On integral bases of real octic 2-elementary abelian extensions (Algebraic Number Theory and Related Topics)

Author(s)
PARK, Kyoung Ho; NAKAHARA, Toru; MOTODA, Yasuo

Citation
数理解析研究所講究録 (2006), 1521: 176-184

Issue Date
2006-10

URL
http://hdl.handle.net/2433/58782

Type
Departmental Bulletin Paper

Textversion
publisher

Kyoto University
On integral bases of real octic 2-elementary abelian extensions
(実8次2-基本アーベル拡大体の整数基について)

Graduate school of Science and Engineering,
Saga University

Faculty of Science and Engineering,
Saga University

Faculty of General Education,
Yatsushiro National College of Technology

Abstract. Let $K$ be an abelian field whose Galois group is 2-elementary abelian over the rationals $Q$. If an octic field $K$ is monogenic and a quadratic subfield with odd discriminant and a quartic subfield of $K$ are linearly disjoint, then $K$ coincides with the field $Q(\sqrt{-1}, \sqrt{2}, \sqrt{-3})$, namely $K$ is equal to the cyclotomic field $Q(\zeta_{24})$ [MN]. In this article, we explain how to prove that all the real octic fields $K$ are non-monomogenic, that is, the rings $Z_{K}$ of integers in $K$ do not have any power integral basis. Finally, we propose a few problems on the evaluation on the field index of $K$ and the non-essential factor (außerwesentliche Diskriminanteil) of $K$.

§1. Introduction

Let $K$ be an algebraic number field over the rationals $Q$. We denote the ring of integers in $K$ by $Z_{K}$. When $Z_{K} = Z[\alpha]$ for some element $\alpha$ of $Z_{K}$, it is said that $\alpha$ generates a power integral basis of the ring $Z_{K}$ or simply $Z_{K}$ has a power integral basis. The field $K$ is called monogenic if $Z_{K}$ has a power integral basis. It is known as a problem of Hasse to characterize whether a field $K$ is monogenic or not[1]. In this article, we consider the fields $K$ whose Galois groups are 2-elementary abelian. Since the field $K$ for $[K : Q] \geq 16$

AMS subject classification: Primary: 11R04.

1) Partially supported by grant (116540029) from the Japan Society for the Promotion of Science.
On integral bases of real octic 2-elementary abelian extensions

is non-monogenic, i.e., the ring $Z_K$ of integers in $K$ has no power integral basis by virtue of the decomposition theory of a prime number ([Lemma 1, SN], [MNS], [Wa]) and by the works of K. S. Williams, M.-N. Gras and F. Tanoé for Dirichlet fields $K,([Wi], [GT])$ it is enough for us to investigate the octic 2-elementary abelian fields. Let $k$ and $L$ be a quadratic subfield of odd discriminant and a quartic subfield of $K$, respectively. If $k$ and $L$ are linearly disjoint, then such an octic field $K = kL$ is non-monogenic except for the cyclotomic field $Q(\zeta_{24})$ of conductor 24 [MN]. In this paper, we will show an integral basis of the ring $Z_K$ over the ring $Z$ of rational integers in an octic field $K$ [Theorem 1]. Next, being based on the linear equations

$$a_1 E_{1i} + a_2 E_{2i} + a_3 E_{3i} = 0 \quad (1 \leq i \leq 7)$$

with suitable factors $a_{ij}$ of the field discriminant $D_K$, where $(a_{ij}, D_i) = 1$ and units $E_{ij}$ as coefficients of valuables $a_{ij}$ in each quadratic subfield $k_j = Q(\sqrt{D_j})$ [Proposition 2], we can prove that all the real 2-elementary abelian fields $K$ of degree 8 have no power integral basis [Theorem 2].

§2. Integral bases

We determine explicit integral bases of some octic fields $K$ whose Galois groups are 2-elementary abelian. We denote the Galois group

$$\langle \tau, \sigma, \rho \mid \tau: \sqrt{mn} \mapsto -\sqrt{mn}, \sigma: \sqrt{dn} \mapsto -\sqrt{dn}, \rho: \sqrt{d_1m_1n_1\ell} \mapsto -\sqrt{d_1m_1n_1\ell} \rangle$$

of $K/Q$ by $G$.

