Bull. Math. Soc. Sci. Math. Roumanie
Tome 58(106) No. 4, 2015, 419–433

Integral bases and relative monogenity of pure octic fields

by
(1) Abdul Hameed and (2) Toru Nakahara

Abstract

Let $m \neq 1$ be a square-free integer. The aim of this paper is to construct an integral basis of the pure octic field $L = \mathbb{Q}(\sqrt[8]{m})$ and to consider relative monogenity of L over its quartic subfield $K = \mathbb{Q}(\sqrt[4]{m})$ as well as over its quadratic subfield $k = \mathbb{Q}(\sqrt[2]{m})$. We prove that the field L is relatively monogenic over k for the case of $m \equiv 5, 13 \pmod{16}$ and does not have relative power integral basis over k for $m \equiv 1, 9 \pmod{16}$. Moreover we prove that L has a relative power integral basis over K in the case of $m \equiv 5, 9, 13 \pmod{16}$. We show that the field $\mathbb{Q}(\sqrt[8]{m})$ is monogenic as well as relatively monogenic over k and K when $m \equiv 2, 3 \pmod 4$. In the case of $m = -1$ we prove our results by observing that the field L coincides with the 16th cyclotomic field k_{16}.

Key Words: Pure octic field, integral basis, relative norm, power integral basis, monogenity.
2010 Mathematics Subject Classification: Primary 11R04, Secondary 11R16, 11R21.

1 Introduction

Let F be a number field over the field $\mathbb{Q}$ of rational numbers. We denote the ring of integers of F by $\mathbb{Z}_F$. For a finite field extension F/K of degree n, it is said that an element $\eta \in \mathbb{Z}_F$ generates a relative power integral basis $1, \eta, , \eta^2, \cdots, \eta^{n-1}$ for F over K if $\mathbb{Z}_F = \mathbb{Z}_K[\eta] = \mathbb{Z}_K 1 + \mathbb{Z}_K \eta + \cdots + \mathbb{Z}_K \eta^{n-1}$ is of rank n. For $K = \mathbb{Q}$, an element $\eta \in \mathbb{Z}_F$ generates power integral basis if $\mathbb{Z}_F = \mathbb{Z}[\eta]$. When a field F has a power integral basis over K, the field F is said to be relatively monogenic over K. In the case of $K = \mathbb{Q}$, we say that $\mathbb{Z}_F$ has a power integral basis or equivalently F is monogenic. The existence of power integral bases in algebraic number fields is a classical problem in algebraic number theory [4, 6, 11]. It is especially delicate in the case of relative extensions when the existence of a relative integral basis is not guaranteed.

For a finite extension field $F/\mathbb{Q}$ of degree n, d_F and $d_F(\alpha_1, \alpha_2 \cdots, \alpha_n)$ with $\alpha_j \in \mathbb{Z}_F$ $(1 \leqq j \leqq n)$ denote the field discriminant of F and the discriminant of the numbers $\alpha_1, \cdots, \alpha_n$ with respect to the extension $F/\mathbb{Q}$, respectively.
If $\alpha_j = \alpha^{j-1}$ for a number $\alpha \in F$, we denote $d_F(\alpha_1, \cdots, \alpha_n)$ by $d_F(\alpha)$, which is called the discriminant of α. We denote the module index $(\mathbb{Z}_F : \mathbb{Z}[\alpha])$ of a submodule $\mathbb{Z}[\alpha]$ in the module $\mathbb{Z}_F$ by $\text{ind}_F(\alpha)$, which is a positive integer given by $d_F(\alpha) = (\text{ind}_F(\alpha))^2 d_F$ [11].

Let L be a pure octic field $\mathbb{Q}(\sqrt[8]{m})$ and $\mathbb{Z}_L$ the ring of integers in L. The purpose of this paper is to construct an integral basis of $\mathbb{Z}_L$ over $\mathbb{Q}$ and relative integral bases of Z_L over the quadratic and quartic subfields. We work in the relative extension L/K and consider the relative trace $T_{L/K}(\eta)$ and the relative norm $N_{L/K}(\eta)$ of an algebraic integer $\eta \in \mathbb{Z}_L$ with respect to a relative extension L/K. To determine the unknown coefficients α, β in K with $\eta = \alpha + \beta\theta$ we use the fact that $T_{L/K}(\eta)$ and $N_{L/K}(\eta)$ are algebraic integers in the subfield K.

On the determination of integral or relative integral bases for Galois and specifically abelian extensions with degree 3 or 4, there are many works [2, 9, 10, 12, 13], but for non Galois extensions with degree greater than or equal to 4, there are a few works [3, 5].

2 Integral Bases of Pure Octic Fields

In this section, we construct an integral basis for the pure octic field $L = \mathbb{Q}(\sqrt[8]{m})$. For $m = -1$ the field $L = \mathbb{Q}(\sqrt[8]{-1})$ coincides with the 16th cyclotomic field k_{16}. Let ζ_{16} be a primitive 16th root of unity. Then it is known that $k_{16} = \mathbb{Q}(\sqrt[8]{-1})$ and each of its maximal real subfield $k_{16}^+ = \mathbb{Q}(\zeta_{16} + \zeta_{16}^{-1})$, the 8th cyclotomic field $k_8 = \mathbb{Q}(\zeta_{16}^2)$, $k_8^+ = \mathbb{Q}(\zeta_8^2 + \zeta_8^{-2})$, $k_8^- = \mathbb{Q}(\zeta_8^2 - \zeta_8^{-2})$ and $k_4 = \mathbb{Q}(\zeta_{16}^4) = \mathbb{Q}(i)$ are monogenic [14]. The subfield structure of $k_{16} = \mathbb{Q}(\sqrt[8]{-1})$ and the corresponding Galois groups are shown in Figure 1.

Subfield Structure of $L = \mathbb{Q}(\sqrt[8]{-1})$

The actions of the two automorphisms are ${\zeta_{16}}^{\tau} = \zeta_{16}^3$ and ${\zeta_{16}}^{\rho} = \zeta_{16}^{-1}$. Then $G =< \tau, \rho : \tau^4 = \rho^2 = 1, \tau\rho = \rho\tau >$ the Galois group of k_{16} is the direct product of $\mathbb{Z}_4$ by $\mathbb{Z}_2$. In general, for $h = 2^{n+1}$ with $n \geqq 2$ the Galois group of the cyclotomic field $\mathbb{Q}(\zeta_h)$ is the direct product

$$\mathbb{Z}_{2^{n-1}} \times \mathbb{Z}_2 =< \tau, \rho : \tau^{2^{n-1}} = \rho^2 = 1, \tau\rho = \rho\tau >$$

with τ and ρ having the same action as above. Here ${\zeta_h}^{\tau} = \zeta_h^3$ gives
${\zeta_h}^{\tau^{2^{n-1}}} = \zeta_h$, because $3^{2^{n-1}} \equiv 1 \pmod{2^{n+1}}$.

