A}_2^t$ defined by* (2) *are principal, then $\mathfrak{A}_1$ and $\mathfrak{A}_2$ are principal.*

Proof. As $s < t$, we see that $[si/p] < [ti/p]$ for some i with $1 \leq i \leq p-1$. Let k be the smallest such integer. Then

$$[s(k-1)/p] = [t(k-1)/p] = [sk/p] = a, \qquad [tk/p] = a+1$$

for some integer a. This is because $[s(i+1)/p] = [si/p]$ or $[si/p]+1$. Therefore, from the assumption, the ideals $\mathfrak{B}_{k-1} = \mathfrak{A}_1^a\mathfrak{A}_2^a$ and $\mathfrak{B}_k = \mathfrak{A}_1^a\mathfrak{A}_2^{a+1}$ are principal. Hence, $\mathfrak{A}_2$ is principal. Let r be the smallest integer with $[sr/p] \geq 1$. Then $[sr/p] = 1$ and $\mathfrak{B}_r = \mathfrak{A}_1\mathfrak{A}_2^{[tr/p]}$. Hence, $\mathfrak{A}_1$ is also principal. ■

LEMMA 5. *Let K be a number field with $\zeta_p \in K^\times$, and let λ_1 and λ_2 be integers of K such that the principal ideals $\lambda_1\mathcal{O}_K$ and $\lambda_2\mathcal{O}_K$ are square free and relatively prime to each other and to p. Let $a = \lambda_1\lambda_2^{p-1}$, and $L = K(a^{1/p})$. Assume that L/K has a NIB. Then $a \equiv \eta^p \bmod \pi^p$ and $\lambda_i \equiv \eta_i \bmod \pi$ for some units $\eta, \eta_i \in E_K$ with $i = 1, 2$. Further, when $p = 3$, we have $\lambda_i \equiv \eta_i \bmod 3$ for some $\eta_i \in E_K$.*

Proof. When $a \in (K^\times)^p$, we easily see that a, λ_1 and λ_2 are units of K from the conditions on λ_i, and hence the assertion is obvious. So, we may as well assume that $[L : K] = p$. Let $\alpha = a^{1/p}$, and choose a generator g of $\mathrm{Gal}(L/K)$ so that $\alpha^g = \zeta_p\alpha$. For $1 \leq i \leq p-1$, let $\alpha_i = \alpha^i/\lambda_2^{i-1}$. Then $\alpha_i \in \mathcal{O}_L^{(i)}$, and the ideal $\alpha_i^p\mathcal{O}_K = \lambda_1^i\lambda_2^{p-i}\mathcal{O}_K$ of K is pth power free. Hence, by the assumption and Lemma 1, we have $\mathcal{O}_L^{(i)} = \mathcal{O}_K\alpha_i$. Therefore, by Lemma 2, the congruence

$$\delta_0 + \delta_1\alpha + \delta_2\frac{\alpha^2}{\lambda_2} + \ldots + \delta_{p-1}\frac{\alpha^{p-1}}{\lambda_2^{p-2}} \equiv 0 \bmod p$$

holds for some units $\delta_i \in E_K$. It follows from this that

$$\sum_{i=1}^{p-1}\delta_{p-i}\lambda_2^{i-1}\alpha^{p-i} + \delta_0\lambda_2^{p-2} \equiv 0 \bmod p, \tag{4}$$

and that

$$\frac{\delta_0}{\alpha^2} + \frac{\delta_1}{\alpha} + \frac{\delta_2}{\lambda_2} + \sum_{i=1}^{p-3}\frac{\delta_{i+2}}{\lambda_2^{i+1}}\alpha^i \equiv 0 \bmod p. \tag{5}$$

For a congruence $(*)$ such as (4) and (5), let $(*)^g$ be the congruence obtained by letting g act on $(*)$. Let

$$c_j = 1 + \zeta_p + \zeta_p^2 + \ldots + \zeta_p^j = \frac{\zeta_p^{j+1}-1}{\zeta_p - 1} \qquad (0 \leq j \leq p-2)$$

be a cyclotomic unit. Dividing (4) − $(4)^g$ by $\pi\alpha$, we obtain

$$\sum_{i=1}^{p-2}\delta_{p-i}c_{p-1-i}\lambda_2^{i-1}\alpha^{p-1-i}+\delta_1\lambda_2^{p-2}\equiv 0 \bmod \pi^{p-2}. \tag{6}$$

Again, dividing (6) − $(6)^g$ by $\pi\alpha$, we obtain

$$\sum_{i=1}^{p-3}\delta_{p-i}c_{p-1-i}c_{p-2-i}\lambda_2^{i-1}\alpha^{p-2-i}+\delta_2 c_1\lambda_2^{p-3}\equiv 0 \bmod \pi^{p-3}.$$

Repeating this process, we finally obtain

$$\delta_{p-1}\Big(\prod_{i=1}^{p-2}c_i\Big)\alpha+\delta_{p-2}\Big(\prod_{i=0}^{p-3}c_i\Big)\lambda_2\equiv 0 \pmod{\pi},$$

and hence

$$\alpha\equiv\frac{\delta_{p-2}}{\delta_{p-1}}\,\lambda_2 \bmod \pi. \tag{7}$$

Starting from the congruence (5), we similarly obtain

$$\alpha\equiv\delta_0/\delta_1 \bmod \pi.$$

From the last two congruences, we obtain the assertion for the general case.