The following lemma and proposition are available to deduce the type of 2-elementary abelian extension fields $K$ which would have power integral bases.

Lemma 1([SN]). Let $\ell$ be a prime number and let $F/Q$ be a Galois extension of degree $n = efg$ with ramification index $e$ and the relative degree $f$ with respect to $\ell$. If one of the following conditions is satisfied, then $Z_F$ has no power integral basis, i.e., $F$ is non-monogenic;

1. $ef\ell < n$ if $f = 1$;
   
   or

2. $ef\ell \leq n + e - 1$ if $f \geq 2$.

Proposition 1([MN]). Let $a_1, a_2, \cdots, a_r$ be square free rational integers and $F$ be the field $Q(\sqrt{a_1}, \sqrt{a_2}, \cdots, \sqrt{a_r})$ of degree $2^r, r \geq 4$. Then $F$ is non-monogenic.

Proof. Without loss of generality, we may assume that there exists at most two generators $\sqrt{a_1}, \sqrt{a_2}$ of $F$ with $a_j \not\equiv 1 \pmod{4}(1 \leq j \leq 2)$. Then the ramification index $e$ of the prime
is at most $2^2$. Since the Galois group $G = Gal(F/Q)$ is 2-elementary, the relative degree $f$ of the prime 2 is at most 2, because the inertia subgroup of $G$ is cyclic. In Lemma 1 let $\ell$ be equal to 2. Then we can deduce $e\ell^j \leq 2^2 \cdot 2^1 < 2^r$ if $f = 1$ and $e\ell^j \leq 2^2 \cdot 2^2 \leq 2^f + e - 1$ if $f = 2$. Thus $F$ is non-monogenic.

By the proof of Proposition 1, if an octic field $K$ is monogenic, it is sufficient to consider that $K$ contains two quadratic subfields of even discriminant and one of odd discriminant.

The main theorem is based on the following theorem, which is an extension of a result of the case of quartic fields [M1, M2, Wi].

**Theorem 1** ([PMN]). Let $K$ be an octic field $Q(\sqrt{mn}, \sqrt{dn}, \sqrt{d_1m_1n_1\ell})$ with $d = d_1d_2, m = m_1m_2, n = n_1n_2, mn \equiv 3, dn \equiv 2, d_1m_1n_1\ell \equiv 1, d_2 \equiv 2 \text{ (mod 4)}, d_1, m_1, n_1 \geq 1$ and $dmn\ell$ is square free. Let $D_K$ be the field discriminant of the octic field $K$. Then we have $D_K = 2^{12}(dmn\ell)^4$ and an integral basis of $K$ is:

$$Z_K = \mathbb{Z}\left[1, \sqrt{mn}, \sqrt{dn}, \frac{\sqrt{dm} + \sqrt{dn}}{2}, \frac{1 + \sqrt{d_1m_1n_1\ell}}{2}, \frac{\sqrt{mn} + \sqrt{d_1m_2n_2\ell}}{2}, \frac{\sqrt{dn} + \sqrt{d_2m_1n_2\ell}}{2}\right]$$

where $e_i = \pm 1$ ($i = 1, 2$), $e_1 \equiv d_1m_1, e_2 \equiv d_1n_1 \text{ (mod 4)}$.

§ 3. Non-monogenic field

It is known that in the case of $d_1m_1n_1 = 1$ that is, there exist a quartic subfield $L$ and a quadratic $k$ of $K$ with $(D_L, D_k) = 1$, the fields $K$ are non-monogenic except for the cyclotomic field $Q(\zeta_{24})$ of conductor 24 [MN], where $D_F$ means the discriminant of an algebraic number field $F$ over $Q$. From now on, we consider the case of $d_1m_1n_1 \geq 1$ and as an application of Theorem 1, we can slightly generalize Proposition 5 in [MN], whose proof was done using the relative different with respect to $K$ over a suitable quadratic subfield. We assume that $K$ is monogenic.