For $m = 2$, the pure octic field $\mathbb{Q}(\sqrt[8]{m})$ coincides with the maximal real subfield $k_{32}^+ = \mathbb{Q}(\zeta_{32} + \zeta_{32}^{-1})$ and is monogenic by Proposition 2.16 of [14]. For $m = -2$, the field coincides with the maximal imaginary subfield $k_{32}^- = \mathbb{Q}(\zeta_{32} - \zeta_{32}^{-1})$ whose monogenity is proved in the next lemma.

Lemma 1. *Let $h = 2^{n+1}$ with $n \geqq 2$. Put $\eta = \zeta_h - \zeta_h^{-1}$ with $\zeta_h = e^{\frac{2\pi i}{h}}$. Then the maximal imaginary subfield $k_h^- = \mathbb{Q}(\zeta_h - \zeta_h^{-1})$ is monogenic.*

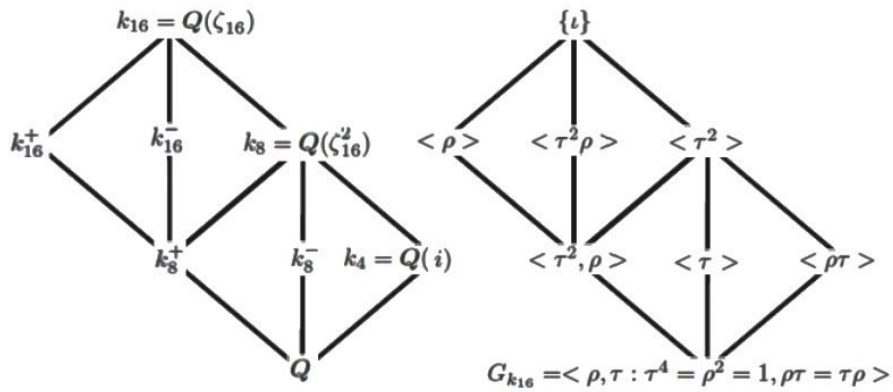

Figure 1:

Proof: By $\eta^{\tau^{(\frac{h}{2^3})}\rho} = (\zeta_h^{\tau^{\frac{h}{2^3}}} - \zeta_h^{-\tau^{\frac{h}{2^3}}})^{\rho} = (-\zeta_h + \zeta_h^{-1})^{\rho} = \zeta_h - \zeta_h^{-1} = \eta, \mathbb{Q}(\eta)$ coincides with the fixed field k_h^- of the subgroup $<\tau^{\frac{h}{4}}\rho>$ of $G(k_h/\mathbb{Q})$ for $n \geqq 3$ and of $<\tau>$ of $G(k_8/\mathbb{Q})$ for $n = 2$. Since $\eta^2 = \zeta_h^2 - 2 + \zeta_h^{-2}, \cdots$ and $\eta^{2^n-1} = \zeta_h^{2^n-1} - \cdots - \zeta_h^{-(2^n-1)}$ hold, we have $\mathbb{Z}[1, \eta, \cdots, \eta^{\frac{h}{2}-1}] \subseteqq Z_{k_h^-}$. If there exists an integer $\alpha \in Z_{k_h^-} \backslash \mathbb{Z}[\eta]$, with $a_\ell \in \mathbb{Q} \backslash \mathbb{Z}$ and $a_j \in \mathbb{Z}$ for $j \geqq \ell + 1$ such that $\alpha = a_0 + \cdots + a_\ell \eta^\ell + a_{\ell+1}\eta^{\ell+1} + \cdots + a_{\frac{h}{2}-1}\eta^{\frac{h}{2}-1}$, then
$\beta = \alpha - (a_{\ell+1}\eta^{\ell+1} + \cdots + a_{\frac{h}{2}-1}\eta^{\frac{h}{2}-1}) \in Z_{k_h^-} \subset Z_{k_h}$. However the coefficient a_ℓ of ζ_h^ℓ $(0 \leqq \ell \leqq \frac{h}{2} - 1)$ is not a rational integer, which contradicts that $\beta \in Z_{k_h}$ $= \mathbb{Z}[\zeta_h^{-(\frac{h}{2}-1)}, \cdots, 1, \cdots, \zeta_h^{\frac{h}{2}-1}]$. □

For $m \neq \pm 1, \pm 2$, the Galois closure of $L = \tilde{L} = L(\zeta_8) = \mathbb{Q}(\sqrt[8]{m}, \zeta_8)$ has degree 32. Let G be the corresponding Galois group $G(\tilde{L}/\mathbb{Q})$ of $\tilde{L}$ over $\mathbb{Q}$. Then G is generated by three automorphisms σ, ρ and τ. The actions of the automorphisms on θ and ζ_8 are shown in Table 1.

	θ	ζ_8
σ	$\theta\zeta_8$	ζ_8
τ	θ	ζ_8^3
ρ	θ	ζ_8^{-1}

Table 1: Action of Automorphisms of G on θ and ζ_8

Thus $G =<\sigma, \tau, \rho : \sigma^8 = \tau^2 = \rho^2 = (\sigma\tau)^2 = (\sigma\rho)^2 = (\tau\rho)^2 = \iota>$ with the identity map ι of $\tilde{L}$. In Figure 2, we identify an isomorphism $\rho \in G$ and its restriction map $\rho \mid F$ to any subfield F of $\tilde{L}$. Then the structure of the subfields F of $\tilde{L}$ and the corresponding subgroups H_F of G for a square-free integer $m \neq \pm 1, \pm 2$ is depicted in Figure 2.

The Galois Structure of a Pure Octic Field $L = \mathbb{Q}(\sqrt[8]{m})$ for $m \neq \pm 1, \pm 2$.

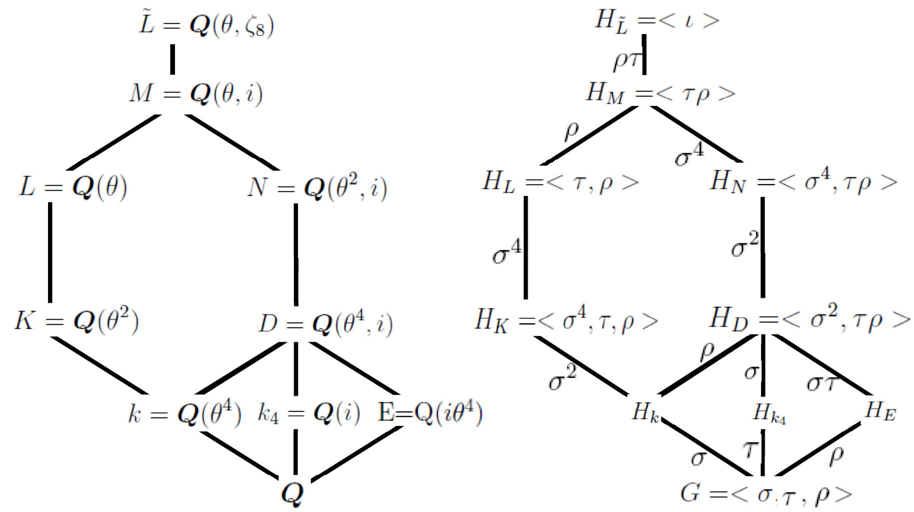

Figure 2:

