A note on unramified quadratic extensions over algebraic number fields

By Humio Ichimura

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

(Communicated by Shokichi Iyanaga, M. J. A., May 12, 2000)

Abstract: We construct for each integer $n\,(\geq 3)$, infinitely many number fields of degree n each of which has an unramified quadratic extension with a power integral basis but no normal integral basis.

Key words: Unramified quadratic extension; power integral basis; normal integral basis.

1. Introduction. Let L/K be a finite extension of an algebraic number field K, and O_L (resp. O_K) the ring of integers of L (resp. K). One says that L/K has a power integral basis (PIB for short) when $O_L = O_K[\alpha]$ for some $\alpha \in O_L$. If L/K is Galois, it has a normall integral basis (NIB for short) when O_L is free of rank one over the group ring $O_K[\mathrm{Gal}(L/K)]$. Let p be a prime number. Assume that K contains a primitive p-th root ζ_p of unity and that L/K is an unramified cyclic extension of degree p. Here, L/K is "unramified" when it is unramified at all finite prime divisors. Then, it is known that L/K has a PIB if it has a NIB (see Childs [1] and the author [3]). On the other hand, the converse does not hold in general. Actually, we give in [4] some examples of real quadratic fields which has an unramified quadratic extension with PIB but no NIB. In this note, we prove that for each integer $n \geq 3$, there exist infinitely many number fields of degree n each of which has an unramified quadratic extension with PIB but no NIB. We give a more precise statement in the next section after introducing some notation.

2. Theorem. Let K be a number field and $E = E_K$ the group of units of K. We denote by $\mathcal{H}(K)$ the subgroup of $K^\times/(K^\times)^2$ consisting of classes $[\alpha]\,(\alpha \in K^\times)$ such that $K(\alpha^{1/2})/K$ is unramified (at all finite prime divisors). We put

$$\mathcal{E}(K) := \mathcal{H}(K) \cap E(K^\times)^2/(K^\times)^2,$$
$$\mathcal{N}(K) := \{[\epsilon] \in E(K^\times)^2/(K^\times)^2 \mid \epsilon \in E,\ \epsilon \equiv 1 \mod 4\}.$$

It is well known (cf. Washington [7, Exercises 9.2, 9.3]) that for a unit $\epsilon \in E$, the extension $K(\epsilon^{1/2})/K$ is unramified if and only if

$$\epsilon \equiv u^2 \mod 4 \quad \text{for some } u \in O_K.$$

Therefore, it follows that

$$\mathcal{N}(K) \subseteq \mathcal{E}(K) \subseteq \mathcal{H}(K).$$

In [1], Childs proved that for $[\alpha] \in \mathcal{H}(K)$, the unramified quadratic extension $K(\alpha^{1/2})/K$ has a NIB if and only if $[\alpha] \in \mathcal{N}(K)$. F. Kawamoto, N. Suwa and the author independently proved that for $[\alpha] \in \mathcal{H}(K)$, $K(\alpha^{1/2})/K$ has a PIB if and only if $[\alpha] \in \mathcal{E}(K)$. For a proof of this assertion, see [3]. We say that a finite extension L/K is strongly unramified when it is unramified at all prime divisors including the infinite ones. Let $\widetilde{\mathcal{H}}(K)$ be the subgroup of $\mathcal{H}(K)$ consisting of classes $[\alpha] \in \mathcal{H}(K)$ such that $K(\alpha^{1/2})/K$ is strongly unramified, and

$$\widetilde{\mathcal{E}}(K) := \mathcal{E}(K) \cap \widetilde{\mathcal{H}}(K),$$
$$\widetilde{\mathcal{N}}(K) := \mathcal{N}(K) \cap \widetilde{\mathcal{H}}(K).$$

The groups defined above are naturally regarded as vector spaces over $\mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z}$. For a vector space M over $\mathbf{F}_2$, $\dim(M)$ denotes its dimension.

We prove the following:

Theorem. *Let n, r_1 and r_2 be integers with $n = r_1 + 2r_2$ and $n \geq 3$, $r_1 \geq 1$, $r_2 \geq 1$. Then, there exist infinitely many number fields K of degree n each of which has exactly r_1 real prime divisors and satisfies the inequalities*

$$(1) \quad \begin{cases} \dim(\widetilde{\mathcal{E}}(K)/\widetilde{\mathcal{N}}(K)) \geq 1, \\ \dim(\widetilde{\mathcal{N}}(K)) \geq [r_1/2] + r_2 - 1. \end{cases}$$

Partially supported by Grant-in-Aid for Scientific Research (C) (No. 11640041), the Ministry of Education, Science, Sports and Culture of Japan.