Let

$$\xi = b_1\sqrt{mn} + b_2\sqrt{dn} + b_3\frac{\sqrt{dm} + \sqrt{dn}}{2} + b_4\frac{1 + \sqrt{d_1m_1n_1\ell}}{2} + b_5\frac{\sqrt{mn} + \sqrt{d_1m_2n_2\ell}}{2}$$

$$+ b_6\frac{\sqrt{dn} + \sqrt{d_2m_1n_2\ell}}{2} + b_7\frac{\sqrt{dm} + \sqrt{dn} + e_1\sqrt{d_2m_2n_1\ell} + e_2\sqrt{d_2m_1n_2\ell}}{4}$$

be a generator of a power integral basis of $Z_K$. Now we calculate a factor $(\xi - \xi^\sigma)(\xi - \xi^\rho)$
of the discriminant $d_{K/Q}(\xi) = \Delta^2 \left[ 1, \xi, \xi^2, \xi^3, \xi^4, \xi^5, \xi^6, \xi^7 \right]$ of a number $\xi$.

$$(\xi - \xi^\sigma)(\xi - \xi^\rho)^\rho = \left\{ (2b_2 + b_3 + b_6 + \frac{b_7}{2}) \sqrt{dn} + (b_6 + \frac{b_7e_2}{2}) \sqrt{d_2m_1n_2\ell} + b_7e_1\sqrt{d_2m_1n_2\ell} \right\} \times \left\{ (2b_2 + b_3 + b_6 + \frac{b_7}{2}) \sqrt{dm} - (b_6 + \frac{b_7e_2}{2}) \sqrt{d_2m_1n_2\ell} - b_7e_1\sqrt{d_2m_1n_2\ell} \right\}^2$$

$$= \left\{ (2b_2 + b_3 + b_6 + \frac{b_7}{2}) \sqrt{dn} + (b_6 + \frac{b_7e_2}{2}) \sqrt{d_2m_1n_2\ell} + b_7e_1\sqrt{d_2m_1n_2\ell} \right\}^2 - \left\{ (b_6 + \frac{b_7e_2}{2}) \sqrt{d_2m_1n_2\ell} + b_7e_1\sqrt{d_2m_1n_2\ell} \right\}^2$$

$$= \left\{ (2b_2 + b_3 + b_6)^2 + (2b_2b_7 + b_3b_7 + b_6b_7) + \frac{b_7^2}{4} \right\}dn^\lrcorner - \left\{ (b_3^2 + b_3b_7 + \frac{b_7^2}{4})dm - \left\{ (b_6^2 + b_6b_7\ell + \frac{b_7^2}{4})d_2m_1n_2\ell - \frac{b_7^2m_2n_1p}{4} \right\} \right\} \sqrt{mn},$$

namely, this factor is an integer of the quadratic field $k_1 = Q(\sqrt{mn})$ of the fixed field by the subgroup $< \sigma, \rho >$ in $G$. Then we denote it by $\eta_{11} = B + C(\sqrt{mn})$. Thus we obtain

$$B/d_2 \equiv \left\{ b_3^2 + b_6^2 + b_3b_7 + \frac{b_7^2}{4} \right\}d_1n + \left\{ b_3^2 + b_3b_7 + \frac{b_7^2}{4} \right\}d_1m$$

$$- \left\{ b_6^2 + b_6b_7 + \frac{b_7^2}{4} \right\}m_1n_2\ell - \frac{b_7^2m_2n_1\ell}{4}$$

$$\equiv \frac{b_7^2}{4} (d_1(m + n) - (m_1n_2 + m_2n_1)\ell)$$

$$\equiv \frac{1}{4} \left\{ d_1(m + n) - (d_1n + 4k + d_1m + 4k) \right\} \equiv 0 \pmod{2},$$

by $d_1m_1n_1\ell \equiv 1 + 4k \pmod{8}$ and $m + n \equiv 0 \pmod{4}$, since $m_1n_2\ell \cdot 1 \equiv d_1m_2n_1n_2\ell^2 + 4m_1n_2\ell k \equiv d_1n + 4k \pmod{8}$ and $m_2n_1(1) \equiv d_1m_1m_2n_1^2\ell^2 + 4m_2n_1\ell k \equiv d_1m + 4k \pmod{8}$.