For $m \equiv 2, 3 \pmod 4$, since the defining polynomials $f(x) = x^8 - m$ for $m \equiv 2 \pmod 4$ and $f(x+1) = (x+1)^8 - m$ for $m \equiv 3 \pmod 4$ are of Eisenstein type with respect to a prime number 2, by [7] the field L has a power integral basis generated by $\theta = \sqrt[8]{m}$, i.e $\mathbb{Z}_L = \mathbb{Z}[\theta]$.
Our main result is based on the description of an explicit integral basis for a pure quartic field given by T. Funakura [3].

Lemma 2. [3] *For an eighth root $\theta = \sqrt[8]{m}$ of a square free integer $m \neq 1$, let K be the pure quartic field $\mathbb{Q}(\theta^2)$ and k the quadratic subfield $\mathbb{Q}(\omega)$ with $\omega = (1+\theta^4)/2$ if $m \equiv 1 \pmod 4$, and $\omega = \theta^4$ otherwise. Let $\mathbb{Z}_K$ and $\mathbb{Z}_k$ be the ring of integers in K and k, respectively. Then we have*

$$\mathbb{Z}_K = \begin{cases} \mathbb{Z}[1, \theta^2, \theta^4, \theta^6] = \mathbb{Z}_k[\theta^2] & \text{if } \ m \equiv 2, 3 \pmod 4, \\ \mathbb{Z}[1, \omega, \theta^2, \omega\theta^2] = \mathbb{Z}_k[\theta^2] & \text{if } \ m \equiv 5, 13 \pmod{16}, \\ \mathbb{Z}[1, \omega, \theta^2, \omega\frac{1+\theta^2}{2}] & \text{if } \ m \equiv 1, 9 \pmod{16} \end{cases}$$

and hence

$$d_K = \begin{cases} -2^8 m^3 = -2^2 \cdot d_k^3 & \text{if } \ m \equiv 2, 3 \pmod 4, \\ -2^4 m^3 = -2^4 \cdot d_k^3 & \text{if } \ m \equiv 5, 13 \pmod{16}, \\ -2^2 m^3 = -2^2 \cdot d_k^3 & \text{if } \ m \equiv 1, 9 \pmod{16}. \end{cases}$$

In the case $m \equiv 1 \pmod 4$, the following lemma is indispensable in constructing an integral basis.

Lemma 3. *Let $\eta = \alpha + \beta\theta$ be any integer in L with $\alpha, \beta \in K$. Then 2α and 2β are integers in K, namely* $\mathrm{ind}_K(\eta) = 1$ *or* 2.

Proof: For any integer η in the field L, there exist numbers α and β in K such that $\eta = \alpha + \beta\theta$. Since η is an integer in L, the relative trace $T_{L/K}(\eta) = \eta + \eta^{\sigma^4} = 2\alpha$ of η and its relative norm $N_{L/K}(\eta) = \eta\eta^{\sigma^4} = \alpha^2 - \beta^2\theta^2$ are integers in K. Thus $2\alpha \in \mathbb{Z}_K$. Taking norms on both sides of $2\eta = 2\alpha + 2\beta\theta$ with respect to L/K, we have $4N_{L/K}(\eta) = (2\alpha)^2 - (2\beta)^2\theta^2 \in \mathbb{Z}_K$ and hence $(2\beta)^2\theta^2 \in \mathbb{Z}_K$ holds. In the ideal decomposition $\mathfrak{A}/\mathfrak{B}$ of the principal ideal (2β) with $(\mathfrak{A}, \mathfrak{B}) = 1$, assume that $\mathfrak{B} \ncong 1$. Then there exists a prime factor $\mathfrak{P}$ of $\mathfrak{B}$. Since the principal ideal $(2\beta)^2\theta^2$ is integral, then θ^2 is divisible by $\mathfrak{P}^2$, namely $\theta^2 = \mathfrak{P}^2\mathfrak{C}$ holds for an ideal $\mathfrak{C}$. Taking the ideal norm of both sides with respect to $K/\mathbb{Q}$, it follows that

$$m = \theta^2(\zeta_8^2\theta)^2(\zeta_8^4\theta)^2(\zeta_8^6\theta)^2 = \theta^2(\theta^2)^{\sigma^2}(\theta^2)^{\sigma^4}(\theta^2)^{\sigma^6} = (\mathrm{N}_K\mathfrak{P})^2\mathrm{N}_K\mathfrak{C} = (p^{ef})^2\mathrm{N}_K\mathfrak{C},$$

where $\mathrm{N}_K(\cdot)$ means the norm of an ideal from K to $\mathbb{Q}$, and e and f denote the ramification index and the residue class degree of $\mathfrak{P}$ in $K/\mathbb{Q}$, respectively. Since $ef \geqq 1$, m is divisible by p^2, which contradicts that m is square-free. Thus $2\beta \in Z_K$ holds. □

Then we have our main result as follows;

Theorem 1. *For an eighth root $\theta = \sqrt[8]{m}$ of a square-free integer $m \neq 1$, let L be the pure octic field $\mathbb{Q}(\sqrt[8]{m})$ and $\mathbb{Z}_L$ its ring of integers. Then we have*

$$\mathbb{Z}_L = \begin{cases} \mathbb{Z}[\theta] = \mathbb{Z}_K[\theta] = \mathbb{Z}_k[\theta^2][\theta] & if\ m \equiv 2, 3 \,(\mathrm{mod}\ 4), \\ \mathbb{Z}[1, \omega, \theta^2, \omega\theta^2, \theta, \omega\theta, \theta^3, \omega\theta^3] & if\ m \equiv 5, 13 \,(\mathrm{mod}\ 16), \\ \mathbb{Z}[1, \omega, \theta^2, \omega\frac{1+\theta^2}{2}, \theta, \omega\theta, \theta^3, \omega\frac{\theta+\theta^3}{2}] & if\ m \equiv 9 \,(\mathrm{mod}\ 16), \\ \mathbb{Z}[1, \omega, \theta^2, \omega\frac{1+\theta^2}{2}, \theta, \omega\theta, \theta^3, \omega\frac{1+\theta^2}{2}\frac{1+\theta}{2}] & if\ m \equiv 1 \,(\mathrm{mod}\ 16), \end{cases}$$

and hence

$$d_L = \begin{cases} -2^{24}m^7 = -2^8 \cdot d_k \cdot d_K^2 & if\ m \equiv 2, 3 \,(\mathrm{mod}\ 4), \\ -2^{16}m^7 = -2^8 \cdot d_k \cdot d_K^2 & if\ m \equiv 5, 13 \,(\mathrm{mod}\ 16), \\ -2^{12}m^7 = -2^8 \cdot d_k \cdot d_K^2 & if\ m \equiv 9 \,(\mathrm{mod}\ 16), \\ -2^{10}m^7 = -2^6 \cdot d_k \cdot d_K^2 & if\ m \equiv 1 \,(\mathrm{mod}\ 16). \end{cases}$$

Proof: When $m \equiv 2, 3 \,(\mathrm{mod}\ 4)$ we have already proved the monogenity.