1991 Mathematics Subject Classification. 11R33.

Here, $[x]$ denotes the largest integer not exceeding x.

Let K be a number field satisfying the conditions in the Theorem. Then, by the results in [1] and [3] recalled above, K has a strongly unramified quadratic extension with PIB but no NIB, and $[r_1/2]+r_2-1$ strongly unramified quadratic extensions with NIB which are linearly independent over K.

Remark 1. For a number field K satisfying the conditions in the Theorem, the 2–rank of the ideal class group (in the usual sense) in larger than or equal to $\delta(r_1,r_2)=[r_1/2]+r_2$. Ishida [5], the author [2] and Nakano [6, Theorem 2] already constructed infinitely many number fields of degree n for which the 2–rank of the ideal class group is larger than $\delta(r_1,r_2)$, without imposing any condition on the structure of the rings of integers of the associated unramified quadratic extensions.

Remark 2. In [4, Section 3], we have constructed infinitely many sextic fields K with $\zeta_3 \in K^\times$ each of which has an unramified cubic cyclic extension with PIB but no NIB.

3. Proof of the Theorem. We fix integers n, r_1 and r_2 with $n=r_1+2r_2$ and $n\geq 3$, $r_1\geq 1$, $r_2\geq 1$. We deal with a number field defined by a polynomial of the form

$$f(X)=\prod_{i=1}^{r_1}(X-a_i)\prod_{j=1}^{r_2}(X^2-b_jX+c_j)-2$$

for some integers a_i, b_j, c_j. We assume that these integers and $f(X)$ satisfy the following five conditions. The first two of them are as follows.

(C1) $a_i\equiv 0 \bmod 8$ $(1\leq i\leq r_1)$, $b_j\equiv c_j\equiv 4 \bmod 8$ $(1\leq j\leq r_2)$.

(C2) $f(X)$ has r_1 real roots and $2r_2$ imaginary roots.

We can choose a_i, b_j, c_j satisfying (C2) by imposing the condition:

(C3) $a_i<a_{i+1}$ with $a_{i+1}-a_i$ sufficiently large $(1\leq i\leq r_1-1)$, and $b_j^2-4c_j<0$ $(1\leq j\leq r_2)$.

We choose and fix r_1+r_2-1 prime numbers ℓ_I $(2\leq I\leq r_1)$ and ρ_J $(1\leq J\leq r_2)$ different from each other such that

$$\ell\equiv 5 \bmod 8 \quad \text{and,} \tag{2}$$

$$2n\not\equiv 1 \bmod \ell \tag{3}$$

with $\ell=\ell_I,\ \rho_J$. The last two assumptions on a_i, b_j, c_j are as follows.

(C4) For each I $(2\leq I\leq r_1)$, the following congruences hold:

$$a_I\equiv -1 \mod \ell_I,$$
$$a_i\equiv 0 \mod \ell_I\ (1\leq i\leq r_1,\ i\neq I),$$
$$b_j\equiv c_j\equiv 0 \mod \ell_I\ (1\leq j\leq r_2).$$

(C5) For each J $(1\leq J\leq r_2)$, the following congruences hold:

$$a_i\equiv 0 \mod \rho_J\ (1\leq i\leq r_1),$$
$$b_J\equiv -1 \mod \rho_J,$$
$$b_j\equiv 0 \mod \rho_J\ (1\leq j\leq r_2,\ j\neq J),$$
$$c_j\equiv 0 \mod \rho_J\ (1\leq j\leq r_2).$$

By (C1), $f(X)$ is an Eisenstein polynomial, and hence is irreducible. Let θ be a root of $f(X)$, and $K=\mathbf{Q}(\theta)$. We prove the following:

Proposition. *Under the above setting, K satisfies the conditions in the Theorem.*

It is clear from (C2) that K has exactly r_1 real primes divisors. So, we prove that K satisfies the inequalities (1) of the Theorem.

