ACTA ARITHMETICA
106.2 (2003)

An infinite family of totally real number fields

by

HUMIO ICHIMURA (Yokohama) and FUMINORI KAWAMOTO (Tokyo)

1. Introduction. This is a continuation of [7]. Let F be a totally real number field of degree n (≥ 2) and ι_i $(1 \leq i \leq n)$ all real embeddings of F. We denote by $\mathfrak{l}_i$ the real prime of F corresponding to ι_i and put $\mathfrak{l}_0 = \mathfrak{l}_0(F) := \mathfrak{l}_1\mathfrak{l}_2 \ldots \mathfrak{l}_n$. For $\mathfrak{l} \mid \mathfrak{l}_0$, $F(\mathfrak{l})$ denotes the ray class field of F mod $\mathfrak{l}$. In particular, $F(1)$ is the Hilbert class field of F. Let K/F be a subextension of $F(\mathfrak{l})/F$ and G its Galois group. We denote by $\mathfrak{o}_F$ and $\mathfrak{o}_K$ the rings of integers in F and K, respectively. If there exists some x in $\mathfrak{o}_K$ such that $\{s(x)\}_{s \in G}$ is a free $\mathfrak{o}_F$-basis of $\mathfrak{o}_K$, then we say that the tamely ramified abelian extension K/F has a *normal integral basis* (abbreviated NIB). Such an element x is called a *generator of NIB* of K/F. We ask whether K/F has an NIB. For this, we consider a subgroup of an elementary abelian 2-group $\mathfrak{o}_F^{\times}/\mathfrak{o}_F^{\times 2}$:

$$\begin{aligned} \mathcal{N}^{\mathfrak{l}} &= \mathcal{N}^{\mathfrak{l}}(F) \\ &:= \{[\eta] \in \mathfrak{o}_F^{\times}/\mathfrak{o}_F^{\times 2} \mid \eta \in \mathfrak{o}_F^{\times}, \eta \equiv 1 \bmod 4, \iota_i(\eta) > 0 \text{ for all } \mathfrak{l}_i \mid \mathfrak{l}_0\mathfrak{l}^{-1}\}. \end{aligned}$$

Here, for a ring R, $R^{\times}$ denotes the group of units in R and $[\eta]$ is the residue class of η. We denote by $\mathbb{Z}$ the ring of all rational integers and put $\mathbb{F}_2 := \mathbb{Z}/2\mathbb{Z}$. Then we can regard $\mathcal{N}^{\mathfrak{l}}$ as a vector space over $\mathbb{F}_2$ with dimension $\leq n$. Furthermore, we put

$$L^{\mathfrak{l}} := F(\{\sqrt{\eta} \mid [\eta] \in \mathcal{N}^{\mathfrak{l}}\}).$$

By Kummer theory, $L^{\mathfrak{l}}$ is a subfield of $F(\mathfrak{l})$ and $L^{\mathfrak{l}}/F$ is an elementary abelian 2-extension of degree $2^{\dim \mathcal{N}^{\mathfrak{l}}}$, where $\dim V$ is the dimension of an $\mathbb{F}_2$-vector space V. In [7], we proved the following theorem, using Brinkhuis [2, Corollary 2.10] (or [3, Corollary 2.1]) and Childs [4, Theorem B].

THEOREM 1. *Let F be a totally real number field and $\mathfrak{l} \mid \mathfrak{l}_0$.*

(i) *The extension $L^{\mathfrak{l}}/F$ is the maximal subextension of $F(\mathfrak{l})/F$ which has an NIB. Furthermore, if $\{[\eta_1], \ldots, [\eta_r]\}$ is an $\mathbb{F}_2$-basis of $\mathcal{N}^{\mathfrak{l}}$ with $\eta_i \equiv 1 \bmod 4$, then $x := \prod_{i=1}^{r}((1 + \sqrt{\eta_i})/2)$ is a generator of NIB of $L^{\mathfrak{l}}/F$.*

2000 *Mathematics Subject Classification*: Primary 11R33.

(ii) *Let K/F be a subextension of $F(\mathfrak{l})/F$. Then K/F has an NIB if and only if $K \subset L^{\mathfrak{l}}$. If the condition is satisfied, then $\mathrm{Tr}_{L^{\mathfrak{l}}/K}(x)$ is a generator of NIB of K/F. In particular, $F(\mathfrak{l})/F$ has an NIB if and only if $h_F = |\mathcal{N}^{\mathfrak{l}}|[F(\mathfrak{l}) : F(1)]^{-1}$. Here, $\mathrm{Tr}_{L^{\mathfrak{l}}/K}$ is the trace map from $L^{\mathfrak{l}}$ to K and h_F denotes the class number of F.*

In view of this theorem, the $\mathbb{F}_2$-vector space $\mathcal{N}^{\mathfrak{l}}$ is naturally of interest. In [7], we determined an $\mathbb{F}_2$-basis of $\mathcal{N}^{\mathfrak{l}}$ for all real quadratic fields and all cyclic cubic fields. The main purpose of this article is to determine an $\mathbb{F}_2$-basis of $\mathcal{N}^{\mathfrak{l}}$ and a generator x of NIB of the abelian extension $L^{\mathfrak{l}}/F$ for a certain family of totally real number fields F which are defined by Eisenstein polynomials

$$f(X) = \prod_{i=1}^{n}(X - a_i) - 2.$$

Here, a_i's are integers satisfying $8 \mid a_i$ and some other conditions. (These types of polynomials are also dealt with in [5].) We state the main result (Proposition 3) in Section 2, and show it in Section 3. Applying Proposition 3 and Theorem 1, we examine whether $F(\mathfrak{l})/F$ has an NIB in (Proposition 6 of) Section 4. The final section is of supplementary nature. First, we show that the above mentioned family of totally real number fields of degree n contains infinite ones (Proposition 7). Next, we give an assertion (Proposition 9) on Galois extensions of prime power degree. As its consequence, we see that when $n = 3$, the cubic fields in this article are not cyclic ones which are dealt with in [7].

Acknowledgments. The second author expresses his appreciation to Yoshitaka Odai for suggesting Proposition 9.

