Normal integral basis and ray class group modulo 4

By Humio ICHIMURA*) and Fuminori KAWAMOTO**)

(Communicated by Shokichi IYANAGA, M. J. A., Nov. 12, 2003)

Abstract: We prove that a number field K satisfies the following property (B) if and only if the ray class group of K defined modulo 4 is trivial. (B): For any tame abelian extensions N_1 and N_2 over K of exponent 2, the composite N_1N_2/K has a relative normal integral basis (NIB) if both N_1/K and N_2/K have a NIB.

Key words: Normal integral basis; ray class group.

1. Introduction. For a number field K and an integral divisor $\mathfrak{M}$ of K, let $K(\mathfrak{M})$ be the ray class field of K modulo $\mathfrak{M}$, and $Cl_{K,\mathfrak{M}}$ the ray class group modulo $\mathfrak{M}$. Denote by $\mathfrak{M}_\infty$ the product of the real primes of K. When K is totally real and $\mathfrak{M}$ divides $\mathfrak{M}_\infty$, Kawamoto and Odai [6] showed that there exists a unique intermediate field $L_{\mathfrak{M}}$ of $K(\mathfrak{M})/K$ such that (i) $L_{\mathfrak{M}}/K$ has a relative normal integral basis (NIB for short) and (ii) any intermediate field N of $K(\mathfrak{M})/K$ is contained in $L_{\mathfrak{M}}$ if N/K has a NIB. Further, it is shown that the Galois group $\mathrm{Gal}(L_{\mathfrak{M}}/K)$ is of exponent 2, and a generator of a NIB of $L_{\mathfrak{M}}/K$ is given in terms of units of K. (Here, an abelian group G is of exponent 2 when $x^2 = 1$ for all $x \in G$.) These results are obtained by using some results of Brinkhuis [1] and Childs [2].

In Kawamoto [5], we asked the following question on the existence of such an intermediate field $L_{\mathfrak{M}}$ for general $\mathfrak{M}$.

Question. Characterize a number field K enjoying the following property (A).

(A) For any integral divisor $\mathfrak{M}$ of K, there exists a unique intermediate field $L_{\mathfrak{M}}$ of $K(\mathfrak{M})/K$ such that

(i) $L_{\mathfrak{M}}/K$ has a NIB and $\mathrm{Gal}(L_{\mathfrak{M}}/K)$ is of exponent 2,

and

(ii) any intermediate field N of $K(\mathfrak{M})/K$ is contained in $L_{\mathfrak{M}}$ if N/K has a NIB and $\mathrm{Gal}(N/K)$ is of exponent 2.

We easily see that the condition (A) on K is equivalent to the following condition:

(B) For any (tame) abelian extensions N_1 and N_2 over K of exponent 2, the composite N_1N_2/K has a NIB if both N_1/K and N_2/K have a NIB.

Let $h_K = |Cl_{K,1}|$ be the class number of K in the usual sense. In [5], it is shown that if a number field K satisfies (A), then $h_K = 1$ and $Cl_{K,4\mathfrak{M}_\infty}$ is of exponent 2. The purpose of the present article is to strengthen this result as follows:

Theorem. *A number field K enjoys the property* (A) *if and only if the ray class group $Cl_{K,4}$ is trivial.*

For a number field K, let $\mathcal{O}_K$ be the ring of integers and $E_K = \mathcal{O}_K^\times$ the group of units of K. For an integer $n \geq 2$, let $[E_K]_n$ be the subgroup of the multiplicative group $(\mathcal{O}_K/n)^\times = (\mathcal{O}_K/n\mathcal{O}_K)^\times$ generated by the classes containing units of K. We have $Cl_{K,4} = \{0\}$ if and only if $h_K = 1$ and $(\mathcal{O}_K/4)^\times = [E_K]_4$. The condition $(\mathcal{O}_K/4)^\times = [E_K]_4$ is satisfied only when K is totally real (Lemma 4). In Section 3, we deal with a real quadratic field with odd class number and give a simple necessary and sufficient condition for $(\mathcal{O}_K/4)^\times = [E_K]_4$.