By (C1), the prime number 2 is totally ramified in K; $(2)=\mathcal{P}^n$. Further, it also follows from (C1) and $f(\theta)=0$ that

$$(\theta-a_i)=\mathcal{P} \quad \text{and} \quad (\theta^2-b_j\theta+c_j)=\mathcal{P}^2.$$

Therefore, the following $r=r_1+r_2-1$ elements are units of K:

$$\epsilon_i=\frac{\theta-a_i}{\theta-a_1}, \quad \eta_j=\frac{\theta^2-b_j\theta+c_j}{(\theta-a_1)^2}$$

with $2\leq i\leq r_1$ and $1\leq j\leq r_2$. For an element $x\in K^\times$, we say that x is totally positive and write $x\gg 0$ when x is positive at all real prime divisors. It follows from the last condition in (C3) that

$$\eta_j\gg 0\ (1\leq j\leq r_2). \tag{4}$$

It also follows from (C3) that

$$\begin{cases} \epsilon_{2k}\epsilon_{2k+1}\gg 0\,(1\leq k\leq (r_1-1)/2), \\ \qquad\qquad\qquad \cdots \text{ when } r_1 \text{ is odd}, \\ \epsilon_2\gg 0,\ \epsilon_{2k-1}\epsilon_{2k}\gg 0\ (2\leq k\leq r_1/2), \\ \qquad\qquad\qquad \cdots \text{ when } r_1 \text{ is even}. \end{cases} \tag{5}$$

This is shown as follows. Assume that r_1 is odd. Let $\theta_1,\ \theta_2,\ldots,\theta_{r_1}$ be the r_1 real roots of $f(X)$ with $\theta_i<\theta_{i+1}$. From the conditions in (C3), we see that

$$\theta_{2k}<a_{2k}<a_{2k+1}<\theta_{2k+1}\Big(1\leq k\leq \frac{r_1-1}{2}\Big).$$

Then, we easily see that $\theta-a_{2k}$ and $\theta-a_{2k+1}$ have the same signatures. The assertion (5) follows from this when r_1 is odd. When r_1 is even, it is shown in a similar way.

We see from (C1) that

$$(6) \qquad \begin{cases} \epsilon_1 \equiv 1 \mod 4, \\ \eta_j \equiv (1-2/\theta)^2 \mod 4, \\ \eta_j \not\equiv 1 \mod 4,\ \eta_j\eta_{j'} \equiv 1 \mod 4 \end{cases}$$

with $2 \le i \le r_1$ and $1 \le j,\ j' \le r_2$.

To prove the Proposition, we have to show the following:

Lemma. *A basis of the vector space E/E^2 over $\mathbf{F}_2$ of dimension $r+1 = r_1 + r_2$ is given by*

$$\{[-1],\ [\epsilon_i],\ [\eta_j] \mid 2 \le i \le r_1,\ 1 \le j \le r_2\}.$$

Proof. It suffices to show that $r+1$ elements $[-1]$, $[\epsilon_i]$, $[\eta_j]$ are linearly independent over $\mathbf{F}_2$. Assume that

$$(7) \qquad (-1)^{e_1} \prod_{i=2}^{r_1} \epsilon_i^{e_i} \prod_{j=1}^{r_2} \eta_j^{f_j} \in E^2$$

with $e_i,\ f_j \in \{0,1\}$. First, let I be an integer with $2 \le I \le r_1$, and show $e_I = 0$. By (C4), we have

$$f(X) \equiv X^n + X^{n-1} - 2 \mod \ell_I.$$

In particular, $f(1) \equiv 0 \mod \ell_I$. Further, we see from (3) that $1 \mod \ell_I$ is not a multiple root of $f(X) \mod \ell_I$. Hence, there exists a prime ideal $\mathcal{L}_I$ of K over ℓ_I which is of degree one and contains $\theta - 1$. Then, reducing the relation (7) modulo $\mathcal{L}_I$, we see that $(-1)^{e_1}2^{e_I} \mod \ell_I$ is a square in $\mathbf{F}_{\ell_I}^\times$ from (C4) and the definition of ϵ_i, η_j. Here, $\mathbf{F}_\ell = \mathbf{Z}/\ell\mathbf{Z}$ for a prime number ℓ. Therefore, we obtain $e_I = 0$ by (2) and the supplementary laws for the quadratic residue symbols. Next, we can show $f_J = 0$ $(1 \le J \le r_2)$ is a similar way using the prime number ρ_J and the condition (C5) in place of ℓ_I and (C4). Finally, we obtain $e_1 = 0$ from $(-1)^{e_1} \in E^2$ since $r_1 \ge 1$. □