2. Main result. We introduce a family of totally real number fields of Eisenstein type. Let $n \geq 2$ be a positive integer and take $n-1$ odd primes p_i $(2 \leq i \leq n)$ such that

$$p_i \equiv 5 \bmod 8, \quad p_i \nmid (2n-1). \tag{2.1}$$

Furthermore, let $a_1, \ldots, a_n$ be integers which satisfy the conditions (2.2)–(2.5):

$$1 \leq i < j \leq n \ \Rightarrow\ a_j - a_i > 2\sqrt[n]{2}, \tag{2.2}$$

and for each i $(1 \leq i \leq n)$,

$$a_i \equiv 0 \bmod 8, \tag{2.3}$$

$$a_i \equiv -1 \bmod p_i \quad \text{if } i \neq 1, \tag{2.4}$$

$$a_i \equiv 0 \bmod p_j \quad \text{for all } j\ (2 \leq j \leq n,\ j \neq i). \tag{2.5}$$

Then we put

$$f(X) := \prod_{i=1}^{n}(X - a_i) - 2.$$

Since $f(X) \equiv X^n - 2 \bmod 4$ by (2.3), $f(X)$ is an Eisenstein polynomial for 2. Let θ be a root of $f(X)$, and define

$$F := \mathbb{Q}(\theta), \tag{2.6}$$

where $\mathbb{Q}$ denotes the field of all rational numbers. As we shall show at the end of this section, (2.2) and the intermediate value theorem imply that $f(X)$ has n distinct real roots θ_i $(1 \le i \le n)$ satisfying the following: when n is even,

$$\theta_1 < a_1 < a_2 < \theta_2 < \theta_3 < \ldots < \theta_{n-2} < \theta_{n-1} < a_{n-1} < a_n < \theta_n; \tag{2.7}$$

when n is odd,

$$a_1 < \theta_1 < \theta_2 < a_2 < a_3 < \ldots < \theta_{n-2} < \theta_{n-1} < a_{n-1} < a_n < \theta_n. \tag{2.8}$$

In particular, F is totally real. Also, 2 is totally ramified in F: $2\mathfrak{o}_F = \mathfrak{p}^n$. As a_i $(1 \le i \le n)$ is even, we have $\operatorname{ord}_{\mathfrak{p}}(\theta) = 1 < \operatorname{ord}_{\mathfrak{p}}(a_i)$, so that $\operatorname{ord}_{\mathfrak{p}}(\theta - a_i) = 1$; also, we have $\prod_{i=1}^{n}(\theta - a_i) = 2$ since $f(\theta) = 0$. Hence, $\mathfrak{p} = (\theta - a_i)\mathfrak{o}_F$ for all i $(1 \le i \le n)$. Therefore,

$$\varepsilon_i := \frac{\theta - a_i}{\theta - a_1} \tag{2.9}$$

$(2 \le i \le n)$ are elements of $\mathfrak{o}_F^\times$, and (2.3) implies that $\varepsilon_i \equiv 1 \bmod 4$. By (2.1), (2.4) and (2.5), Lemma 2 follows from the same argument as in the proof of [5, Lemma].

LEMMA 2. *Under the above setting*, $\{[-1], [\varepsilon_i] \mid 2 \le i \le n\}$ *is an* $\mathbb{F}_2$*-basis of* $\mathfrak{o}_F^\times/\mathfrak{o}_F^{\times 2}$.

For each i $(1 \le i \le n)$, we define a real embedding ι_i of F by putting $\iota_i(\theta) := \theta_i$. Let $\mathfrak{l}_i$ be the real prime of F corresponding to ι_i. We have $\mathfrak{l}_0 = \mathfrak{l}_1\mathfrak{l}_2\ldots\mathfrak{l}_n$. For $\mathfrak{l} \mid \mathfrak{l}_0$, we define a group $\bar{E}^{\mathfrak{l}}$ by

$$\bar{E}^{\mathfrak{l}} := \{[\eta] \in \mathfrak{o}_F^\times/\mathfrak{o}_F^{\times 2} \mid \eta \in \mathfrak{o}_F^\times,\ \iota_i(\eta) > 0 \text{ for all } \mathfrak{l}_i \mid \mathfrak{l}_0\mathfrak{l}^{-1}\},$$

which we also regard as a vector space over $\mathbb{F}_2$. The vector space $\mathcal{N}^{\mathfrak{l}}$ is a subspace of $\bar{E}^{\mathfrak{l}}$. We determine $\mathbb{F}_2$-bases of $\mathcal{N}^{\mathfrak{l}}$ and of $\bar{E}^{\mathfrak{l}}$, respectively, in Proposition 3 which we show in the next section.

DEFINITION 2.1. Let $\mathfrak{l} \mid \mathfrak{l}_0$. When n is even (resp. odd), we define

$$\begin{aligned} S = S^{\mathfrak{l}} := \{k \mid\ & 1 \le k \le (n-2)/2 \text{ (resp. } (n-1)/2), \\ & i = 2k \text{ or } 2k+1 \text{ (resp. } 2k-1 \text{ or } 2k) \text{ with some } \mathfrak{l}_i \mid \mathfrak{l}_0\mathfrak{l}^{-1}\} \end{aligned}$$

and put $\sigma = \sigma^{\mathfrak{l}} := |S|$. We write $S = \{k_1, \ldots, k_\sigma\}$ with $k_1 < \ldots < k_\sigma$.