$$C/d_2 \equiv (b_6b_7 + \frac{b_7^2}{2})d_1 - \left\{ b_6b_7e_1\ell + \frac{b_7^2e_2e_1\ell}{2} \right\} \equiv b_6b_7(d_1 - e_1\ell) + \frac{b_7^2}{2} (d_1 - e_2e_1\ell) \equiv 0 \pmod{2}$$

by $e_1 \equiv d_1m_1$, $e_2 \equiv d_1n_1 \pmod{4}$, since $d_1 - e_2e_1\ell \equiv d_1 - e_1\ell \equiv d_1(1-d_1m_1n_1\ell) \equiv 0 \pmod{4}$. So we can write $\eta_{11} = (\xi - \xi^\sigma)(\xi - \xi^\rho)^\rho = 2d_2E_1$ for an integer $E_1 = B_1 + C_1\sqrt{mn}$ in $k_1 = Q(\sqrt{mn})$. By the same computation, we obtain $\eta_{12} = (\xi - \xi^\sigma)(\xi - \xi^\rho)^\sigma = \ell E_2$, $\eta_{13} = (\xi - \xi^\rho)(\xi - \xi^\rho)^\rho = d_1E_3$ for units $E_j$ in $k_1(j = 2, 3)$. By the assumption that $Z_K$ is generated by $\xi$, we have

$$d_{K/Q}(\xi) = \pm N_K(\mathfrak{a}(\xi)) = \pm D_K,$$
where $d(\alpha), N_K(\alpha)$ and $N_K(a)$ means the different of a number, norm of $\alpha$ and an ideal $a$ with respect to $K/Q$, respectively [Wa]. Then, because $\eta_{1j}$ is a partial factor of $d_{K/Q}(\xi)$, the integers $E_j$ should be units in $k_1 = Q(\sqrt{m\ell})$. Here the following is our basic identity:

$$(\xi - \xi^\sigma)(\xi - \xi^\rho) - (\xi - \xi^\rho)(\xi - \xi^\sigma) = 0$$

for $(\xi - \xi^\sigma)(\xi - \xi^\rho) = \eta_{11}, (\xi - \xi^\rho)(\xi - \xi^\sigma) = \eta_{12}$ and $(\xi - \xi^\sigma)(\xi - \xi^\rho) = \eta_{13}$. Then we have the equation

$$2d_1E_1 - \ell E_2 - d_1E_3 = 0$$

in $k_1 = Q(\sqrt{D_1})$, $D_1 = m_1 \cdot 2m_2 \cdot n_1 \cdot 2n_2$, where $E_1, E_2$ and $E_3$ are units in $k_1$.

In the same way, we obtain seven equations corresponding to each of the seven quadratic subfields $k_j$ of $K$.

**Proposition 2.** If $K = Q(\sqrt{mn}, \sqrt{dn}, \sqrt{d_1m_1n_1\ell})$ is monogenic, then the following simultaneous equations hold:

1. $\ell E_{11} + 2d_2E_{12} + d_1E_{13} = 0$ in $k_1 = Q(\sqrt{D_1})$, $D_1 = m_1 \cdot 2m_2 \cdot n_1 \cdot 2n_2$, $E_{11}, E_{12}, E_{13}$ are units in the corresponding quadratic subfield $k_1$ of $K$ and $D_1$ the field discriminant of $k_1$, respectively.

2. $\ell E_{21} + 2m_2E_{22} + m_1B_{3} = 0$ in $k_2 = Q(\sqrt{D_2})$, $D_2 = d_1 \cdot 2d_2 \cdot n_1 \cdot 2n_2$, $E_{21}, E_{22}, E_{23}$ are units in the corresponding quadratic subfield $k_2$ of $K$ and $D_2$ the field discriminant of $k_2$, respectively.

3. $\ell E_{31} + 2n_2E_{32} + n_1E_{33} = 0$ in $k_3 = Q(\sqrt{D_3})$, $D_3 = d_1 \cdot 2d_2 \cdot m_1 \cdot 2m_2$, $E_{31}, E_{32}, E_{33}$ are units in the corresponding quadratic subfield $k_3$ of $K$ and $D_3$ the field discriminant of $k_3$, respectively.