Finally, let us deal with the case $p=3$. By (4), we have

$$\delta_2\alpha^2+\delta_1\lambda_2\alpha+\delta_0\lambda_2\equiv 0 \bmod 3.$$

For an element $x\in L^\times$ with $x\equiv 1 \bmod \pi_3$, we have $x^2+x+1\equiv 0 \bmod 3$. Hence, it follows from (7) that

$$\delta_2\alpha^2+\delta_1\lambda_2\alpha+\delta_1^2\delta_2^{-1}\lambda_2^2\equiv 0 \bmod 3.$$

From these two congruences, it follows that $\lambda_2\equiv\delta_0\delta_1^{-2}\delta_2 \bmod 3$. The assertion for the case $p=3$ follows from this. ∎

For an ideal $\mathfrak{A}$ of K with $(\mathfrak{A},p)=1$, let $[\mathfrak{A}]_\pi$ be the ideal class in $\mathrm{Cl}_K(\pi)$ represented by $\mathfrak{A}$.

LEMMA 6. *Let K be a number field with $\zeta_p\in K^\times$, $a\in\mathcal{O}_K$ an integer such that $a\equiv 1 \bmod \pi^p$, and $L=K(a^{1/p})$. Assume that* (i) *L/K has a NIB, and* (ii) *$a\mathcal{O}_K=\mathfrak{A}_1^r\mathfrak{A}_2^{p-r}\mathfrak{A}_3^p$ for some $1\le r\le p-1$ and some integral ideals $\mathfrak{A}_i$ of K such that $\mathfrak{A}_1$ and $\mathfrak{A}_2$ are square free and relatively prime to each other. Then the classes $[\mathfrak{A}_i]_\pi\in\mathrm{Cl}_K(\pi)$ are trivial for $i=1,2,3$.*

Proof. As L/K has a NIB, we see from Theorem 5 that there exists an integer $b\in\mathcal{O}_K$ with $L=K(b^{1/p})$ such that $b\mathcal{O}_K$ is pth power free and the ideals associated to $b\mathcal{O}_K$ by (1) and (2) are principal. By assumption (ii), we see that $b\mathcal{O}_K=\mathfrak{A}_1^s\mathfrak{A}_2^{p-s}$ for some $1\le s\le p-1$. It follows from Lemma 4 that $\mathfrak{A}_i=\lambda_i\mathcal{O}_K$ for some $\lambda_i\in\mathcal{O}_K$ with $i=1,2$. Then

$$L=K((\varepsilon_1\lambda_1\lambda_2^{p-1})^{1/p}) \tag{8}$$

for some unit $\varepsilon_1 \in E_K$. As L/K has a NIB, we see from Lemma 5 that $\lambda_i \equiv \eta_i \bmod \pi$. Hence, the classes $[\mathfrak{A}_1]_\pi$ and $[\mathfrak{A}_2]_\pi$ are trivial. It also follows from Lemma 5 that $\varepsilon_1\lambda_1\lambda_2^{p-1} \equiv \eta^p \bmod \pi^p$ for some $\eta \in E_K$. From this and $\lambda_2 \equiv \eta_2 \bmod \pi$, it follows that

$$\varepsilon_1^r\lambda_1^r\lambda_2^{p-r} \equiv \delta^p \bmod \pi^p \tag{9}$$

for some $\delta \in E_K$. From assumption (ii) and (8), we see that $a = \varepsilon_1^r\lambda_1^r\lambda_2^{p-r}x^p$ for some $x \in \mathcal{O}_K$ and that $\mathfrak{A}_3 = x\mathcal{O}_K$. Then, by (9) and $a \equiv 1 \bmod \pi^p$, it follows that x is congruent to a unit modulo π. Therefore, $[\mathfrak{A}_3]_\pi = 1$. ∎

For a number field K and an integer $a \in \mathcal{O}_K$, we write $\mathcal{O}_K/a = \mathcal{O}_K/a\mathcal{O}_K$ for brevity, and let $[E_K]_a$ be the subgroup of the multiplicative group $(\mathcal{O}_K/a)^\times$ generated by the classes containing units of K. For an element $x \in K^\times$ with $(x, a) = 1$, $[x]_a$ denotes the class represented by x. When F is a subfield of K and $a \in \mathcal{O}_F$, we naturally regard $(\mathcal{O}_F/a)^\times$ as a subgroup of $(\mathcal{O}_K/a)^\times$.