Next we consider the case when $m \equiv 5, 13 \,(\mathrm{mod}\ 16)$.

For an integer $\eta = \alpha' + \beta'\theta \in \mathbb{Z}_L$ with $\alpha', \beta' \in K$, we have the relative norm $4\mathrm{N}_{L/K}(\eta) = \alpha^2 - \beta^2\theta^2 \equiv 0 \,(\mathrm{mod}\ 4)$ with $2\eta = \alpha + \beta\theta$. Using $\alpha = \alpha_0 + \alpha_1\theta^2$ and $\beta = \beta_0 + \beta_1\theta^2$ with $\alpha_j, \beta_j \in \mathbb{Z}_k (j = 0, 1)$, we obtain

$$\alpha^2 - \beta^2\theta^2 = (\alpha_0 + \alpha_1\theta^2)^2 - (\beta_0 + \beta_1\theta^2)^2\theta^2$$

$$\equiv \alpha_0^2 + \alpha_1^2\theta^4 + 2\alpha_0\alpha_1\theta^2 - (\beta_0^2 + \beta_1^2\theta^4 + 2\beta_0\beta_1\theta^2)\theta^2 \equiv 0 \,(\mathrm{mod}\ 4\mathbb{Z}_K). \qquad (2.1)$$

Reducing modulo 2, we deduce

$$\alpha^2 - \beta^2\theta^2 \equiv \alpha_0^2 + \alpha_1^2\theta^4 - (\beta_0^2 + \beta_1^2\theta^4)\theta^2 \equiv 0 \,(\mathrm{mod}\ 2\mathbb{Z}_K). \qquad (2.2)$$

As $(m-1)/4 \equiv 1 \pmod 2$ the following congruences hold modulo $2\mathbb{Z}_K$, namely $\theta^4 = 2\omega - 1 \equiv 1$ and $\omega^2 = \omega + (m-1)/4 \equiv \omega + 1$. Therefore, relation (2.2) gives

$$\alpha^2 - \beta^2\theta^2 \equiv \alpha_0^2 + \alpha_1^2 + (\beta_0^2 + \beta_1^2)\theta^2 \equiv 0 \pmod{2\mathbb{Z}_K}. \tag{2.3}$$

Using $\alpha_j = a_{j0} + a_{j1}\omega$ and $\beta_j = b_{j0} + b_{j1}\omega$ with $a_{ij}, b_{ij} \in \mathbb{Z}$ $(0 \leqq i, j \leqq 1)$ together with the fact that $x^2 \equiv x \pmod 2$ for all $x \in \mathbb{Z}$ we have
$\alpha^2 - \beta^2\theta^2 \equiv (a_{00} + a_{10} + a_{01} + a_{11}) + (a_{01} + a_{11})\omega + (b_{00} + b_{10} + b_{01} + b_{11})\theta^2$ $+ (b_{01} + b_{11})\omega\theta^2 \equiv 0 \pmod{2\mathbb{Z}_K}$.
Since the set $\{1, \omega, \theta^2, \omega\theta^2\}$ is an integral basis of K, the coefficients of $1, \omega, \theta^2, \omega\theta^2$ are congruent to 0 modulo 2, namely

$$a_{00} + a_{10} + a_{01} + a_{11} \equiv 0 \pmod 2,\ a_{01} + a_{11} \equiv 0 \pmod 2,$$
$$b_{00} + b_{10} + b_{01} + b_{11} \equiv 0 \pmod 2 \text{ and } b_{01} + b_{11} \equiv 0 \pmod 2.$$

Then we have

$$a_{01} \equiv a_{11}, b_{01} \equiv b_{11} \pmod 2 \text{ and } a_{00} \equiv a_{10}, b_{00} \equiv b_{10} \pmod 2. \tag{2.4}$$

Thereby

$$a_{01}^2 \equiv a_{11}^2, b_{01}^2 \equiv b_{11}^2, a_{00}^2 \equiv a_{10}^2 \text{ and } b_{00}^2 \equiv b_{10}^2 \pmod 4, \tag{2.5}$$

and

$$2a_{00}a_{01} \equiv 2a_{10}a_{11} \text{ and } 2b_{00}b_{01} \equiv 2b_{10}b_{11} \pmod 4. \tag{2.6}$$

Substituting (2.5) and (2.6) into (2.1) we obtain
$\alpha^2 - \beta^2\theta^2 \equiv 2(a_{00}^2 + a_{01}^2\omega^2)\omega$
$+2(b_{00}^2 + b_{01}^2\omega^2) + \{2(a_{00}^2 + a_{01}^2\omega^2) - 2(b_{00}^2 + b_{01}^2\omega^2)\omega\}\theta^2 \equiv 0 \pmod{4\mathbb{Z}_K}$.
Since $\{1, \theta^2\}$ is a relative integral basis of $\mathbb{Z}_K$ over $\mathbb{Z}_k$, the coefficients of 1 and θ^2 in the above relation are congruent to 0 modulo 4. The coefficient of 1 gives $2(a_{00}^2 + a_{01}^2\omega^2)\omega + 2(b_{00}^2 + b_{01}^2\omega^2) \equiv 0 \pmod 4$, which implies that
$a_{00}\omega + a_{01}(\omega^2 + \omega) + b_{00} + b_{01}(\omega + 1) \equiv 0 \pmod 2$. Thus

$$a_{01} + b_{00} + b_{01} + (a_{00} + b_{01})\omega \equiv 0 \pmod 2. \tag{2.7}$$

The coefficient of θ^2 gives $2(a_{00}^2 + a_{01}^2\omega^2) + 2(b_{00}^2 - b_{01}^2\omega^2)\omega$
$\equiv 2(a_{00} + a_{01}(\omega + 1)) + 2(b_{00}\omega + b_{01}) \equiv 0 \pmod 4$,
from this, we obtain

$$a_{00} + a_{01} + b_{01} + (a_{01} + b_{00})\omega \equiv 0 \pmod 2. \tag{2.8}$$

Since $1, \omega$ are linearly independent over $\mathbb{Z}_k$, it follows from (2.7) and (2.8) that

$$a_{01} + b_{00} + b_{01} \equiv 0 \pmod 2, \quad a_{00} + b_{01} \equiv 0 \pmod 2,$$
$$a_{00} + a_{01} + b_{01} \equiv 0 \pmod 2 \quad \text{and} \quad a_{01} + b_{00} \equiv 0 \pmod 2.$$

From these congruences we deduce $a_{01} \equiv 0 \equiv b_{01} \pmod 2$ and hence $b_{00} \equiv 0 \equiv a_{00} \pmod 2$. Together with the congruences in (2.4) we conclude that all the coefficients a_{ij}, b_{ij} $(0 \leqq i, j \leqq 1)$ are even and hence $\eta = \alpha' + \beta'\theta$ is an integer, so that $\mathbb{Z}_L \subsetneqq \mathbb{Z}_K[\theta]$.