4. $2d_2E_{41} + 2m_2E_{42} + 2n_2E_{43} = 0$ in $k_4 = Q(\sqrt{D_4})$, $D_4 = d_1 \cdot m_1 \cdot n_1 \cdot \ell$, $E_{41}, E_{42}, E_{43}$ are units in the corresponding quadratic subfield $k_4$ of $K$ and $D_4$ the field discriminant of $k_4$, respectively.

5. $2d_2E_{51} + m_1E_{52} + n_1E_{53} = 0$ in $k_5 = Q(\sqrt{D_5})$, $D_5 = d_1 \cdot 2d_2 \cdot n_1 \cdot \ell$, $E_{51}, E_{52}, E_{53}$ are units in the corresponding quadratic subfield $k_5$ of $K$ and $D_5$ the field discriminant of $k_5$, respectively.

6. $d_2E_{61} + 2m_2E_{62} + n_1E_{63} = 0$ in $k_6 = Q(\sqrt{D_6})$, $D_6 = 2d_2 \cdot m_1 \cdot 2n_2 \cdot \ell$, $E_{61}, E_{62}, E_{63}$ are units in the corresponding quadratic subfield $k_6$ of $K$ and $D_6$ the field discriminant of $k_6$, respectively.

7. $d_1E_{71} + m_1E_{72} + 2n_2E_{73} = 0$ in $k_7 = Q(\sqrt{D_7})$, $D_7 = 2d_2 \cdot m_2 \cdot n_1 \cdot \ell$, $E_{71}, E_{72}, E_{73}$ are units in the corresponding quadratic subfield $k_7$ of $K$ and $D_7$ the field discriminant of $k_7$, respectively.

For the case of a real quadratic field, the following lemma holds:

**Lemma 2.** Let $E_j$ be a power $\epsilon_0^j = \frac{u_j + v_j\sqrt{D}}{2}$ of the fundamental unit $\epsilon_0 = \frac{u + v\sqrt{D}}{2} > 1$ in a real quadratic field $Q(\sqrt{D})$ with the field discriminant $D$ and $\overline{\alpha} = \alpha^\gamma$ for $\alpha$ in $Q(\sqrt{D})$ and $\gamma(\neq I)$ in $Gal(Q(\sqrt{D})/Q)$. Let

$$a + bE_j + cE_k = 0,$$

$$a + b\overline{E_j} + c\overline{E_k} = 0$$

for $abc \neq 0$. Denote the matrix

$$\begin{pmatrix}
1 & E_j & E_k \\
1 & \overline{E_j} & \overline{E_k}
\end{pmatrix}$$

for $abc \neq 0$. Denote the matrix

$$\begin{pmatrix}
1 & E_j & E_k \\
1 & \overline{E_j} & \overline{E_k}
\end{pmatrix}$$

for $abc \neq 0$. Denote the matrix

$$\begin{pmatrix}
1 & E_j & E_k \\
1 & \overline{E_j} & \overline{E_k}
\end{pmatrix}$$
On integral bases of real octic 2-elementary abelian extensions

attached to the equation (*) by $A$ and the rank of $A$ by $r_D$. Then we have a solution
$(a, b, c)$ of rational integers:

$$\begin{cases}
a \pm b \pm c = 0 & \text{for } r_D = 1, \\
\frac{a}{u_k v_j - u_j v_k} = \frac{b}{2v_k} = \frac{c}{-2v_j} & \text{for } r_D = 2
\end{cases}$$

with $E_i = \frac{u_i + v_i \sqrt{D}}{2}$.

Proof. This lemma means that the integral solutions should be on the plane for the rank
$r_D = 1$ of the coefficient matrix $A$ and on the line i.e. the intersection of two planes for
$r_D = 2$, respectively.