LEMMA 7. (I) *For a number field K with $\zeta_p \in K^\times$, the exponent of $\mathrm{Cl}_K(p)$ divides p if $\mathrm{Cl}_K(\pi) = \{0\}$.*

(II) *Let F be a number field with $\zeta_p \notin F^\times$, and $K = F(\zeta_p)$. Assume that $\mathrm{Cl}_K(\pi) = \{0\}$. Then $\mathrm{Cl}_K(p)^{\Delta_F} = \{0\}$ if and only if $(\mathcal{O}_F/p)^\times \subseteq [E_K]_p$.*

Proof. We put

$$A = (1 + \pi\mathcal{O}_K)/(1 + p\mathcal{O}_K)\ (\subseteq (\mathcal{O}_K/p)^\times) \quad \text{and} \quad B = A[E_K]_p/[E_K]_p.$$

As $\mathrm{Cl}_K(\pi) = \{0\}$, we see that $\mathrm{Cl}_K(p) = B$ from the exact sequence

$$\{0\} \to B \to \mathrm{Cl}_K(p) \to \mathrm{Cl}_K(\pi) \to \{0\}.$$

Then the first assertion is obvious as A is of exponent p. Let us show the second one. The "only if" part holds as $(\mathcal{O}_K/p)^\times/[E_K]_p$ is a subgroup of $\mathrm{Cl}_K(p)$. We show the "if" part. We have $\mathrm{Cl}_K(p) = B$ as $\mathrm{Cl}_K(\pi) = \{0\}$. Let $d = [K : F]$, and let $\mathcal{C} = [x]_p$ be a class in B^{Δ_F} with $x \in \mathcal{O}_K$. Then, since $\mathcal{C}^d = [N_{K/F}x]_p$, we obtain $\mathcal{C}^d = 1$ by $(\mathcal{O}_F/p)^\times \subseteq [E_K]_p$. Here, $N_{K/F}$ denotes the norm map. Therefore, $\mathcal{C} = 1$ as d divides $p - 1$ and B is a p-abelian group. ∎

Let F be a number field with $\zeta_p \notin F^\times$, and $K = F(\zeta_p)$. When $[K : F] = 2$, for an element x (resp. an ideal $\mathfrak{A}$) of K, let x' (resp. $\mathfrak{A}'$) denotes the conjugate over F.

LEMMA 8. *Let F be a number field with $\zeta_p \notin F^\times$, and $K = F(\zeta_p)$. Assume that $[K : F] = 2$. Assume further that $\mathrm{Cl}_K(\pi)$ and $\mathrm{Cl}_K(p)^{\Delta_F}$ are trivial. Let a be an integer of K relatively prime to p such that $a\mathcal{O}_K$ is square free and $(a, a') = 1$, and let $b = a(a')^{p-1}$. Then the cyclic extension $L = K(b^{1/p})/K$ has a NIB if it is tame.*

Proof. Let $\mathfrak{B}_j$ be the ideals of K associated to $b\mathcal{O}_K$ by (1) and (2). Then

$$\mathfrak{B}_0 = \mathfrak{B}_1 = \mathcal{O}_K, \quad \mathfrak{B}_j = (a')^{j-1}\mathcal{O}_K \quad \text{for } 2 \le j \le p-1.$$

As L/K is tame, $b \equiv u^p \bmod \pi^p$ for some $u \in \mathcal{O}_K$. We see that $u \equiv \varepsilon \bmod \pi$ for some unit $\varepsilon \in E_K$ because $\mathrm{Cl}_K(\pi) = \{0\}$. Hence, $b = a(a')^{p-1} \equiv \varepsilon^p \bmod \pi^p$. On the other hand, aa' $(\in \mathcal{O}_F)$ is congruent to a unit modulo p since $\mathrm{Cl}_K(p)^{\Delta_F} = \{0\}$. Hence, so is $(a')^{p-2} = b/(aa')$. This implies that $a' \equiv \delta \bmod p$ for some unit $\delta \in E_K$ because $\mathrm{Cl}_K(p)$ and its subgroup $(\mathcal{O}_K/p)^\times/[E_K]_p$ are p-abelian groups (by Lemma 7). Now, let $\beta = b^{1/p}$ $(\equiv \varepsilon \bmod \pi)$. Then

$$1 + \frac{\beta}{\varepsilon} + \sum_{j=2}^{p-1} \delta^{j-1}\, \frac{\beta^j}{(a')^{j-1}\varepsilon^j} \equiv \sum_{j=0}^{p-1} (\beta/\varepsilon)^j \equiv 0 \bmod p.$$

Therefore, L/K has a NIB by Theorem 5. ∎

The following is one more consequence of Theorem 5, for which see [11, Proposition 1]. For a number field F, let h_F be the class number of F (in the usual sense).

LEMMA 9. *Let p be a prime number, F a number field, and $K = F(\zeta_p)$. Assume that $h_F = 1$ and $(\mathcal{O}_F/p)^\times \subseteq [E_K]_p$. Then F satisfies* (B_p).