2. Proof of Theorem. The following assertion was shown in Ichimura [3, Proposition 3].

Lemma 1. *For a number field K, the following two conditions are equivalent.*

(i) *Any tame abelian extension over K of exponent 2 has a NIB.*

(ii) *We have $Cl_{K,4} = \{0\}$.*

Proof of the "if" part of Theorem. Let $L_{\mathfrak{M}}$ be the composite of all tame quadratic extensions of K contained in $K(\mathfrak{M})$. Then, from Lemma 1, we see that $L_{\mathfrak{M}}$ has the desired property. □

2000 Mathematics Subject Classification. 11R33.

*) Department of Mathematics, Faculty of Sciences, Yokohama City University, 22-2, Seto, Kanazawa-ku, Yokohama, Kanagawa 236-0027.

**) Department of Mathematics, Faculty of Sciences, Gakushuin University, 1-5-1, Mejiro, Toshima-ku, Tokyo 171-8588.

The following lemma was shown in Massy [7, Section 3].

Lemma 2. *Let N/K be a tame quadratic extension of a number field K, and let $\wp_1, \dots, \wp_r$ be all the prime ideals of K ramified at N. Then, N/K has a NIB if and only if there exists an integer d of K with $N = K(\sqrt{d})$ such that $d \equiv 1 \bmod 4$ and $d\mathcal{O}_K = \wp_1 \cdots \wp_r$.*

Lemma 3. *Assume that a number field K satisfies the property* (A). *Then, the ray class group $Cl_{K,2}$ is trivial.*

Proof. Let $\mathfrak{P}$ be an arbitrary prime ideal of K with $\mathfrak{P} \nmid 2$, and $C \in Cl_{K,4}$ the ray ideal class modulo 4 containing $\mathfrak{P}$. Let $\mathfrak{Q}_1$, $\mathfrak{Q}_2$ be prime ideals of K contained in C^{-1} with $\mathfrak{Q}_i \nmid 2\mathfrak{P}$ and $\mathfrak{Q}_1 \neq \mathfrak{Q}_2$. Then, there exist integers $d_i \in \mathcal{O}_K$ $(i = 1, 2)$ such that

$$(1) \qquad d_i \equiv 1 \bmod 4 \quad \text{and} \quad \mathfrak{P}\mathfrak{Q}_i = d_i\mathcal{O}_K.$$

We put $N_1 = K(\sqrt{d_1})$, $N_2 = K(\sqrt{d_2})$, $N_3 = K(\sqrt{d_1 d_2})$. These are quadratic extensions over K. By Lemma 2 and (1), N_1/K and N_2/K have a NIB. Then, the composite N_1N_2/K has a NIB as K satisfies (A) (or equivalently, (B)). Hence, N_3/K has a NIB as $N_3 \subseteq N_1N_2$. By Lemma 2, we can write $N_3 = K(\sqrt{d})$ for some integer $d \in \mathcal{O}_K$ such that

$$(2) \qquad d \equiv 1 \bmod 4 \quad \text{and} \quad d\mathcal{O}_K = \mathfrak{Q}_1\mathfrak{Q}_2.$$

As $K(\sqrt{d_1 d_2}) = K(\sqrt{d})$, we have

$$d_1 d_2 = dx^2$$

for some $x \in K^\times$. Therefore, it follows from (1) and (2) that $\mathfrak{P} = x\mathcal{O}_K$ and $x^2 \equiv 1 \bmod 4$. The last condition implies $x \equiv 1 \bmod 2$. Hence, it follows that the ray class group $Cl_{K,2}$ is trivial as $\mathfrak{P}$ is an arbitrary prime ideal (with $\mathfrak{P} \nmid 2$). □

Proof of the "only if" part of Theorem. Assume that K satisfies the condition (A) (or equivalently, (B)). Then, by Lemma 3, we have $Cl_{K,2} = \{0\}$. Namely, we have $h_K = 1$ and $(\mathcal{O}_K/2)^\times = [E_K]_2$. It follows from these conditions that any tame quadratic extension N/K has a NIB. Though this fact is known to specialists, we give a proof for the sake of completeness.