First, we consider the case of $r_D = 1$, then for
$$\begin{cases}
E_i = \frac{u_i + v_i \sqrt{D}}{2}, \\
E_i = \frac{u_i - v_i \sqrt{D}}{2}
\end{cases}$$

$E_i, E_i$ should be a rational number. Then we have $E_j = u_j = \pm 1$ and $E_k = u_k = \pm 1$.
Hence $a \pm b \pm c = 0$. Second, we assume $r_D = 2$. Then we have

$$a : b : c = \left| \begin{array}{ccc}
E_j & E_k & \frac{1}{E_j} \\
E_j & \frac{1}{E_k} & \frac{1}{E_j}
\end{array} \right| = u_k v_j - u_j v_k : 2v_k : -2v_j.$$  

Hence

$$\frac{a}{u_k v_j - u_j v_k} = \frac{b}{2v_k} = \frac{c}{-2v_j}.$$ 

In the case of any octic field $Q(\sqrt{m_1 m_2 n_1 n_2}, \sqrt{d_1 d_2 n_1 n_2}, \sqrt{d_1 m_1 n_1 \ell})$, by the following
lemma, we can deduce to evaluate the rank $r_D$ of a quadratic field $Q(\sqrt{D})$ for a few
cases with respect to the order of values $d_1, 2d_2, m_1, 2m_2, n_1, 2n_2, \ell$ in the set of seven
parameters.

**Lemma 3.** Let denote the set $\{d_1, 2d_2, m_1, 2m_2, n_1, 2n_2, \ell\}$ by $D$. Then it holds that:

1. For one parameter $s$ in $D$, there exist only four quadratic subfields $k_j$ whose
discriminants $D_j$ are divisible by $s$.

2. For two parameters $s, t$ in $D$, there exist only two quadratic subfields $k_j$ whose
discriminants $D_j$ are divisible by $st$.

3. Let $s, t, u$ be three parameters in $D$, such that $stu$ is a divisor of the field discrimi-
nant of $D_j$ of $k_j$. Then there exists only one quadratic subfield $k_j$ whose discriminant $D_j$
is divisible by $stu$. 

\square
Proof. (1) We can confirm the claim (1) for each of \( \binom{\#D}{1} = 7 \) parameter in \( D \) from seven equations in Proposition 2, such that there exist just four fields \( k_1, k_3, k_4, k_6 \) whose discriminant is divisible by \( m_1 \).

(2) We can do the claim (2) of \( \binom{\#D}{2} = 21 \) pairs of parameters in \( D \) by the same way as in (1). For instance, there exist just two fields \( k_3, k_7 \) whose discriminants are divisible by \( d_2m_2 \).

(3) We assume that \( D_i = stua \) and \( D_j = stub \). Then we have \( D_iD_j = (stu)^2ab \). However, the quadratic subfield \( Q(\sqrt{ab}) \) does not coincide with any \( k_j(1 \leq j \leq 7) \).

Remark 1. We can confirm that the number of triplets \((s, t, u)\) within the order of parameters in \( D \) is equal to \( 28 = 7 \times 1 \times 4 \) such that each of \( stu \) is a divisor of the field discriminant \( D_j \) of \( k_j \).

Next, we prepare the key lemma for the proof of Theorem 2.

Lemma 4. For the set \( D = \{a, b, c, d, e, f, g\} \) of seven positive rational integers, assume that \( a > b \geq c > \max\{d, e, f, g\} \) and \( d > f \) or \( a > b > c \geq \max\{d, e, f, g\} \) and \( d > f \).

Then

(1) For the field \( Q(\sqrt{bcst}) \), where \( s, t \in D \setminus \{a, b, c\} \) and units \( E_i \) in \( Q(\sqrt{bcst}) \), the rank \( r_{bcst} \) of the equations

\[
\begin{align*}
&\{a + uE_j + vE_k = 0, \\
&a + u\overline{E}_j + v\overline{E}_k = 0,
\end{align*}
\]

with \( \{u, v\} = D \setminus \{a, b, c, s, t\} \) is equal to 1.

(2) For the field \( Q(\sqrt{astu}) \), where \( s, t, u \in D \setminus \{a, b, c\} \) and units \( E_i \) in \( Q(\sqrt{astu}) \), the rank \( r_{astu} \) of the equations

\[
\begin{align*}
&\{b + cE_j + vE_k = 0, \\
&b + c\overline{E}_j + v\overline{E}_k = 0,
\end{align*}
\]

with \( \{v\} = D \setminus \{a, b, c, s, t, u\} \) is equal to 1.