4. Proofs of Theorems 1 and 2. First, we derive Theorem 2 from Theorem 1.

Proof of Theorem 2. Assume that F satisfies (A_p). Then $\mathrm{Cl}_K(\pi)$ and $\mathrm{Cl}_K(p)^{\Delta_F}$ are trivial by Theorem 1. Since $[K:F] = 2$ and $\mathrm{Cl}_K(p)^{\Delta_F} = \{0\}$, we see that $h_F = 1$, or $h_F = 2$ and K/F is the Hilbert class field of F. Hence, by the second assumption of Theorem 2, we must have $h_F = 1$. On the other hand, $(\mathcal{O}_F/p)^\times \subseteq [E_K]_p$ by Lemma 7. Hence, F satisfies (B_p) by Lemma 9. ∎

To prove Theorem 1, the following theorem of Greither *et al.* [6, Corollary] is crucial.

THEOREM 6 (Greither *et al.*). *If a number field F has property* (A_p), *then the exponent of the quotient $(\mathcal{O}_F/p)^\times/[E_F]_p$ divides $(p-1)^2/2$.*

Proof of Theorem 1. This is done in several steps.

LEMMA 10. *Under the setting of Theorem* 1, *assume that $[K:F] = 2$ and that F satisfies* (A_p). *Then $\mathrm{Cl}_K(\pi^p)$ is a p-abelian group. Hence*, $\mathrm{Cl}_K(p)$, $\mathrm{Cl}_K(\pi)$ *and* Cl_K *are p-abelian groups.*

Proof. Let $\mathcal{C}$ be an ideal class in $\mathrm{Cl}_K(\pi^p)$ whose order n is relatively prime to p. It suffices to show that $\mathcal{C} = 1$. Let $\mathfrak{P} \in \mathcal{C}$ be a prime ideal of K with $(\mathfrak{P}, \mathfrak{P}') = 1$. Then $\mathfrak{P}^n = a\mathcal{O}_K$ for some integer $a \in \mathcal{O}_K$ with $a \equiv 1 \bmod \pi^p$. Let $b = a(a')^{p-1}$ and $L = K(b^{1/p})$. Since

$$b\mathcal{O}_K = \mathfrak{P}^n(\mathfrak{P}')^{n(p-1)} \quad \text{and} \quad p \nmid n, \tag{10}$$

the extension L/K is of degree p. It is tame as $b \equiv 1 \bmod \pi^p$. As $bb' \in (K^\times)^p$, there uniquely exists a tame cyclic extension N/F of degree p with $L = NK$. As F satisfies (A_p), N/F and hence L/K have a NIB. Now, it follows from (10) and Lemma 6 that $\mathfrak{P} = \lambda\mathcal{O}_K$ for some $\lambda \in \mathcal{O}_K$ and that $\lambda \equiv \delta \bmod \pi$ for some $\delta \in E_K$. As $\lambda^p \equiv \delta^p \bmod \pi^p$, we see that $\mathcal{C}^p$ is trivial in $\mathrm{Cl}_K(\pi^p)$. This implies that $\mathcal{C} = 1$. ∎

LEMMA 11. *Under the setting and assumptions of Lemma* 10, *we have* $\mathrm{Cl}_K(\pi) = \{0\}$.

Proof. We have a natural surjection $\varphi : \mathrm{Cl}_K(\pi^p) \to \mathrm{Cl}_K(\pi)$ compatible with the action of Δ_F. Let $\mathcal{C}$ be a nontrivial class in $\mathrm{Cl}_K(\pi^p)$. By Lemma 10, the order of $\mathcal{C}$ equals p^e for some $e \geq 1$. It suffices to show that $\varphi(\mathcal{C}) = 1$.

Let us first show that $\varphi(\mathcal{C}\mathcal{C}') = 1$. Let $\mathfrak{P}, \mathfrak{Q} \in \mathcal{C}$ be prime ideals of K with $(\mathfrak{P}, \mathfrak{Q}) = (\mathfrak{P}, \mathfrak{Q}') = 1$. Then $\mathfrak{P}\mathfrak{Q}^{p^e-1} = a\mathcal{O}_K$ for some integer a with $a \equiv 1 \bmod \pi^p$. Let $b = a(a')^{p-1}$ and $L = K(b^{1/p})$. We have

$$b\mathcal{O}_K = (\mathfrak{P}\mathfrak{Q}')(\mathfrak{P}'\mathfrak{Q})^{p-1}\mathfrak{A}^p \tag{11}$$

with

$$\mathfrak{A} = \mathfrak{Q}^{p^{e-1}-1}(\mathfrak{Q}')^{p^e-p^{e-1}-1}. \tag{12}$$

In particular, the cyclic extension L/K is of degree p. As $b \equiv 1 \bmod \pi^p$, it is tame. As $bb' \in (K^\times)^p$, there exists a tame cyclic extension N/F of degree p with $L = NK$. As F satisfies (A_p), L/K has a NIB. Then it follows from (11) and Lemma 6 that $\varphi(\mathcal{C}\mathcal{C}') = [\mathfrak{P}\mathfrak{Q}']_\pi = 1$.