Proof of the Proposition. It suffices to show that the number field K satisfies the inequalities (1) in the Theorem. First, we deal with the case where r_1 is odd. By (4), (5) and (6), the classes of the units

$$\epsilon_{2k}\epsilon_{2k+1},\ \eta_1\eta_j \quad \left(1 \le k \le \frac{r_1 - 1}{2},\ 2 \le j \le r_2\right)$$

are elements of $\widetilde{\mathcal{N}}(K)$. Then, by the Lemma, K satisfies the second inequality in (1). By (4) and (6), $[\eta_1] \in \widetilde{\mathcal{E}}(K)$. Assume that $[\eta_1] \in \mathcal{N}(K)$. This implies that $\eta_1 \equiv \delta^2 \mod 4$ for some $\delta \in E$. By the Lemma, the subgroup of E generated by the $r+1$ units -1, ϵ_i, η_j is of finite index, and the index is odd. Therefore, we obtain

$$\eta_1^e \equiv \left(\prod_{i=2}^{r_1} \epsilon_1^{e_i} \prod_{j=1}^{r_2} \eta_j^{f_j}\right)^2 \mod 4$$

for some odd integer e and some integers e_j, f_j. However, this is impossible because of (6) since e is odd. Therefore, $[\eta_1] \notin \mathcal{N}(K)$, and hence K satisfies the first inequality in (1). Thus, the assertion of the Proposition is proved when r_1 is odd. When r_1 is even, we can prove it in a similar wary. □

Proof of the Theorem. Assume that we have number fields $K_1, \ldots, K_s$ satisfying the conditions of the Theorem. Let ℓ be a prime number which splits completely in the composite $K_1 \cdots K_s$ with $\ell \ne \ell_I$ and $\ell \ne \rho_J$. Let α be an integer such that $\alpha \mod \ell$ is not a square in $\mathbf{F}_\ell^\times$. Choose integers a_i, b_j, c_j satisfying (C1), ..., (C5) and the following congruences:

$$\begin{aligned} a_i &\equiv 0 \mod \ell\ (1 \le i \le r_1), \\ b_j &\equiv c_j \equiv 0 \mod \ell\ (1 \le j \le r_2 - 1), \\ b_{r_2} &\equiv -2\alpha^{-(n-1)/2},\ c_{r_2} \equiv -\alpha \mod \ell, \\ &\qquad \cdots \text{ when } r_1 \text{ is odd,} \\ b_{r_2} &\equiv 0,\ c_{r_2} \equiv 2\alpha^{-(n-2)/2} - \alpha \mod \ell, \\ &\qquad \cdots \text{ when } r_1 \text{ is even.} \end{aligned}$$

Let θ be a root of the polynomial $f(X)$ for the above a_i, b_j, c_j, and $K_{s+1} = \mathbf{Q}(\theta)$. By the Proposition, K_{s+1} satisfies the conditions of the Theorem. We easily see that the remainder in the division of X^m by $X^2 - \alpha$ equals $\alpha^{(m-1)/2}X$ or $\alpha^{m/2}$ according as m is odd or even. From this and the above congruences, we see that

$$f(X) \equiv (X^2 - \alpha)g(X) \mod \ell$$

for some $g(X) \in \mathbf{Z}[X]$. Therefore, ℓ does not split completely in K_{s+1}, and hence $K_{s+1} \ne K_1, \ldots, K_s$. □

References

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

[2] Ichimura, H.: On 2–rank of the ideal class groups of totally real number fields. Proc. Japan Acad., **58A**, 329–332 (1982).

[3] Ichimura, H.: On power integral bases of unramified cyclic extensions of prime degree (1999) (preprint).

[4] Ichimura, H.: A note on integral bases of unramified cyclic extensions of prime degree (1999) (preprint).

[5] Ishida, M.: On 2–rank of the ideal class groups of algebraic number fields. J. Reine Angew. Math., **273**, 165–169 (1975).

[6] Nakano, S.: On the ideal class groups of algebraic number fields. J. Reine Angew. Math., **358**, 61–75 (1985).

[7] Washington, L.: Introduction to Cyclotomic Fields. 2nd ed., Springer, Berlin-Heidelberg-New York (1996).