Proposition 3. *Let F be a totally real number field as in* (2.6) *of degree n and ε_i $(2 \le i \le n)$ units of F as in* (2.9). *Let $\mathfrak{l} \mid \mathfrak{l}_0$. Then, under the notation of Definition* 2.1, *we have* $\dim \mathcal{N}^{\mathfrak{l}} = n - 1 - \sigma^{\mathfrak{l}}$. *Furthermore, the following hold* (*when* $n = 2$, *we put* $k_0 := 0$ *and* $\varepsilon_1 := 1$):

(i) *Suppose that n is even, and put*

$$\begin{aligned}
A_0 &:= \{[\varepsilon_i] \mid 2 \le i \le 2k_1\},\\
B_0 &:= \{[\varepsilon_i \varepsilon_{2k_{s+1}}] \mid 1 \le s \le \sigma - 1,\ 2k_s + 1 \le i \le 2k_{s+1} - 1\},\\
C_0 &:= \{[-\varepsilon_i] \mid 2k_\sigma + 1 \le i \le n\},\\
D_0 &:= \{[\varepsilon_i \varepsilon_n] \mid 2k_\sigma + 1 \le i \le n - 1\}.
\end{aligned}$$

If $\mathfrak{l}_1 \mathfrak{l}_n \mid \mathfrak{l}$, *then* $A_0 \cup B_0 \cup C_0$ (*resp.* $A_0 \cup B_0 \cup D_0$) *is an* $\mathbb{F}_2$*-basis of* $\bar{E}^{\mathfrak{l}}$ (*resp.* $\mathcal{N}^{\mathfrak{l}}$). *In particular*, $\dim \bar{E}^{\mathfrak{l}} = n - \sigma^{\mathfrak{l}}$. *If* $\mathfrak{l}_1 \mathfrak{l}_n \nmid \mathfrak{l}$, *then* $\bar{E}^{\mathfrak{l}} = \mathcal{N}^{\mathfrak{l}}$, *and* $A_0 \cup B_0 \cup D_0$ *is an* $\mathbb{F}_2$*-basis of* $\mathcal{N}^{\mathfrak{l}}$.

(ii) *Suppose that n is odd, and put*

$$\begin{aligned}
A_1 &:= \{[\varepsilon_i] \mid 2 \le i \le 2k_1 - 1\},\\
B_1 &:= \{[\varepsilon_i \varepsilon_{2k_{s+1}-1}] \mid 1 \le s \le \sigma - 1,\ 2k_s \le i \le 2k_{s+1} - 2\},\\
C_1 &:= \{[-\varepsilon_i] \mid 2k_\sigma \le i \le n\},\\
D_1 &:= \{[\varepsilon_i \varepsilon_n] \mid 2k_\sigma \le i \le n - 1\}.
\end{aligned}$$

If $\mathfrak{l}_n \mid \mathfrak{l}$, *then* $A_1 \cup B_1 \cup C_1$ (*resp.* $A_1 \cup B_1 \cup D_1$) *is an* $\mathbb{F}_2$*-basis of* $\bar{E}^{\mathfrak{l}}$ (*resp.* $\mathcal{N}^{\mathfrak{l}}$). *In particular*, $\dim \bar{E}^{\mathfrak{l}} = n - \sigma^{\mathfrak{l}}$. *If* $\mathfrak{l}_n \nmid \mathfrak{l}$, *then* $\bar{E}^{\mathfrak{l}} = \mathcal{N}^{\mathfrak{l}}$, *and* $A_1 \cup B_1 \cup D_1$ *is an* $\mathbb{F}_2$*-basis of* $\mathcal{N}^{\mathfrak{l}}$.

Since $\varepsilon_i \equiv 1 \bmod 4$ for all i, Theorem 1(i) and Proposition 3 yield:

Corollary 4. *Let the assumption and notation be as in Proposition* 3. *Then an element x of the following form is a generator of NIB of* $L^{\mathfrak{l}}/F$: *when n is even,*

$$x = \prod_{i=2}^{2k_1} \left(\frac{1+\sqrt{\varepsilon_i}}{2}\right) \prod_{s=1}^{\sigma-1} \prod_{i=2k_s+1}^{2k_{s+1}-1} \left(\frac{1+\sqrt{\varepsilon_i \varepsilon_{2k_{s+1}}}}{2}\right) \prod_{i=2k_\sigma+1}^{n-1} \left(\frac{1+\sqrt{\varepsilon_i \varepsilon_n}}{2}\right);$$

when n is odd,

$$x = \prod_{i=2}^{2k_1-1} \left(\frac{1+\sqrt{\varepsilon_i}}{2}\right) \prod_{s=1}^{\sigma-1} \prod_{i=2k_s}^{2k_{s+1}-2} \left(\frac{1+\sqrt{\varepsilon_i \varepsilon_{2k_{s+1}-1}}}{2}\right) \prod_{i=2k_\sigma}^{n-1} \left(\frac{1+\sqrt{\varepsilon_i \varepsilon_n}}{2}\right).$$

Example 2.2. When n is even and $1 \le k \le (n-2)/2$, we list $\dim \mathcal{N}^{\mathfrak{l}}$ for some $\mathfrak{l}$ in Table I.

Table I

$\mathfrak{l}$	$\sigma^{\mathfrak{l}}$	$\dim \mathcal{N}^{\mathfrak{l}}$
$\mathfrak{l}_0$	0	$n-1$
$\mathfrak{l}_0\mathfrak{l}_1^{-1}\mathfrak{l}_n^{-1}$	0	$n-1$
$\mathfrak{l}_2\mathfrak{l}_3\mathfrak{l}_4\dots\mathfrak{l}_{2k+1}$	$(n-2)/2-k$	$n/2+k$
$\mathfrak{l}_2\mathfrak{l}_4\mathfrak{l}_6\dots\mathfrak{l}_{2k}$	$(n-2)/2$	$n/2$
$\mathfrak{l}_1\mathfrak{l}_n$	$(n-2)/2$	$n/2$
1	$(n-2)/2$	$n/2$

Example 2.3. When n (≥ 3) is odd and $1 \leq k \leq (n-1)/2$, we list $\dim \mathcal{N}^{\mathfrak{l}}$ for some $\mathfrak{l}$ in Table II.