Let us deal with the case $e = 1$. By (12), we have $\mathfrak{A} = (\mathfrak{Q}')^{p-2}$. By (11) and Lemma 6, the class $\varphi(\mathcal{C}')^{p-2} = [\mathfrak{A}]_\pi$ is trivial in $\mathrm{Cl}_K(\pi)$. This implies that $\varphi(\mathcal{C}) = 1$ since $\mathrm{Cl}_K(\pi)$ is a p-abelian group by Lemma 10.

Finally, we deal with the case $e \geq 2$. Let $\mathfrak{R}, \mathfrak{Q}_1, \ldots, \mathfrak{Q}_{p-1} \in \mathcal{C}$ be prime ideals of K which are relatively prime to each other and to their conjugates over F. Then

$$\mathfrak{R}(\mathfrak{Q}_1 \ldots \mathfrak{Q}_{p-1})^{(p^e-1)/(p-1)} = a_1\mathcal{O}_K$$

for some $a_1 \in \mathcal{O}_K$ with $a_1 \equiv 1 \bmod \pi^p$. Let $b_1 = a_1(a_1')^{p-1}$ and $L_1 = K(b_1^{1/p})$. Then L_1/K is of degree p, and has a NIB as F satisfies (A_p). We have

$$b_1\mathcal{O}_K = (\mathfrak{R}\mathfrak{Q}_1 \ldots \mathfrak{Q}_{p-1})(\mathfrak{R}'\mathfrak{Q}_1' \ldots \mathfrak{Q}_{p-1}')^{p-1}\mathfrak{B}^p$$

with

$$\mathfrak{B} = (\mathfrak{Q}_1 \ldots \mathfrak{Q}_{p-1})^{(p^{e-1}-1)/(p-1)}(\mathfrak{Q}_1' \ldots \mathfrak{Q}_{p-1}')^{p^{e-1}-1}.$$

As L_1/K has a NIB, it follows from Lemma 6 that

$$[\mathfrak{B}]_\pi = \varphi(\mathcal{C})^{p^{e-1}-1}\varphi(\mathcal{C}')^{(p-1)(p^{e-1}-1)} = 1.$$

On the other hand, we have seen above that $\varphi(\mathcal{C}) = \varphi(\mathcal{C}')^{-1}$. Hence, $\varphi(\mathcal{C}')^{(p-2)(p^{e-1}-1)} = 1$. Therefore, $\varphi(\mathcal{C}) = 1$ as $\mathrm{Cl}_K(\pi)$ is a p-abelian group. ∎

LEMMA 12. *Under the setting and assumptions of Lemma* 10, *we have* $\mathrm{Cl}_K(p)^{\Delta_F} = \{0\}$.

Proof. By Lemma 10, $(\mathcal{O}_K/p)^\times/[E_K]_p$ is a p-abelian group. Therefore, we see from Theorem 6 that $(\mathcal{O}_F/p)^\times \subseteq [E_K]_p$. Then we obtain $\mathrm{Cl}_K(p)^{\Delta_F} = \{0\}$ from Lemmas 7(II) and 11. ∎

Now, Theorem 1 follows from Lemmas 11 and 12. ∎

5. Proofs of Theorems 3, 4 and Proposition

5.1. *Proof of Theorem 4.* In all what follows, we let $p = 3$ and $\pi = \pi_3 = \zeta_3 - 1$. We begin with the following lemma.

LEMMA 13. *Let* F, K *be as in Theorem* 4, N/F *a tame cyclic cubic extension*, *and* $L = NK$. *Then* L/K *has a NIB if and only if there exists an integer* $\lambda \in \mathcal{O}_K$ *with* $L = K((\lambda(\lambda')^2)^{1/3})$ *satisfying the following conditions*:

(i) $\lambda\mathcal{O}_K$ *is square free and* $(\lambda, \lambda') = 1$,
(ii) $\varepsilon_1^3\lambda(\lambda')^2 \equiv 1 \bmod \pi^3$ *for some unit* $\varepsilon_1 \in E_K$,
(iii) $\lambda \equiv \varepsilon_2 \bmod 3$ *for some unit* $\varepsilon_2 \in E_K$.