Conversely, since ω and θ are integers in L, $\mathbb{Z}_K[\theta] = \mathbb{Z}[1, \omega, \theta^2, \omega\theta^2][1, \theta] \subsetneqq \mathbb{Z}_L$ holds. Thus we obtain $\mathbb{Z}_L = \mathbb{Z}[1, \omega, \theta^2, \omega\theta^2, \theta, \omega\theta, \theta^3, \omega\theta^3]$ as asserted.
We now determine d_L. Let A be the representation matrix of ${}^t(1, \theta, \theta^2, \theta^3, \theta^4, \theta^5, \theta^6, \theta^7)$ with respect to an integral basis ${}^t(1, \theta, \theta^2, \theta^3, \omega, \omega\theta, \omega\theta^2, \omega\theta^3)$, where ${}^tC$ denotes the transpose of the matrix C. Then we obtain $A = \begin{pmatrix} E_4 & O_4 \\ -E_4 & 2E_4 \end{pmatrix}$, where E_4 is the 4×4 identity matrix and O_4 is the 4×4 zero matrix. Thus by $d_L(\theta) = det(A)^2 \cdot d_L$, we have

$$\mathrm{N}_L(f'(\theta)) = (2^3)^8 \mathrm{N}_L(\theta^7) = 2^{24}(-m)^7 = 2^8 \cdot d_L$$

and hence $d_L = -2^{16}m^7$.

Next, we consider the case of $m \equiv 9 \pmod{16}$, i.e., $m = 9 + 16m_1, m_1 \in \mathbb{Z}$. By Lemma 2 and $\mathbb{Z}_K = \mathbb{Z}[1, \omega, \theta^2, \omega\frac{1+\theta^2}{2}]$, for any integer $\eta \in \mathbb{Z}_L$ we have $2\eta = \alpha + \beta\theta$ with $\alpha, \beta \in \mathbb{Z}_K$ such that

$$4N_{L/K}(\eta) = N_{L/K}(2\eta) = (\alpha + \beta\theta)(\alpha + \beta(-\theta)) = \alpha^2 - \beta^2\theta^2$$

with $\alpha = a_{00} + a_{01}\omega + a_{10}\theta^2 + a_{11}\omega\frac{1+\theta^2}{2}$ and $\beta = b_{00} + b_{01}\omega + b_{10}\theta^2 + b_{11}\omega\frac{1+\theta^2}{2}$. Put $\eta_3 = \omega\frac{1+\theta^2}{2}$. Then

$$\begin{aligned} \alpha^2 - \beta^2\theta^2 \equiv\ & a_{00}^2 + a_{01}^2\omega^2 + a_{10}^2\theta^4 + a_{11}^2\eta_3^2 \\ & - \{b_{00}^2 + b_{01}^2\omega^2 + b_{10}^2\theta^4 + b_{11}^2\eta_3^2\}\theta^2 \pmod{2\mathbb{Z}_K}. \end{aligned} \tag{2.9}$$

We have the following congruences

$$\begin{aligned} \omega^2 &= \omega + 2 + 4m_1 \equiv \omega \pmod{2\mathbb{Z}_K}, \\ \eta_3^2 &= \eta_3 + 1 + 2m_1 + (1 + 2m_1)(1 + \theta^2) + (1 + 2m_1)(\omega - 1) \\ &\equiv \eta_3 + \theta^2 + 1 + \omega \pmod{2\mathbb{Z}_K}, \\ \theta^4 &= 2\omega - 1 \equiv 1 \pmod{2\mathbb{Z}_K} \\ \omega\theta^2 &= 2\eta_3 - \omega \equiv \omega \pmod{2\mathbb{Z}_K} \\ \text{and } \eta_3\theta^2 &= \eta_3 - \omega\omega^\sigma \equiv \eta_3 \pmod{2\mathbb{Z}_K}. \end{aligned}$$

Substituting these congruences into (2.9) we obtain

$$\begin{aligned} \alpha^2 - \beta^2\theta^2 \equiv\ & (a_{00} + a_{10} + a_{11} + b_{11}) + (a_{01} + a_{11} + b_{01} + b_{11})\omega \\ & + (a_{11} + b_{00} + b_{10} + b_{11})\theta^2 + (a_{11} + b_{11})\eta_3 \equiv 0 \pmod{2\mathbb{Z}_K}. \end{aligned}$$

Thus we have

$$\begin{aligned} & a_{00} + a_{10} + a_{11} + b_{11} \equiv 0 \pmod 2, && a_{01} + a_{11} + b_{01} + b_{11} \equiv 0 \pmod 2, \\ & a_{11} + b_{00} + b_{10} + b_{11} \equiv 0 \pmod 2, && \text{and} \quad a_{11} + b_{11} \equiv 0 \pmod 2. \end{aligned}$$

From these congruences we deduce that

$$a_{00} \equiv a_{10},\ a_{01} \equiv b_{01},\ b_{00} \equiv b_{10},\ a_{11} \equiv b_{11} \pmod 2. \tag{2.10}$$

Next, for the congruence
$0 \equiv 4N_{L/K}(\eta) = \alpha^2 - \beta^2\theta^2 \equiv c_0 \cdot 1 + c_1 \cdot \omega + c_2 \cdot \theta^2 + c_3 \cdot \eta_3 \pmod{4\mathbb{Z}_K}$ we evaluate the coefficients $c_j (0 \leqq j \leqq 3)$. From (2.10) we have

$$a_{00}^2 \equiv a_{10}^2, a_{01}^2 \equiv b_{01}^2, b_{00}^2 \equiv b_{10}^2, a_{11}^2 \equiv b_{11}^2 \pmod 4, \tag{2.11}$$

$$2a_{00}a_{10} \equiv 2a_{00}^2, 2a_{01}a_{10} \equiv 2a_{01}a_{00}, 2a_{10}a_{11} \equiv 2a_{00}a_{11} \pmod 4, \tag{2.12}$$

$$2b_{00}b_{10} \equiv 2b_{00}^2, 2b_{01}b_{10} \equiv 2b_{01}b_{00}, 2b_{10}b_{11} \equiv 2b_{00}b_{11} \pmod 4. \tag{2.13}$$