Table II

$\mathfrak{l}$	$\sigma^{\mathfrak{l}}$	$\dim \mathcal{N}^{\mathfrak{l}}$
$\mathfrak{l}_0$	0	$n-1$
$\mathfrak{l}_0\mathfrak{l}_n^{-1}$	0	$n-1$
$\mathfrak{l}_1\mathfrak{l}_2\mathfrak{l}_3\dots\mathfrak{l}_{2k}$	$(n-1)/2-k$	$(n-1)/2+k$
$\mathfrak{l}_1\mathfrak{l}_3\mathfrak{l}_5\dots\mathfrak{l}_{2k-1}$	$(n-1)/2$	$(n-1)/2$
$\mathfrak{l}_n$	$(n-1)/2$	$(n-1)/2$
1	$(n-1)/2$	$(n-1)/2$

In order to prove (2.8), we assume that n is odd, and let $1 \leq i \leq n$. Then $f(a_i) = -2 < 0$. If i is odd, since $n-i$ is even, (2.2) implies that

$$\begin{aligned} f(a_i + \sqrt[n]{2}) &= \prod_{j=1}^{i}(a_i - a_j + \sqrt[n]{2}) \prod_{j=i+1}^{n}(a_j - a_i - \sqrt[n]{2}) - 2 \\ &> \sqrt[n]{2}(3\sqrt[n]{2})^{i-1} \cdot (\sqrt[n]{2})^{n-i} - 2 \geq (\sqrt[n]{2})^n - 2 = 0. \end{aligned}$$

Hence, the intermediate value theorem shows that $f(X)$ has a real root in the open interval $(a_i, a_i + \sqrt[n]{2})$. If i is even, since $n-(i-1)$ is even, the same argument implies that $f(a_i - \sqrt[n]{2}) > 0$. Consequently, $f(X)$ has a real root in $(a_i - \sqrt[n]{2}, a_i)$. This implies the condition (2.8), and similarly we obtain (2.7).

3. Proof of Proposition 3. In this section we prove Proposition 3. Let $2 \leq i \leq n$. Then we claim the following: when n is even and $1 \leq k \leq (n-2)/2$,

$$\begin{aligned} &\iota_1(\varepsilon_i) > 0,\ \iota_n(\varepsilon_i) > 0; \quad \iota_{2k}(\varepsilon_i) > 0,\ \iota_{2k+1}(\varepsilon_i) > 0 \quad \text{if } i \leq 2k; \\ &\iota_{2k}(\varepsilon_i) < 0,\ \iota_{2k+1}(\varepsilon_i) < 0 \quad \text{if } i \geq 2k+1; \end{aligned} \tag{3.1}$$

when n is odd and $1 \le k \le (n-1)/2$,

$$\begin{aligned} \iota_n(\varepsilon_i) > 0; \quad \iota_{2k-1}(\varepsilon_i) > 0,\ \iota_{2k}(\varepsilon_i) > 0 \quad \text{if } i \le 2k-1; \\ \iota_{2k-1}(\varepsilon_i) < 0,\ \iota_{2k}(\varepsilon_i) < 0 \quad \text{if } i \ge 2k. \end{aligned} \tag{3.2}$$

These are shown as follows. For each j $(1 \le j \le n)$, we have $\iota_j(\varepsilon_i) = (\theta_j - a_i)/(\theta_j - a_1)$. Assume that n is even and $1 \le k \le (n-2)/2$. Since $\theta_1 < a_1 < a_2 \le a_i$ by (2.7), we obtain $\iota_1(\varepsilon_i) > 0$; also, $a_1 < a_i < \theta_n$ implies that $\iota_n(\varepsilon_i) > 0$. Furthermore, we have

$$a_{2k} < \theta_{2k} < \theta_{2k+1} < a_{2k+1} < a_{2k+2}$$

from (2.7). Hence, if $i \le 2k$ (resp., $i > 2k$), as $a_1 < \theta_{2k}$, we have $\iota_{2k}(\varepsilon_i) > 0$ and $\iota_{2k+1}(\varepsilon_i) > 0$ (resp., $\iota_{2k}(\varepsilon_i) < 0$ and $\iota_{2k+1}(\varepsilon_i) < 0$). Thus (3.1) holds. Similarly, (3.2) follows from (2.8).

Lemma 2 shows that

$$\mathcal{N}^{\mathfrak{l}_0} = \prod_{i=2}^{n} \langle [\varepsilon_i] \rangle \quad \text{and} \quad \mathfrak{o}_F^{\times}/\mathfrak{o}_F^{\times 2} = \langle [-1] \rangle \times \mathcal{N}^{\mathfrak{l}_0}, \tag{3.3}$$

because $\varepsilon_i \equiv 1 \bmod 4$ $(2 \le i \le n)$ and $-1 \not\equiv 1 \bmod 4$. In the remainder of the proof, we let $[\eta] \in \mathfrak{o}_F^{\times}/\mathfrak{o}_F^{\times 2}$, and write $[\eta] = [-1]^{e_1} \prod_{i=2}^{n} [\varepsilon_i]^{e_i}$ with some e_1, e_i in $\{0, 1\}$. It follows immediately from (3.3) that

$$[\eta] \in \mathcal{N}^{\mathfrak{l}} \ (\subset \mathcal{N}^{\mathfrak{l}_0}) \ \Rightarrow \ e_1 = 0. \tag{3.4}$$

If $1 \le j \le n$, then $[\iota_j(\eta)] = [-1]^{e_1} \prod_{i=2}^{n} [\iota_j(\varepsilon_i)]^{e_i}$. We prove only the assertion (i) of Proposition 3, since the same argument implies (ii). By (3.1), if $j = 2k$ or $2k+1$, then

$$\iota_j(\eta) > 0 \ \Leftrightarrow \ e_1 + \sum_{i=2k+1}^{n} e_i \equiv 0 \bmod 2.$$

It follows from this and the definition of $S^{\mathfrak{l}}$ that

$$\begin{aligned} [\eta] \in \bar{E}^{\mathfrak{l}} \ &\Leftrightarrow \ e_1 + \sum_{i=2k_s+1}^{n} e_i \equiv 0 \bmod 2 \text{ for all } s \ (1 \le s \le \sigma) \\ &\Leftrightarrow \ \sum_{i=2k_s+1}^{2k_{s+1}} e_i \equiv 0 \bmod 2 \text{ for all } s \ (1 \le s \le \sigma - 1), \\ &\qquad \text{and } e_1 + \sum_{i=2k_\sigma+1}^{n} e_i \equiv 0 \bmod 2. \end{aligned} \tag{3.5}$$

First, assume that $\mathfrak{l}_1 \mathfrak{l}_n \mid \mathfrak{l}$, and $[\eta] \in \bar{E}^{\mathfrak{l}}$ (resp., $\in \mathcal{N}^{\mathfrak{l}}$). Then (3.5) and (3.4) imply that $e_{2k_{s+1}} \equiv \sum_{i=2k_s+1}^{2k_{s+1}-1} e_i$ for all s $(1 \le s \le \sigma - 1)$, and $e_1 \equiv$