Let N/K be a tame quadratic extension. Then, as $h_K = 1$, we see that $N = K(\sqrt{a})$ for some integer $a \in \mathcal{O}_K$ with $(a, 2) = 1$ such that the integral ideal $a\mathcal{O}_K$ is square free in the semi-group of integral ideals of K. As N/K is tame, we have $a \equiv u^2 \bmod 4$ for some $u \in \mathcal{O}_K$. It follows from this that $a \equiv \epsilon^2 \bmod 4$ for some unit $\epsilon \in E_K$ because $(\mathcal{O}_K/2)^\times = [E_K]_2$. Hence, by Lemma 2, N/K has a NIB.

Now, from the above, we see that any tame abelian extension of exponent 2 has a NIB since we are assuming the condition (B). Therefore, we obtain $Cl_{K,4} = \{0\}$ by Lemma 1. □

3. Real quadratic fields. First, we show the following lemma mentioned in Section 1.

Lemma 4. *For a number field K, the condition $(\mathcal{O}_K/4)^\times = [E_K]_4$ is satisfied only when K is totally real.*

Proof. Denote by ρ_1 and ρ_2 the 2-ranks of the abelian groups $[E_K]_4$ and $(\mathcal{O}_K/4)^\times$, respectively. Let r_1 (resp. r_2) be the number of real (resp. complex) primes of K. By the Dirichlet unit theorem, we have

$$\rho_1 \leq r_1 + r_2.$$

Let $2\mathcal{O}_K = \wp_1^{e_1} \cdots \wp_s^{e_s}$ be the prime decomposition in K,and let f_i be the degree of the prime ideal $\wp_i$. Let A be the subgroup of $(\mathcal{O}_K/4)^\times$ consisting of classes $[x]_4$ with $x \equiv 1 \bmod 2$. Clearly, we have

$$A = \bigoplus_{i=1}^{s} A_i$$

with

$$A_i = \frac{\{x \in \mathcal{O}_K \mid x \equiv 1 \bmod \wp_i^{e_i}\}}{\{x \in \mathcal{O}_K \mid x \equiv 1 \bmod \wp_i^{2e_i}\}}.$$

As A is of exponent 2, we see that

$$\rho_2 \geq \mathrm{ord}_2(|A|) = \sum_i \mathrm{ord}_2(|A_i|)$$
$$= \sum_i e_i f_i = r_1 + 2r_2.$$

Here, $|X|$ is the cardinality of a finite set X, and $\mathrm{ord}_2(*)$ is the additive valuation on the rationals $\boldsymbol{Q}$ with $\mathrm{ord}_2(2) = 1$. The assertion follows from the above two inequalities. □

Let $K = \boldsymbol{Q}(\sqrt{m})$ be a real quadratic field with a square free integer $m > 1$, and let ϵ be a fundamental unit of K. We show the following:

Proposition. *Under the above setting, assume that the class number h_K of K is odd. Then, we have $(\mathcal{O}_K/4)^\times = [E_K]_4$ if and only if one of the following three conditions holds.*

(i) $m = 2$.
(ii) *$m = p$ is a prime number with $p \equiv 1 \bmod 8$.*
(iii) *$m = p$ is a prime number with $p \equiv 5 \bmod 8$, and $\epsilon^2 \not\equiv 1 \bmod 4$.*

For brevity, we write $X_K = (\mathcal{O}_K/4)^\times$ and $[E_K] = [E_K]_4$. For an integer $x \in \mathcal{O}_K$ with $(x, 2) = 1$, let $[x]$ be the class in X_K represented by x. The group $[E_K]$ is generated by the classes $[-1]$ and $[\epsilon]$. Let $\omega = \sqrt{m}$ or $(1+\sqrt{m})/2$ according to whether $m \equiv 2, 3 \bmod 4$ or $m \equiv 1 \bmod 4$. The set $\{1, \omega\}$ is a free basis of $\mathcal{O}_K$ over $\boldsymbol{Z}$. Let $M = (m-1)/4$ when $m \equiv 1 \bmod 4$. We distinguish the following three cases to show Proposition:

(I) 2 ramifies,
(II) 2 splits,
(III) 2 remains prime in K.

For the case (III), we need the following lemma (cf. Kawamoto [4, Lemma 6.6]).

Lemma 5. *In the case* (III), *we have*

$$X_K = \langle [-1] \rangle \times \langle [1+2\omega] \rangle \times \langle [M+\omega] \rangle,$$

and this is an abelian group of type (2, 2, 3).