In this case we use the congruences
$\omega^2 \equiv \omega + 2 \pmod{4\mathbb{Z}_K}, \theta^4 = 2\omega - 1, \omega\theta^2 \equiv 2\eta_3 - \omega, \omega\eta_3 = \eta_3 + (1+\theta^2)(1+2m_1)$, $\eta_3\theta^2 \equiv \eta_3 + 2 \pmod{4\mathbb{Z}_K}$ and $\eta_3^2 = \eta_3 + (1+2m_1) + (1+2m_1)\omega + (1+2m_1)\theta^2$. Together with (2.11), (2.12) and (2.13) we have

$$\begin{aligned}
\alpha^2 &\equiv \{a_{00}^2 + 2a_{01}^2 - a_{10}^2 + a_{11}^2(1+2m_1) + 2a_{01}a_{11}\} \\
&\quad + \{a_{01}^2 + 2a_{10}^2 + a_{11}^2(1+2m_1) + 2a_{00}a_{01} - 2a_{01}a_{10}\}\omega \\
&\quad + \{a_{11}^2(1+2m_1) + 2a_{00}a_{10} + 2a_{01}a_{11}\}\theta^2 + \{a_{11}^2 + 2a_{00}a_{11} + 2a_{01}a_{11} + 2a_{10}a_{11}\}\eta_3 \\
&\equiv \{2a_{01}^2 + a_{11}^2(2m_1+1) + 2a_{01}a_{11}\} + \{a_{01}^2 + 2a_{00}^2 + a_{11}^2(2m_1+1)\}\omega \\
&\quad + \{a_{11}^2(2m_1+1) + 2a_{00}^2 + 2a_{01}a_{11}\}\theta^2 + \{a_{11}^2 + 2a_{01}a_{11}\}\eta_3 \pmod{4\mathbb{Z}_K} \text{ and}
\end{aligned}$$

$$\begin{aligned}
\beta^2\theta^2 &\equiv -\{a_{11}^2(2m_1+1) + 2b_{00}^2 + 2a_{01}a_{11} - 2a_{11}^2 - 4a_{01}a_{11}\} \\
&\quad - \{a_{01}^2 + 2b_{00}^2 + a_{11}^2(2m_1+1) - 2a_{11}^2(2m_1+1) - 4b_{00}^2 - 4a_{01}a_{11}\}\omega \\
&\quad + \{2a_{01}^2 + a_{11}^2(2m_1+1) + 2a_{01}a_{11}\}\theta^2 \\
&\quad + \{2a_{01}^2 + 4b_{00}^2 + 2a_{11}^2(2m_1+1) + a_{11}^2 + 2a_{01}a_{11}\}\eta_3 \pmod{4\mathbb{Z}_K}.
\end{aligned}$$

Then we obtain

$$\begin{aligned}
0 &\equiv \alpha^2 - \beta^2\theta^2 \equiv \{2a_{01}^2 + 2a_{11}^2\} + \{2a_{01}^2 + 2a_{00}^2 + a_{11}^2 + 2b_{00}^2\}\omega \\
&\quad + \{2a_{01}^2 + 2a_{11}^2 + 2a_{00}^2\}\theta^2 + \{2a_{01}^2\}\eta_3 \pmod{4Z_K}.
\end{aligned}$$

As the set $\{1, \omega, \theta^2, \eta_3\}$ forms an integral basis of $\mathbb{Z}_K$, we have

$$0 \equiv 2a_{01}^2 + 2a_{11}^2 \pmod 4, 0 \equiv 2a_{01}^2 + 2a_{00}^2 + a_{11}^2 + 2b_{00}^2 \pmod 4,$$
$$0 \equiv 2a_{01}^2 + 2a_{11}^2 + 2a_{00}^2 \pmod 4 \text{ and } 0 \equiv a_{01} \pmod 4,$$

which yields

$$a_{01} \equiv a_{11} \equiv a_{00} \equiv b_{00} \equiv 0 \pmod 2.$$

Together with the congruences (2.10) we have proved that all the coefficients $a_{ij}, b_{ij} (0 \leqq i, j \leqq 1)$ of η are even. Thus it follows that $\mathbb{Z}_L \subseteqq \mathbb{Z}_K[1,\theta]$ and $\mathbb{Z}_K[1,\theta] \subseteqq \mathbb{Z}_L$ because θ is an integer of L. Therefore we obtain

$$\mathbb{Z}_L = \mathbb{Z}_K[1,\theta] = \mathbb{Z}[1, \omega, \theta^2, \omega\tfrac{1+\theta^2}{2}, \theta, \omega\theta, \theta^3, \omega\tfrac{\theta+\theta^3}{2}].$$

Let B be the representation matrix of ${}^t(1, \theta, \theta^2, \theta^3, \theta^4, \theta^5, \theta^6, \theta^7)$ with respect to the integral basis ${}^t(1, \theta, \theta^2, \theta^3, \omega, \omega\theta, \omega\frac{1+\theta^2}{2}, \omega\frac{\theta+\theta^3}{2})$. Then we obtain

$B = \begin{pmatrix} E_4 & O_4 \\ A_4 & B_4 \end{pmatrix}$ with $B_4 = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ -1 & 0 & 4 & 0 \\ 0 & -1 & 0 & 4 \end{pmatrix}$ and a suitable 4×4 matrix

A_4. Thus from $d_L(\theta) = det(B)^2 \cdot d_L$, we deduce $-2^{24}m^7 = (2^6)^2 \cdot d_L$ and hence $d_L = -2^{12}m^7$.

Finally, we consider the case of $m \equiv 1 \pmod{16}$. We set $m-1 = 16m_1$, where $m_1 \in \mathbb{Z}$. As in the case $m \equiv 9 \pmod{16}$, by Lemmas 2 and 3, for any integer $\eta \in Z_L$, there exist $\alpha, \beta \in \mathbb{Z}_K$ such that $2\eta = \alpha + \beta\theta$ with
$\alpha = a_{00} + a_{01}\omega + a_{10}\theta^2 + a_{11}\omega\frac{1+\theta^2}{2}$ and $\beta = b_{00} + b_{01}\omega + b_{10}\theta^2 + b_{11}\omega\frac{1+\theta^2}{2}$.
Then we have $\mathrm{N}_{L/K}(2\eta) = (\alpha + \beta\theta)(\alpha + \beta(-\theta)) = \alpha^2 - \beta^2\theta^2 \equiv 0 \pmod{4\mathbb{Z}_K}$.
Thus $\alpha^2 - \beta^2\theta^2 \equiv (a_{00} + a_{10}) \cdot 1 + (a_{01} + b_{10})\omega + (b_{00} + b_{10})\theta^2 + (a_{11} + b_{11})\eta_3$
$\equiv 0 \pmod{2\mathbb{Z}_K}$ holds. Here we used $\omega^2 = \omega + 4m_1 \equiv \omega \pmod{4\mathbb{Z}_K}$,
$\theta^4 = 2\omega - 1 \equiv 1 \pmod{2\mathbb{Z}_K}$, $\eta_3^2 \equiv \eta_3 \pmod{2\mathbb{Z}_K}, \omega^2\theta^2 \equiv \omega \pmod{2\mathbb{Z}_K}$,
and $\theta^6 = \theta^2(2\omega - 1) \equiv \theta^2 \pmod{2\mathbb{Z}_K}$. Thus, it follows that