Proof. We can easily show the "if" part using Theorem 5 by an argument similar to the proof of Lemma 8. So, we assume that L/K has a NIB, and show the "only if" part. As L/K has a NIB, there exists an integer $a \in \mathcal{O}_K$ relatively prime to 3 with $L = K(a^{1/3})$ satisfying the conditions in Theorem 5. As $a\mathcal{O}_K$ is cube free, $a\mathcal{O}_K = \mathfrak{A}_1\mathfrak{A}_2^2$ for some square free integral ideals $\mathfrak{A}_i$ of K with $(\mathfrak{A}_1, \mathfrak{A}_2) = 1$. By Lemma 6, the ideals $\mathfrak{A}_1$ and $\mathfrak{A}_2$ are principal. As $L = NK$, we must have $aa' \in (K^\times)^3$. From this, it follows that $\mathfrak{A}_2 = \mathfrak{A}_1'$. Hence, we can write $a = \eta\lambda(\lambda')^2$. Here, η is a unit of K, and $\lambda \in \mathcal{O}_K$ is an integer such that $\lambda\mathcal{O}_K$ is square free and $(\lambda, \lambda') = 1$. From $aa' \in (K^\times)^3$, we have $\eta\eta' = \eta_1^3$ for some $\eta_1 \in E_K$. As $[K : F] = 2$, we see that $\eta_1 \in E_F$. Further, as the quotient $E_F/N_{K/F}E_K$ is of exponent 2, we have $\eta_1 = \eta_2\eta_2'$ for some $\eta_2 \in E_K$. Therefore, $\eta = \eta_2^3\delta$ for some unit $\delta \in E_K$ with $\delta\delta' = 1$. Hence, replacing a with a/η_2^3 and λ with $\delta'\lambda$, we can write $a = \lambda(\lambda')^2$. Now, the assertion follows from Lemma 5. ∎

We now turn to the proof of Theorem 4. It suffices to show the "if" part. Assume that L/K has a NIB, and choose λ, ε_1, ε_2 as in Lemma 13.

Let $b = \varepsilon_1^3\lambda(\lambda')^2$, and $\beta = b^{1/3}$ ($\equiv 1 \bmod \pi$). We have $\beta' = \varepsilon_1\varepsilon_1'\lambda\lambda'/\beta$. By Lemma 1,

$$\mathcal{O}_L^{(1)} = \mathcal{O}_K\beta, \qquad \mathcal{O}_L^{(2)} = \mathcal{O}_K\,\frac{\varepsilon_1\varepsilon_1'\lambda\lambda'}{\beta}.$$

By Lemma 3, it suffices to show that there exists a unit $\eta \in E_K$ such that

$$1 + \beta\eta + \frac{\varepsilon_1\varepsilon_1'\lambda\lambda'}{\beta}\,\eta' \equiv 0 \bmod 3.$$

This is equivalent to saying that

$$(\beta\eta)^2 + \beta\eta + \varepsilon_1\varepsilon_1'\lambda\lambda'\eta\eta' \equiv 0 \bmod 3. \tag{13}$$

As $\beta \equiv 1 \bmod \pi$, we see that $\beta' \equiv 1 \bmod \pi$ and hence

$$\varepsilon_1\varepsilon_1'\lambda\lambda' \equiv 1 \bmod \pi. \tag{14}$$

On the other hand, we have

$$b/b' \equiv \varepsilon_1^3(\varepsilon_1')^{-3}\lambda^{-1}\lambda' \equiv 1 \bmod \pi. \tag{15}$$

From (14) and (15), it follows that $\varepsilon_1^4(\varepsilon_1')^{-2}(\lambda')^2 \equiv 1 \bmod \pi$, and hence

$$\lambda^2\varepsilon_1^{-2}(\varepsilon_1')^4 - 1 = (\lambda\varepsilon_1^{-1}(\varepsilon_1')^2 - 1)(\lambda\varepsilon_1^{-1}(\varepsilon_1')^2 + 1) \equiv 0 \bmod \pi.$$

Claim. $\lambda\varepsilon_1^{-1}(\varepsilon_1')^2 \equiv 1 \bmod \pi$.

Indeed, let $\mathfrak{P}$ be a prime ideal of K over p, and $e = \mathrm{ord}_{\mathfrak{P}}\pi$. From the above congruence, we see that $\lambda\varepsilon_1^{-1}(\varepsilon_2')^2 \equiv 1$ or $-1 \bmod \mathfrak{P}^e$ because

$$(\lambda\varepsilon_1^{-1}(\varepsilon_2')^2 - 1, \lambda\varepsilon_1^{-1}(\varepsilon_2')^2 + 1) \mid 2 \quad \text{and} \quad p \neq 2.$$

Assume that $x = \lambda\varepsilon_1^{-1}(\varepsilon_1')^2 \equiv -1 \bmod \mathfrak{P}^e$. By the above, we have $x \equiv \pm 1 \bmod (\mathfrak{P}')^e$. Hence, $(x')^2 \equiv 1 \bmod \mathfrak{P}^e$. Thus, $b = x(x')^2 \equiv -1 \bmod \mathfrak{P}^e$. This contradicts $b \equiv 1 \bmod \pi$. Hence, the claim is shown.