$\sum_{i=2k_\sigma+1}^{n} e_i \bmod 2$ (resp., $e_n \equiv \sum_{i=2k_\sigma+1}^{n-1} e_i \bmod 2$). Hence,

$$[\eta] = \prod_{i=2}^{2k_1}[\varepsilon_i]^{e_i} \prod_{s=1}^{\sigma-1}\prod_{i=2k_s+1}^{2k_{s+1}-1}[\varepsilon_i\varepsilon_{2k_{s+1}}]^{e_i} \times \prod_{i=2k_\sigma+1}^{n}[-\varepsilon_i]^{e_i}$$
$$\left(\text{resp. } \times \prod_{i=2k_\sigma+1}^{n-1}[\varepsilon_i\varepsilon_n]^{e_i}\right).$$

Also, all elements of $A_0 \cup B_0 \cup C_0$ (resp. $A_0 \cup B_0 \cup D_0$) are in $\bar{E}^{\mathfrak{l}}$ (resp. $\mathcal{N}^{\mathfrak{l}}$) by (3.5), and are linearly independent over $\mathbb{F}_2$ by (3.3). Therefore this set constitutes an $\mathbb{F}_2$-basis of $\bar{E}^{\mathfrak{l}}$ (resp. $\mathcal{N}^{\mathfrak{l}}$). So,

$$\dim \bar{E}^{\mathfrak{l}} = (2k_1 - 1) + \sum_{s=1}^{\sigma-1}(2k_{s+1} - 2k_s - 1) + (n - 2k_\sigma) = n - \sigma.$$

Similarly, we have $\dim \mathcal{N}^{\mathfrak{l}} = n - 1 - \sigma$.

Next, assume that $\mathfrak{l}_1\mathfrak{l}_n \nmid \mathfrak{l}$ and $[\eta] \in \bar{E}^{\mathfrak{l}}$. Then $\iota_1(\eta) > 0$ or $\iota_n(\eta) > 0$; therefore we have $e_1 = 0$ by (3.1). Hence, (3.3) implies that $\bar{E}^{\mathfrak{l}} = \mathcal{N}^{\mathfrak{l}}$. By the same argument as above, $A_0 \cup B_0 \cup D_0$ is an $\mathbb{F}_2$-basis of $\mathcal{N}^{\mathfrak{l}}$. This proves (i). ∎

4. NIB of $F(\mathfrak{l})/F$. In this section, using Proposition 3, we examine whether $F(\mathfrak{l})/F$ has an NIB. We assume that F is a totally real number field as in (2.6) of degree n, and $\mathfrak{l}_i$ $(1 \le i \le n)$ is the real prime of F corresponding to the real embedding ι_i, defined in Section 2. For $\mathfrak{l} \mid \mathfrak{l}_0$, let $\varrho_{\mathfrak{l}}$ denote the number of distinct prime divisors of $\mathfrak{l}$. Then the Galois group $\mathrm{Gal}(F(\mathfrak{l})/F(1))$ is an elementary abelian 2-group, which is also regarded as a vector space over $\mathbb{F}_2$. We have

$$\delta_{\mathfrak{l}} := \dim \mathrm{Gal}(F(\mathfrak{l})/F(1)) = \dim \bar{E}^{\mathfrak{l}_0\mathfrak{l}^{-1}} - \varrho_{\mathfrak{l}_0\mathfrak{l}^{-1}} \tag{4.1}$$

(cf. [7, Section 3]).

LEMMA 5. *Let* $\mathfrak{l} \mid \mathfrak{l}_0$.

(i) *When n is even, if* $\mathfrak{l} \mid \mathfrak{l}_0\mathfrak{l}_1^{-1}\mathfrak{l}_n^{-1}$ *then* $\delta_{\mathfrak{l}} = \varrho_{\mathfrak{l}} - \sigma^{\mathfrak{l}_0\mathfrak{l}^{-1}}$, *and otherwise* $\delta_{\mathfrak{l}} = \varrho_{\mathfrak{l}} - \sigma^{\mathfrak{l}_0\mathfrak{l}^{-1}} - 1$.

(ii) *When n is odd, if* $\mathfrak{l} \mid \mathfrak{l}_0\mathfrak{l}_n^{-1}$ *then* $\delta_{\mathfrak{l}} = \varrho_{\mathfrak{l}} - \sigma^{\mathfrak{l}_0\mathfrak{l}^{-1}}$, *and otherwise* $\delta_{\mathfrak{l}} = \varrho_{\mathfrak{l}} - \sigma^{\mathfrak{l}_0\mathfrak{l}^{-1}} - 1$.

Proof. Using Proposition 3, we can calculate $\delta_{\mathfrak{l}}$ from (4.1). If $\mathfrak{l} \mid \mathfrak{l}_0\mathfrak{l}_1^{-1}\mathfrak{l}_n^{-1}$, since $\mathfrak{l}_1\mathfrak{l}_n \mid \mathfrak{l}_0\mathfrak{l}^{-1}$, we have $\delta_{\mathfrak{l}} = (n - \sigma^{\mathfrak{l}_0\mathfrak{l}^{-1}}) - \varrho_{\mathfrak{l}_0\mathfrak{l}^{-1}} = \varrho_{\mathfrak{l}} - \sigma^{\mathfrak{l}_0\mathfrak{l}^{-1}}$. If $\mathfrak{l} \nmid \mathfrak{l}_0\mathfrak{l}_1^{-1}\mathfrak{l}_n^{-1}$, then $\delta_{\mathfrak{l}} = (n - 1 - \sigma^{\mathfrak{l}_0\mathfrak{l}^{-1}}) - \varrho_{\mathfrak{l}_0\mathfrak{l}^{-1}} = \varrho_{\mathfrak{l}} - \sigma^{\mathfrak{l}_0\mathfrak{l}^{-1}} - 1$. Hence we obtain (i); the proof of (ii) is similar. ∎

PROPOSITION 6. *We have* $2\text{-rank}\,\mathrm{Gal}(F(1)/F) \ge [n/2]$, *where* $[\alpha]$ *denotes the largest integer not exceeding a real number* α. *Furthermore, let*