$$a_{00} \equiv a_{10},\ a_{01} \equiv b_{01},\ b_{00} \equiv b_{10} \text{ and } a_{11} \equiv b_{11} \pmod 2. \tag{2.14}$$

Next we evaluate a_{ij}, b_{ij} modulo 4 $(0 \leqq i, j \leqq 1)$. We have
$\mathrm{N}_{L/K}(2\eta) = \{a_{00} + a_{01}\omega + a_{00}\theta^2 + a_{11}\eta_3\}^2 - \{b_{00} + a_{01}\omega + b_{00}\theta^2 + a_{11}\eta_3\}^2\theta^2$
$\equiv 0 \pmod{4\mathbb{Z}_K}$.
Using $\theta^4 = 2\omega - 1, \omega + \omega^\sigma = 1, \omega - 1 = -\omega^\sigma$,
$\eta_3^2 = \eta_3 + 2m_1\theta^2 + 2m_1\omega - 2m_1$, $\omega\theta^2 = 2\eta_3 - \omega$ and $\omega\eta_3 = \eta_3 + 2m_1 + 2m_1\theta^2$,
we deduce that $\eta_3\theta^2 \equiv \eta_3 \pmod{4\mathbb{Z}_K}$, $\omega^2\theta^2 \equiv (2\eta_3 - \omega) \pmod{4\mathbb{Z}_K}$,
$\theta^6 \equiv (2\omega - \theta^2) \pmod{4\mathbb{Z}_K}$, $\eta_3^2\theta^2 \equiv (\eta_3 + 2m_1\theta^2 + 2m_1\omega + 2m_1) \pmod{4\mathbb{Z}_K}$,
$\omega\theta^4 = \omega(2\omega - 1) \equiv \omega \pmod{4\mathbb{Z}_K}$ and $\omega^2\frac{1+\theta^2}{2}\cdot\theta^2 \equiv \eta_3 + 2m_1\theta^2 + 2m_1 \pmod{4\mathbb{Z}_K}$.
Thus $0 \equiv 4N_{L/K}(\eta) \equiv (2a_{11}m_1 - b_{00}^2 - 2a_{11}m_1 + 2b_{00}) \cdot 1 + (a_{01}^2 + 2a_{00} + 2m_1a_{11}$
$+ 2a_{00}a_{01} - 2a_{01}a_{00} + a_{01}^2 - 2b_{00} - 2m_1a_{11} + 2b_{00}a_{01} + 2a_{01}b_{00})\omega + (2a_{00} - b_{00}^2)\theta^2$
$+ (a_{11}^2 + 2a_{00}a_{11} + 2a_{01}a_{11} + 2a_{00}a_{11} - 2a_{01} - a_{11}^2 - 2b_{00}a_{11} - 2a_{01}a_{11} - 2a_{11}b_{00})\eta_3$
$\pmod{4\mathbb{Z}_K}$. Then we obtain that
i) $0 \equiv b_{00}(b_{00} - 2) \pmod 4$,
ii) $0 \equiv 2a_{01} + 2a_{00} + 2b_{00} \pmod 4$, i.e., $0 \equiv a_{01} + a_{00} + b_{00} \pmod 2$
iii) $0 \equiv 2a_{00} - b_{00}^2 \pmod 4$ and
iv) $0 \equiv 2a_{00}a_{11} + 2a_{01} + 2a_{01}a_{11} \pmod 4$, i.e., $0 \equiv a_{00}a_{11} + a_{01} + a_{01}a_{11} \pmod 2$.
By (i) we see that $b_{00} \equiv 0 \pmod 2$. Then by (iii) we deduce that $a_{00} \equiv 0 \pmod 2$, and hence by ii) $a_{01} \equiv 0 \pmod 2$. The values of a_{00} and a_{01} satisfy the condition iv). Moreover, from (2.14), we get $a_{10} \equiv b_{01} \equiv b_{10} \equiv 0 \pmod 2$ Thus

$$\eta = \frac{\alpha}{2} + \frac{\beta}{2}\theta \equiv a_{11}\omega\frac{1+\theta^2}{2} + b_{11}\omega\frac{1+\theta^2}{2}\theta \pmod{\mathbb{Z}_L}.$$

Next, by (2.14) both a_{11} and b_{11} are of the same parity. In even case
$\eta = 2\eta_3(1+\theta) \equiv 0 \pmod{2\mathbb{Z}_K}$. In the odd case we obtain the integer
$\eta \equiv \omega\frac{1+\theta^2}{2}\frac{1+\theta}{2} \pmod{2\mathbb{Z}_L}$, which is denoted by η_7. In fact η_7 is an integer in $\mathbb{Z}_L$, because $T_{L/K}(\eta_7) = \eta_7 + \eta_7^{\sigma^4} = \eta_3 \in Z_K$ and
$N_{L/K}(\eta_7) = \eta_7 \cdot \eta_7^{\sigma^4} = \omega\frac{1+\theta^2}{2}\frac{1+\theta}{2} \cdot \omega\frac{1+\theta^2}{2}\frac{1-\theta}{2} = \frac{1}{4}\omega\omega^\sigma\eta_3 = m_1\eta_3 \in Z_K$.
Then it follows that $\eta \in \mathbb{Z}[1, \omega, \theta^2, \eta_3, \theta, \omega\theta, \theta^3, \eta_7]$, so that

$\mathbb{Z}_L \subsetneqq \mathbb{Z}[1, \omega, \theta^2, \eta_3, \theta, \omega\theta, \theta^3, \eta_7]$. On the other hand $\mathbb{Z}[1, \omega, \theta^2, \eta_3, \theta, \omega\theta, \theta^3, \eta_7] \subsetneqq \mathbb{Z}_L$ holds as $\eta_7 = \omega\frac{1+\theta^2}{2}\frac{1+\theta}{2} \in \mathbb{Z}_L$. Therefore we obtain $\mathbb{Z}_L = \mathbb{Z}[1, \omega, \theta^2, \eta_3, \theta, \omega\theta, \theta^3, \eta_7]$ for any pure octic field $\mathbb{Q}(\sqrt[8]{m})$ with a square-free integer $m \equiv 1 \pmod{16}, m \neq 1$.