Let $\eta = (\varepsilon_2\varepsilon_1^{-1}(\varepsilon_1')^2)^{-1}$. Then, by the Claim and Lemma 13(iii), we see that

$$\eta \equiv 1 \bmod \pi \quad \text{and} \quad \varepsilon_1\varepsilon_1'\lambda\lambda'\eta\eta' \equiv 1 \bmod 3.$$

Therefore, as $\beta \equiv 1 \bmod \pi$, congruence (13) holds. Hence, N/F has a NIB. ■

5.2. *Proof of Theorem 3.* By Theorem 1, it suffices to show the "if" part. Assume that F satisfies $\mathrm{Cl}_K(\pi) = \{0\}$ and $\mathrm{Cl}_K(3)^{\Delta_F} = \{0\}$. In particular, $h_K = 1$. Let N/F be an arbitrary tame cyclic cubic extension, and $L = NK$. By Theorem 4, it suffices to show that L/K has a NIB. As $h_K = 1$, we can write $L = K(a^{1/3})$ with

$$a = \varepsilon\prod_{i=1}^{r}(\pi_i^{e_i}(\pi_i')^{f_i})\prod_{j=1}^{s}\varrho_j^{g_j} \qquad (e_i \in \{1,2\},\ f_i, g_j \in \{0,1,2\}).$$

Here, $\varepsilon \in E_K$, and π_i (resp. ϱ_j) are integers of K relatively prime to 3 such that $\pi_i\mathcal{O}_K$ (resp. $\varrho_j\mathcal{O}_K$) are prime ideals of K of relative degree one (resp. two) over F. The integers π_i, ϱ_j are chosen so that $N_{K/F}\pi_i$ and ϱ_j are relatively prime to each other. As $L = NK$, we have $aa' \in (K^\times)^3$. Therefore, it follows that $e_i + f_i = 3$ and $g_j = 0$. It also follows that $\varepsilon = \varepsilon_1^3\delta$ for some units $\varepsilon_1, \delta \in E_K$ with $\delta\delta' = 1$. Now, letting

$$b = \delta' \prod_{e_i=1} \pi_i \prod_{e_i=2} \pi_i',$$

we have $a = \varepsilon_1^3 b(b')^2$. Here, in the first (resp. second) product, i runs over integers $1 \le i \le r$ with $e_i = 1$ (resp. $e_i = 2$). As $b\mathcal{O}_K$ is square free and $(b, b') = 1$, we see that L/K has a NIB by Lemma 8. ∎

5.3. *Proof of Proposition.* It is known and easy to show that $F = \mathbb{Q}(\sqrt{-3})$ satisfies (A_3) (cf. [4, p. 110]). Let $K = \mathbb{Q}(\sqrt{\ell}, \sqrt{-3})$ be a $(2,2)$-extension of $\mathbb{Q}$ with ℓ a square free integer, and let Q_K $(= 1, 2)$ be the unit index of K, and ε a fundamental unit of K. Let $\varepsilon_0 > 0$ be a fundamental unit of the maximal real subfield K^+ of K. We can calculate Q_K and ε using a classical result in Hasse [7, Section 26]. When $Q_K = 1$, we have $\varepsilon = \varepsilon_0$. When $Q_K = 2$, we can choose ε so that

$$\varepsilon^2 = \sqrt{-1}\cdot\varepsilon_0 \quad \text{or} \quad -\varepsilon_0 \tag{16}$$

according to whether $\sqrt{-1} \in K^\times$ or not. By Uchida [14], there are exactly 13 K's with $h_K = 1$, namely,

(a) $\ell = 2, 5, 17, 41, 89$,
(b) $\ell = -1, -2, -11$, or
(c) $\ell = -7, -19, -43, -67, -163$.

For this, see also Yamamura [16]. By Theorem 3, a quadratic field F satisfying (A_3) is contained in these K. For a finite abelian group A, we write $A = (n_1, \ldots, n_r)$ when A is isomorphic to the additive group $\mathbb{Z}/n_1 \oplus \ldots \oplus \mathbb{Z}/n_r$.

First, let us deal with quadratic fields contained in those K in (c). We see that $Q_K = 2$ and $(\mathcal{O}_K/\pi)^\times = (8)$. We have $\varepsilon_0 \equiv \pm 1 \bmod \pi$ as 3 is ramified in K^+. Hence, by (16), the order of the class $[\varepsilon]_\pi$ divides 4. Therefore, we see that $[E_K]_\pi \subsetneq (\mathcal{O}_K/\pi)^\times$ and $\mathrm{Cl}_K(\pi) \neq \{0\}$. Hence, by Theorem 3, any quadratic field $F \neq \mathbb{Q}(\sqrt{-3})$ contained in these K does not satisfy (A_3).

Next, let us deal with those K in (b). For these K, we see that $Q_K = 2$, and that by (16),

$$\varepsilon = (-1 - \sqrt{-1} + \sqrt{-3} - \sqrt{3})/2,\ \sqrt{-2} + \sqrt{-3},\ \sqrt{-11} + 2\sqrt{-3},$$

respectively. Using this, we easily see that $(\mathcal{O}_K/3)^\times = [E_K]_3$. As $h_K = 1$, this implies that $\mathrm{Cl}_K(3) = \{0\}$. Then it follows from [8, V, Proposition 2] that K satisfies (A_3). Therefore, by Theorem 4, all quadratic fields contained in these K satisfy (A_3).