$\mathfrak{l} \mid \mathfrak{l}_0$. *Then:*

(i) *When "n is even and $\mathfrak{l}_1\mathfrak{l}_n \nmid \mathfrak{l}$", or n is odd, we have: $F(\mathfrak{l})/F$ has an NIB if and only if $h_F = 2^{[n/2]}$.*

(ii) *When n is even and $\mathfrak{l}_1\mathfrak{l}_n \mid \mathfrak{l}$, $F(\mathfrak{l})/F$ has no NIB.*

Proof. Since L^1 is a subfield of $F(1)$, we have

$$2\text{-rank}\,\mathrm{Gal}(F(1)/F) \geq 2\text{-rank}\,\mathrm{Gal}(L^1/F) = \dim \mathcal{N}^1.$$

Examples 2.2 and 2.3 imply that $\dim \mathcal{N}^1 = [n/2]$. Therefore we obtain $2\text{-rank}\,\mathrm{Gal}(F(1)/F) \geq [n/2]$. If we write $|\mathcal{N}^{\mathfrak{l}}|[F(\mathfrak{l}) : F(1)]^{-1} = 2^{e_{\mathfrak{l}}}$ with some integer $e_{\mathfrak{l}}$, then Proposition 3 yields

$$e_{\mathfrak{l}} = n - 1 - (\sigma^{\mathfrak{l}} + \delta_{\mathfrak{l}}). \tag{4.2}$$

As before, let $S = S^{\mathfrak{l}}$ and $\sigma = \sigma^{\mathfrak{l}}$. For brevity, put $S' := S^{\mathfrak{l}_0\mathfrak{l}^{-1}}$, $\sigma' := |S'|$, and $t := |S \cap S'|$. To show Proposition 6, we first write $\varrho_{\mathfrak{l}}$ and $\varrho_{\mathfrak{l}_0\mathfrak{l}^{-1}}$ in terms of σ, σ', t (and next calculate $e_{\mathfrak{l}}$). For this, the following remark is useful. When n is even, we see from the definition of S and S' that (I) if $k \in S \cap S'$ then either "$\mathfrak{l}_{2k} \mid \mathfrak{l}_0\mathfrak{l}^{-1}$ and $\mathfrak{l}_{2k+1} \mid \mathfrak{l}$", or "$\mathfrak{l}_{2k+1} \mid \mathfrak{l}_0\mathfrak{l}^{-1}$ and $\mathfrak{l}_{2k} \mid \mathfrak{l}$", and that (II) if $k \in S - (S \cap S')$ (resp., $\in S' - (S \cap S')$), then $\mathfrak{l}_{2k}\mathfrak{l}_{2k+1} \mid \mathfrak{l}_0\mathfrak{l}^{-1}$ (resp., $\mathfrak{l}_{2k}\mathfrak{l}_{2k+1} \mid \mathfrak{l}$). A similar assertion holds for n odd.

(A) *The case where n is even.* When $\mathfrak{l} \nmid \mathfrak{l}_0\mathfrak{l}_1^{-1}\mathfrak{l}_n^{-1}$, we put $u := |\{1, n\} \cap \{i;\ \mathfrak{l}_i \mid \mathfrak{l}\}|$. If $\mathfrak{l} \mid \mathfrak{l}_0\mathfrak{l}_1^{-1}\mathfrak{l}_n^{-1}$ (resp., $\mathfrak{l} \nmid \mathfrak{l}_0\mathfrak{l}_1^{-1}\mathfrak{l}_n^{-1}$), by the above remark, we have $\varrho_{\mathfrak{l}_0\mathfrak{l}^{-1}} = t + 2(\sigma - t) + 2$ and $\varrho_{\mathfrak{l}} = t + 2(\sigma' - t)$ (resp., $\varrho_{\mathfrak{l}_0\mathfrak{l}^{-1}} = t + 2(\sigma - t) + 2 - u$ and $\varrho_{\mathfrak{l}} = t + 2(\sigma' - t) + u$). Consequently, $\varrho_{\mathfrak{l}_0\mathfrak{l}^{-1}} - \varrho_{\mathfrak{l}} = 2(\sigma - \sigma') + 2$ (resp., $\varrho_{\mathfrak{l}_0\mathfrak{l}^{-1}} - \varrho_{\mathfrak{l}} = 2(\sigma - \sigma') + 2 - 2u$). On the other hand, we clearly have $\varrho_{\mathfrak{l}_0\mathfrak{l}^{-1}} + \varrho_{\mathfrak{l}} = n$. Therefore, we obtain

$$(n-2)/2 \ (\text{resp. } n/2 + u - 1) = \varrho_{\mathfrak{l}} + \sigma - \sigma'. \tag{4.3}$$

By (4.2) and Lemma 5(i), we obtain $e_{\mathfrak{l}} = n - 1 - (\sigma + \varrho_{\mathfrak{l}} - \sigma')$ (resp., $= n - (\sigma + \varrho_{\mathfrak{l}} - \sigma')$). Hence, (4.3) implies that $e_{\mathfrak{l}} = n/2$ (resp., $= n/2 - (u-1)$). Since $u = 1$ or 2, if $\mathfrak{l}_1\mathfrak{l}_n \nmid \mathfrak{l}$ (resp., $\mathfrak{l}_1\mathfrak{l}_n \mid \mathfrak{l}$) then $e_{\mathfrak{l}} = n/2$ (resp., $= n/2 - 1$).