Proof of Proposition. The case (I). In this case, X_K is an abelian group of type (2, 4). When $m = 2$, we easily see that $X_K = [E_K]$. So, let $m > 2$. Since h_K is odd, we see from genus theory that $m = q$ or $2q$, q being a prime number with $q \equiv 3 \bmod 4$. (For genus theory, see Ono [8, Chapter 4] for example.) First, let $m = q$. Since h_K is odd and the prime 2 ramifies in K, we see that $\epsilon = \pi^2/2$ for some integer $\pi = a + b\omega$ $(a, b \in \boldsymbol{Z})$ ([4, Lemma 3.1]). Clearly, we have $N(\pi) = \pm 2$, where $N(x)$ denotes the norm of $x \in K^\times$. Hence, a and b are odd. From this, we see that $\epsilon^2 = \pi^4/4 \equiv -1 \bmod 4$, and hence $[E_K]$ is a cyclic group. Therefore, we obtain $[E_K] \subsetneqq X_K$ as X_K is of type (2, 4). Next, let $m = 2q$. Since h_K is odd and the prime q ramifies in K, we have $\epsilon = \pi^2/q$ for some integer $\pi = a + b\omega \in \mathcal{O}_K$ ([4, Lemma 3.1]). We easily see that a is odd and that $\epsilon^2 \equiv \pi^4 \equiv 1 \bmod 4$. This implies $[E_K] \subsetneqq X_K$.

The case (II). In this case, X_K is an abelian group of type (2, 2). We easily see that $X_K = [E_K]$ if and only if $N(\epsilon) = -1$. As h_K is odd and the prime 2 splits in K, it follows from genus theory that $m = p$ is a prime number with $p \equiv 1 \bmod 8$, or $m = q_1 q_2$ for some prime numbers q_i satisfying $q_1 \equiv 3 \bmod 4$ and $q_1 \equiv q_2 \bmod 8$. It is known that $N(\epsilon) = -1$ in the former case and $N(\epsilon) = 1$ in the latter case ([8, Theorem 4.5]). The assertion follows from this in this case.

The case (III). As h_K is odd and the prime 2 remains prime in K, it follows from genus theory that $m = p$ is a prime number with $p \equiv 5 \bmod 8$, or $m = q_1 q_2$ for some prime numbers q_i satisfying $q_1 \equiv q_2 \equiv 3 \bmod 4$ and $q_1 \not\equiv q_2 \bmod 8$. We may as well assume that $\epsilon > 1$. First, let $m = p$. Then, by [4, Lemma 3.3 (iv)], we have

$$[\epsilon] = [1+2\omega],\ [-M+\omega] \ \text{ or } \ [M-1+\omega].$$

As is easily seen, we have

$$[-M+\omega] = [1+2\omega][M+\omega]$$

and

$$[M-1+\omega] = [1+2\omega][M+\omega]^2.$$

Then, we see from Lemma 5 that $X_K = [E_K]$ if and only if $\epsilon^2 \not\equiv 1 \bmod 4$. Next, let $m = q_1 q_2$. By [4, Lemma 3.3 (iii)], we have

$$[\epsilon] = [-1],\ [M+1+\omega] \ \text{ or } \ [-M-\omega].$$

Noting that $[M+1+\omega] = [-1][M+\omega]^2$, we see from Lemma 5 that $[E_K] \subsetneqq X_K$. $\square$

Acknowledgements. The first 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.

References

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

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

[3] Ichimura, H.: Note on the ring of integers of a Kummer extension of prime degree, V. Proc. Japan Acad., **78A**, 76–79 (2002).

[4] Kawamoto, F.: On quadratic subextensions of ray class fields of quadratic fields mod $\mathfrak{p}$. J. Number Theory, **86**, 1–38 (2001).

[5] Kawamoto, F.: Normal integral bases and strict ray class groups modulo 4. J. Number Theory, **101**, 131–137 (2003).

[6] Kawamoto, F., and Odai, Y.: Normal integral bases of ∞-ramified abelian extensions of totally real number fields. Abh. Math. Sem. Univ. Hamburg, **72**, 217–233 (2002).

[7] Massy, R.: Bases normales d'entiers relatives quadratiques. J. Number Theory, **38**, 216–239 (1991).

[8] Ono, T.: An Introduction to Algebraic Number Theory. Plenum Press, New York-London (1990).