Finally, let us deal with those K in (a). For these K, we have $Q_K = 1$ and $(\mathcal{O}_K/\pi)^\times = (8)$. Using $\varepsilon = \varepsilon_0 \equiv \pm 1 \pm \sqrt{\ell} \bmod 3$ and $\ell \equiv -1 \bmod 3$, we see that the order of the class $[\varepsilon]_\pi$ (resp. $[\varepsilon]_3$) equals 8. Hence, $(\mathcal{O}_K/\pi)^\times = [E_K]_\pi$. This implies that $\mathrm{Cl}_K(\pi) = \{0\}$ as $h_K = 1$. Let $F = \mathbb{Q}(\sqrt{\ell})$ be a real quadratic field contained in these K. We have $(\mathcal{O}_F/3)^\times = (8)$ and $(\mathcal{O}_K/3)^\times = (3,3,8)$. Thus $(\mathcal{O}_F/3)^\times \subseteq [E_K]_3$ since the class $[\varepsilon]_3$ is of order 8. By Lemma 7, this implies that $\mathrm{Cl}_K(3)^{\Delta_F} = \{0\}$. Hence, by Theorem 3, a real quadratic field $F = \mathbb{Q}(\sqrt{\ell})$ with ℓ in (a) satisfies (A_3). Let $F = \mathbb{Q}(\sqrt{-3\ell})$ be an imaginary quadratic field contained in these K. We see that $(\mathcal{O}_F/3)^\times = (2,3)$, and that $[E_K]_3 = (3,8)$ is generated by the classes $[\zeta_3]_3$ and $[\varepsilon]_3$. Let $x = 1 + \sqrt{-3\ell}$. We see that the class $[x]_3 \in (\mathcal{O}_F/3)^\times$ is of order 3 but $x \not\equiv \zeta_3, \zeta_3^2 \bmod 3$. Hence, $(\mathcal{O}_F/3)^\times \subsetneq [E_K]_3$. Therefore, any imaginary quadratic field $F \neq \mathbb{Q}(\sqrt{-3})$ contained in these K does not satisfy (A_3). Thus, we have shown the Proposition. ∎

Acknowledgements. The author was partially supported by Grant-in-Aid for Scientific Research (C) (no. 13640036), the Ministry of Education, Culture, Sports, Science and Technology of Japan.

Note added in proof. After this paper was accepted for publication, a paper of J. E. Carter appeared in Arch. Math. (Basel) 81 (2003), 266–271. He gives a necessary and sufficient condition for a number field F to satisfy (A_3). His condition is different from ours, and is obtained by a different method. As an application, he determines the quadratic fields satisfying (A_3). However, some quadratic fields seem to be neglected in his result.

References

[1] J. Brinkhuis, *Normal integral bases and Spiegelungssatz of Scholz*, Acta Arith. 69 (1995), 1–9.

[2] R. J. Chapman, *Kummer theory and Galois module structure in global function fields*, Math. Z. 208 (1991), 250–260.

[3] A. Fröhlich and M. J. Taylor, *Algebraic Number Theory*, Cambridge Univ. Press, Cambridge, 1991.

[4] E. J. Gómez Ayala, *Bases normales d'entiers dans les extensions de Kummer de degré premier*, J. Théor. Nombres Bordeaux 6 (1994), 95–116.

[5] C. Greither, *On normal integral bases in ray class fields over imaginary quadratic fields*, Acta Arith. 78 (1997), 315–329.

[6] C. Greither, D. Replogle, K. Rubin and A. Srivastav, *Swan modules and Hilbert–Speiser number fields*, J. Number Theory 79 (1999), 164–173.

[7] H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Akademie Verlag, Berlin, 1952.

[8] H. Ichimura, *Note on the ring of integers of a Kummer extension of prime degree, IV*, Proc. Japan Acad. Ser. A Math. Sci. 77 (2001), 92–94; *V*, ibid. 78 (2002), 76–79.

[9] —, *On a theorem of Childs on normal bases of rings of integers*, J. London Math. Soc. (2) 68 (2003), 25–36; addendum, ibid., in press.

[10] —, *On the ring of integers of a tame Kummer extension over a number field*, J. Pure Appl. Algebra 187 (2004), 169–182.

[11] —, *On a theorem of Kawamoto on normal bases of rings of integers*, Tokyo J. Math., in press.

[12] F. Kawamoto, *On normal integral bases*, Tokyo J. Math. 7 (1984), 221–231.
[13] —, *Remark on "On normal integral bases"*, ibid. 8 (1985), 275.
[14] K. Uchida, *Imaginary abelian number fields of degrees* 2^m *with class number one*, in: Proc. Internat. Conf. on Class Numbers and Fundamental Units of Algebraic Number Fields (Katata, 1986), Y. Yamamoto and H. Yokoi (eds.), Nagoya Univ., Nagoya, 1986, 151–170.
[15] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Springer, Berlin, 1997.
[16] K. Yamamura, *The determination of imaginary abelian fields of class number one*, Math. Comp. 62 (1994), 899–921.

Department of Mathematics
Yokohama City University
22-2, Seto, Kanazawa-ku
Yokohama 236-0027, Japan
E-mail: ichimura@yokohama-cu.ac.jp

Received on 19.8.2003
and in revised form on 9.10.2003 (4599)