(B) *The case where n is odd.* If $\mathfrak{l} \mid \mathfrak{l}_0\mathfrak{l}_n^{-1}$ (resp., $\mathfrak{l} \nmid \mathfrak{l}_0\mathfrak{l}_n^{-1}$), by the above remark, we have $\varrho_{\mathfrak{l}_0\mathfrak{l}^{-1}} = t + 2(\sigma - t) + 1$ and $\varrho_{\mathfrak{l}} = t + 2(\sigma' - t)$ (resp., $\varrho_{\mathfrak{l}_0\mathfrak{l}^{-1}} = t + 2(\sigma - t)$ and $\varrho_{\mathfrak{l}} = t + 2(\sigma' - t) + 1$); consequently, $\varrho_{\mathfrak{l}_0\mathfrak{l}^{-1}} - \varrho_{\mathfrak{l}} = 2(\sigma - \sigma') + 1$ (resp., $\varrho_{\mathfrak{l}_0\mathfrak{l}^{-1}} - \varrho_{\mathfrak{l}} = 2(\sigma - \sigma') - 1$); therefore,

$$(n-1)/2 \ (\text{resp. } (n+1)/2) = \varrho_{\mathfrak{l}} + \sigma - \sigma'. \tag{4.4}$$

By (4.2) and Lemma 5(ii), we obtain $e_{\mathfrak{l}} = n - 1 - (\sigma + \varrho_{\mathfrak{l}} - \sigma')$ (resp., $= n - (\sigma + \varrho_{\mathfrak{l}} - \sigma')$). Hence, (4.4) implies that $e_{\mathfrak{l}} = (n-1)/2$.

Theorem 1(ii) shows that $F(\mathfrak{l})/F$ has an NIB if and only if $h_F = 2^{e_{\mathfrak{l}}}$. When "$n$ is even and $\mathfrak{l}_1\mathfrak{l}_n \nmid \mathfrak{l}$", or n is odd, (A) and (B) imply that $e_{\mathfrak{l}} = [n/2]$. Hence the assertion (i) holds. When n is even and $\mathfrak{l}_1\mathfrak{l}_n \mid \mathfrak{l}$, since $2^{[n/2]} \mid h_F$, it follows from (A) that

$$2^{e_{\mathfrak{l}}} = 2^{n/2-1} < 2^{[n/2]} \le h_F.$$

Hence $F(\mathfrak{l})/F$ has no NIB. This proves our proposition. ∎

Assume that $h_F = 2^{[n/2]}$. When n is even, Proposition 6 implies that $F(\mathfrak{l})/F$ has an NIB if and only if $\mathfrak{l}_1\mathfrak{l}_n \nmid \mathfrak{l}$. Also, when n is odd, $F(\mathfrak{l})/F$ has an NIB for all $\mathfrak{l} \mid \mathfrak{l}_0$. On the other hand, if $h_F \neq 2^{[n/2]}$ then $F(\mathfrak{l})/F$ has no NIB for all $\mathfrak{l} \mid \mathfrak{l}_0$. Thus the existence of NIB of $F(\mathfrak{l})/F$ is determined by the condition on the class number h_F and an integral divisor $\mathfrak{l}$.

REMARK 4.1. Suppose that $n = 2$. Let ε (> 1) be the fundamental unit of F and g the order of ε mod 4 in $(\mathfrak{o}_F/4\mathfrak{o}_F)^\times$. By Lemma 2, we see that the index $(\mathfrak{o}_F^\times : \langle -1\rangle \times \langle \varepsilon_2\rangle)$ is odd, where the unit ε_2 is defined in (2.9). This implies that g is odd and ε is totally positive. Hence, Proposition 6 for $n = 2$ also follows from [7, Corollaries 11 and 12].

EXAMPLE 4.2. Let Cl_F be the ideal class group of F. For a positive integer m, we denote by C_m a cyclic group of order m. We consider a real quadratic field F which is defined by a polynomial of the form $f(X) = X(X - a_2) - 2$, where a_2 is an integer such that $a_2 \equiv 0 \bmod 8$ and $a_2 \equiv -1 \bmod p_2$, p_2 being a prime with $p_2 \equiv 5 \bmod 8$. For all fields F in Table III, by using PARI [1], we see that $F(1)/F$ has a relative integral basis, that is, $\mathfrak{o}_{F(1)}$ has a free $\mathfrak{o}_F$-basis; we can also obtain the same result by using KASH [8] (cf. [7, Section 5]). But, as $h_F \neq 2$, $F(1)/F$ has no NIB by Proposition 6.

Table III

p_2	a_2	Cl_F	h_F
5	224	$C_2 \times C_2$	4
5	424	C_6	6
5	54744	$C_2 \times C_2$	4
5	138944	$C_2 \times C_2$	4
5	156624	$C_2 \times C_2$	4
13	168	C_6	6
13	13896	C_6	6
29	11512	$C_2 \times C_2$	4
157	23392	$C_2 \times C_2$	4

5. Supplements. In this section we prove Propositions 7 and 9.

PROPOSITION 7. *For each positive integer $n \ge 2$, there exist infinitely many totally real number fields F as in* (2.6) *of degree n.*

For the proof, we need:

LEMMA 8. *Let $n \geq 2$ be a positive integer and $\beta \in \mathbb{Z}$, $\beta \neq 0$. Then there exist infinitely many primes l that satisfy the following two conditions*:

(i) $l \nmid \beta n(n-1)$.

(ii) *There is some $a(l)$ in $\mathbb{Z}$ such that* $\mathrm{ord}_l(d(g_a)) = 1$ *for all integers a with $a \equiv a(l) \bmod l^2$, where we put $g_a(X) := X^n - aX^{n-1} - \beta$ and denote by $d(g_a)$ the discriminant of $g_a(X)$.*

Proof. Let ζ_n be a primitive nth root of unity, and put

$$K := \mathbb{Q}(\sqrt[n]{-\beta(n-1)}) \quad \text{and} \quad N := K(\zeta_n).$$

Since $N/\mathbb{Q}$ is Galois, by the Dirichlet density theorem, there exist infinitely many primes l such that $l \nmid \beta n(n-1)$ and l is completely decomposed in N. Take such a prime l and let $\mathcal{L}$ be a prime ideal of $\mathfrak{o}_K$ lying above l. Since l is a prime element of $\mathcal{L}$, we have

$$\mathfrak{o}_K/\mathcal{L}^2 = \{(a_0 + a_1 l) \bmod \mathcal{L}^2 \mid a_0, a_1 \in \mathbb{Z}/l\mathbb{Z}\}.$$