Sketch of Idea. Our idea for the proof of this lemma is as follows. For the quadratic subfield \( k \) including the coefficients of the simultaneous equation (*), if the field discriminant \( D_k \) is divisible by the biggest parameter (case (1)) or the second and the third ones (case (2)), since the fundamental unit (> 1) of \( k \) is relatively big, the ratios for the line in Lemma 2 would not be permitted. Thus the ranks of the coefficient matrix for both cases should be equal to one, respectively, namely any integral solution of (*) lies on the plane [PMN].
Finally, we show the following main theorem, which is a generalization of a prototype [PMN].

**Theorem 2.** Let $K = \mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_r})$ be the 2-elementary abelian extensions over $\mathbb{Q}$ whose degree $2^e$ is greater than 8 or real octic ones for square free integers $a_1, \ldots, a_r$. Then the fields $K$ are non-monogenic.

**Sketch of Proof.** By Proposition 1, it is enough to consider an octic field $K$. Let $(2) = \mathcal{L}_1 \cdots \mathcal{L}_s$ be the prime ideal decomposition of a rational prime 2 in $K$. For the ramification index of 2, if $e \leq 1$, then by Lemma 1 and the relative degree $f$ of a prime 2 is at most 2, we have $1 \cdot 2^1 < 8$ or $1 \cdot 2^2 \leq 8 + 1 - 1$ for $e = 1$ and $2 \cdot 2^2 \leq 8$ or $2 \cdot 2^2 \leq 8 + 2 - 1$ for $e = 2$, namely $K$ is non-monogenic. Then in the case of $e \geq 3$, we can deduce that the type of an octic field is $K = \mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \sqrt{a_3})$, where $a_1 = mn \equiv 3, a_2 = dn \equiv 2, a_3 = d_3m_3n_3 \ell \equiv 1 \pmod{4}$, for $d = d_1d_2, m = m_1m_2, n = n_1n_2$ and $dmn\ell$ is square free. Put $D = \{d_1, 2d_2, m_1, 2m_2, n_1, 2n_2, \ell\}$. We denote again by $\{a, b, c, d, e, f, g\}$ any transposition on the seven parameters in $D$. Without loss of generality, we may assume that $a > b > c \geq \max\{d, e, f, g\}$. Using Lemma 4, it is enough for us to consider the following two cases.

Case (I). The field $K$ includes $k_{ji} = \mathbb{Q}(\sqrt{abc})$ for some $t \in D \{a, b, c\}$, for instance, $t = d$.

Case (II). The field $K$ does not include the field $\mathbb{Q}(\sqrt{abc})$ for any $s \in D \{a, b, c\}$.

In the case (I), we can deduce that the four parameters $a, b, c, d$ with $c = d$ must lie on suitable two planes and in the case (II), $a, b, e, g$ with $e = g$ do on four planes, respectively. However, the order of the parameters would be destroyed. Then we can prove that any real octic fields $K$ does not have a power integral basis [PMN].

**Remark 2.** Recently, in [PNM] we proved that all the 2-elementary abelian fields $K$ with degree $[K : \mathbb{Q}] \geq 8$ are non-monogenic except for the field $\mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{-3}) = \mathbb{Q}(\zeta_{24})$.

**Problem.** For a primitive element $\xi$ in $K$, let $\text{Ind}(\xi)$, $\hat{m}(K)$ and $m(K)$ be the index $\sqrt{\frac{d_k(\xi)}{d_K}}$ of an element $\xi$, the minimum index $\min_{\xi \in K}\{\text{Ind}(\xi)\}$ of $K$ and the field index $\text{gcd}(\text{Ind}(\xi))$ of $K$, respectively. Let the fields $K$ run through all the real octic fields whose Galois groups are 2-elementary abelian. Then evaluate the values of

$$\inf_K \hat{m}(K) \text{ and } \inf_K m(K),$$
Acknowledgement. We wish to express our gratitude to Prof. Y. Taguchi and M. Ozaki for their valuable comments on this article.

References