Therefore there is some b in $\mathbb{Z}$ such that

$$b \equiv \sqrt[n]{-\beta(n-1)}\,\frac{n}{n-1} \bmod \mathcal{L}^2. \tag{5.1}$$

Since $l \nmid \beta n(n-1)$, we have $l \nmid b$. Put $a(l) := b + l$. Let a be an integer with $a \equiv a(l) \bmod l^2$ and put $g(X) := X^n - aX^{n-1} - \beta$. By Swan [9, Theorem 2], we have

$$\begin{aligned} d(g) &= (-1)^{n(n-1)/2}(-\beta)^{n-2}\{(-1)^{n-1}(n-1)^{n-1}(-a)^n - n^n\beta\} \\ &= (-1)^{(n+2)(n-1)/2}\beta^{n-2}\{(n-1)^{n-1}a^n + n^n\beta\}. \end{aligned} \tag{5.2}$$

As the definition of a and (5.1) imply that

$$a^n \equiv a(l)^n \equiv b^n + nb^{n-1}l \equiv -\beta(n-1)(n/(n-1))^n + nb^{n-1}l \bmod l^2,$$

we obtain $(n-1)^{n-1}a^n + n^n\beta \equiv n(n-1)^{n-1}b^{n-1}l \bmod l^2$. Hence, (5.2) yields

$$d(g) \equiv (-1)^{(n+2)(n-1)/2}\beta^{n-2}n(n-1)^{n-1}b^{n-1}l \bmod l^2.$$

As $l \nmid \beta n(n-1)b$, we have $\mathrm{ord}_l(d(g)) = 1$. This proves our lemma. ∎

Proof of Proposition 7. Let $F_1, \ldots, F_t$ be finitely many distinct fields as in (2.6). It follows from Lemma 8 for $\beta = 2$ that there exist some odd prime l and some $a(l)$ in $\mathbb{Z}$ such that $\mathrm{ord}_l(d(g)) = 1$ and l is unramified in each F_i $(1 \leq i \leq t)$, where we put $g(X) := X^n - a(l)X^{n-1} - 2$. Take $n-1$ odd primes p_i $(2 \leq i \leq n)$ with $p_i \neq l$ satisfying (2.1), and let $a_1, \ldots, a_n$ be integers which satisfy (2.2)–(2.5),

$$a_1 \equiv a(l) \bmod l^2, \quad \text{and} \quad a_i \equiv 0 \bmod l^2 \quad \text{for all } i\ (2 \leq i \leq n). \tag{5.3}$$

Then we define a field F as in (2.6). Since (5.3) implies that $f(X) \equiv g(X) \bmod l^2$, we have $\mathrm{ord}_l(d(f)) = 1$. If d_F is the absolute discriminant of F, then $d(f) = d_F \cdot (\mathfrak{o}_F : \mathbb{Z}[\theta])^2$. Hence, $l \mid d_F$. Therefore, l is ramified in F, and $F \neq F_1, \ldots, F_t$. ∎

When the degree n is a power of odd prime, Proposition 9 implies that a field F as in (2.6) is not Galois over $\mathbb{Q}$, because 2 is (totally) ramified in F. In particular, when $n = 3$, we see that F is not a cyclic cubic field.

PROPOSITION 9. *Let $F/\mathbb{Q}$ be a Galois extension of prime power degree, say l^t. Suppose that p is a prime such that $p \neq l$ and $p \not\equiv 1 \bmod l$. Then p is unramified in F. In particular, if l is odd then 2 is unramified in F.*

Proof. Let $G := \mathrm{Gal}(F/\mathbb{Q})$ and $\mathfrak{p}$ a prime ideal of $\mathfrak{o}_F$ lying above p. For each non-negative integer m, we put

$$G_m := \{s \in G \mid s(x) \equiv x \bmod \mathfrak{p}^{m+1} \text{ for all } x \text{ in } \mathfrak{o}_F\}.$$

Then it is known that $|G_0/G_1| \mid (N\mathfrak{p} - 1)$, and $|G_m/G_{m+1}| \mid N\mathfrak{p}$ for each $m \geq 1$ (cf. Iwasawa [6, Proposition 2.19]), where $N\mathfrak{p}$ is the absolute norm of $\mathfrak{p}$. As $p \neq l$, we obtain $G_m = \{1\}$ for all $m \geq 1$. Hence, $|G_0| \mid (N\mathfrak{p} - 1)$. Let f be the residue degree of $\mathfrak{p}$ in $F/\mathbb{Q}$: $N\mathfrak{p} = p^f$. Since $F/\mathbb{Q}$ is Galois, both f and $|G_0|$ divide l^t. By Fermat's little theorem, we obtain $N\mathfrak{p} \equiv p \bmod l$. Then, since the assumption implies that $l \nmid (N\mathfrak{p} - 1)$, we have $l \nmid |G_0|$. Hence, $G_0 = \{1\}$, therefore p is unramified in F. This proves our proposition. ∎

References

[1] C. Batut, K. Belabas, D. Bernardi, H. Cohen and M. Olivier, GP/PARI calculator, Version 2.0.17 (beta).

[2] J. Brinkhuis, *Unramified abelian extensions of CM-fields and their Galois module structure*, Bull. London Math. Soc. 24 (1992), 236–242.

[3] —, *On the Galois module structure over CM-fields*, Manuscripta Math. 75 (1992), 333–347.

[4] L. Childs, *The group of unramified Kummer extensions of prime degree*, Proc. London Math. Soc. 35 (1977), 407–422.

[5] H. Ichimura, *A note on unramified quadratic extensions over algebraic number fields*, Proc. Japan Acad. Ser. A 76 (2000), 78–81.

[6] K. Iwasawa, *Local Class Field Theory*, Oxford Univ. Press, 1986.

[7] F. Kawamoto and Y. Odai, *Normal integral bases of ∞-ramified abelian extensions of totally real number fields*, Abh. Math. Sem. Univ. Hamburg, to appear.

[8] M. Pohst, KANT/KASH calculator, Version 2.2.

[9] R. Swan, *Factorization of polynomials over finite fields*, Pacific J. Math. 12 (1962), 1099–1106.

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

Department of Mathematics
Faculty of Science, Gakushuin University
1-5-1 Mejiro Toshima-ku
Tokyo 171-8588, Japan
E-mail: fuminori.kawamoto@gakushuin.ac.jp

Received on 23.8.2001
and in revised form on 11.3.2002 (4095)