Let C be the representation matrix of ${}^t(1, \theta, \theta^2, \theta^3, \theta^4, \theta^5, \theta^6, \theta^7)$ with respect to the integral basis ${}^t(1, \omega, \theta^2, \eta_3, \theta, \omega\theta, \theta^3, \eta_7)$. Then we obtain $C = \begin{pmatrix} E_4 & O_4 \\ C_4 & D_4 \end{pmatrix}$, where $D_4 = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ -1 & 0 & 4 & 0 \\ -1 & -1 & -1 & 8 \end{pmatrix}$ and a suitable4×4 matrix C_4. From $d_L(\theta) = det(C)^2 \cdot d_L$, we have $-2^{24}m^7 = (2^7)^2 \cdot d_L$ and hence $d_L = -2^{10}m^7$. □

3 Relative Monogenity of a Pure Octic Field over its Quartic and Quadratic Subfield

In this section, we determine the relative monogenity of a pure octic field $L = \mathbb{Q}(\theta)$ with $\theta = \sqrt[8]{m}$ of a square-free integer $m \neq 0, \pm 1$ over its quartic subfield $K = \mathbb{Q}(\theta^2)$ and its quadratic subfield $k = \mathbb{Q}(\theta^4)$. It follows from Lemma 2 and Theorem 1 that $\mathbb{Z}_L = \mathbb{Z}_K[\theta] = \mathbb{Z}_k[\theta]$ for $m \equiv 2, 3 \pmod 4$ and $m \equiv 5, 13 \pmod{16}$, that is, the pure octic field $L = \mathbb{Q}[\sqrt[8]{m}]$ is relatively monogenic over its quartic subfield K and its quadratic subfield k. We also see from Lemma 2 and Theorem 1 that

$$\mathbb{Z}_L = \mathbb{Z}[1, \omega, \theta^2, \omega\frac{1+\theta^2}{2}, \theta, \omega\theta, \theta^3, \omega\frac{\theta+\theta^3}{2}] = \mathbb{Z}_K[\theta],$$

namely L is relatively monogenic over K for $m \equiv 9 \pmod{16}$. We summarize these results in Theorem 2.

Theorem 2. *With the same notation as above, the pure octic field L is relatively monogenic over its quartic subfield K for $m \equiv 2, 3 \pmod 4$ and for $m \equiv 5, 9, 13 \pmod{16}$. Moreover L is relatively monogenic over its quadratic subfield k for $m \equiv 2, 3 \pmod 4$ and for $m \equiv 5, 13 \pmod{16}$.*

Thus we must investigate the existence or non-existence of a relative power integral basis of $\mathbb{Z}_L$ over $\mathbb{Z}_k$ when $m \equiv 9 \pmod{16}$ and over $\mathbb{Z}_K$ and $\mathbb{Z}_k$ when $m \equiv 1 \pmod{16}$. The next lemma is available to avoid lengthy and complicated computations in the succeeding proofs.

Lemma 4. *With the same notation as above, the following congruences modulo $2\mathbb{Z}_L$ hold.*
(i) *Let $m \equiv 9 \pmod{16}$. Then $\theta^4 \equiv 1, \omega^2 \equiv \omega, \omega\theta^2 \equiv \omega$, $\eta_3\omega \equiv 1 + \theta^2 + \eta_3$,*

$\eta_3^2 \equiv 1+\omega+\theta^2+\eta_3$ *and* $\eta_3\theta^2 \equiv \eta_3 \pmod{2\mathbb{Z}_L}$.
(ii) *Let* $m \equiv 1 \pmod{16}$. *Then* $\theta^4 \equiv 1, \omega^2 \equiv \omega\theta^2 \equiv \omega$, $\eta_3\omega \equiv \eta_3^2 \equiv \eta_3\theta^2 \equiv \eta_3$, $\eta_7\omega = \eta_7 + m_1(1+\theta+\theta^2+\theta^3), \eta_7\theta^2 \equiv \eta_7$ *and* $\eta_7^2 \equiv m_1(1+\omega+\theta^2+\eta_3+\theta+\omega\theta+\theta^3)+\eta_7 \pmod{2\mathbb{Z}_L}$.

Proof: (i) Put $m = 9+16n = 1+8m_1$ with $m_1 \equiv 1 \pmod 2$.
Then $\omega = \frac{1+\theta^4}{2}$ gives $\theta^4 = 2\omega - 1 \equiv 1 \pmod{2\mathbb{Z}_L}$,
$\omega^2 = \{\frac{1+\theta^4}{2}\}^2 = \omega + \frac{m-1}{4} = \omega + 2m_1 \equiv \omega \pmod{2\mathbb{Z}_L}$,
$\omega\theta^2 = 2\omega\frac{1+\theta^2}{2} - \omega = 2\eta_3 - \omega \equiv \omega \pmod{2\mathbb{Z}_L}$,
$\eta_3\omega = \omega^2\frac{1+\theta^2}{2} = (\omega+\frac{m-1}{4})(\frac{1+\theta^2}{2}) = (\omega+2m_1)(\frac{1+\theta^2}{2}) = m_1 + m_1\theta^2 + \eta_3$
$\equiv 1+\theta^2+\eta_3$.
Similarly, we have

$$\begin{aligned}\eta_3^2 &= \omega^2(\frac{1+\theta^2}{2})^2 = (\omega+\frac{m-1}{4})(\frac{1+\theta^4+2\theta^2}{4}) = (\omega+2m_1)(\frac{\omega}{2}+\frac{\theta^2}{2})\\ &= m_1(\omega+\theta^2) + \frac{1}{2}(\omega^2+\omega\theta^2) = m_1(\omega+\theta^2)+\frac{1}{2}(2m_1+\omega+2\eta_3-\omega)\\ &= m_1 + m_1\omega + m_1\theta^2 + \eta_3 \equiv 1+\omega+\theta^2+\eta_3 \pmod{2\mathbb{Z}_L},\end{aligned}$$

and finally
$\eta_3\theta^2 = \omega(\frac{1+\theta^2}{2})\theta^2 = \omega(\frac{1+\theta^2}{2})(\theta^2-1+1) = -\omega\omega^\sigma + \eta_3 = 2m_1 + \eta_3$
$\equiv \eta_3 \pmod{2\mathbb{Z}_L}$.

(ii) We prove congruences for $\theta^4, \omega^2, \omega\theta^2, \eta_3\omega, \eta_3^2, \eta_3\theta^2$ and $\eta_3\omega$ modulo $2\mathbb{Z}_L$ by using $\omega\omega^\sigma = -4m_1, \omega^\sigma - 1 = -\omega$ and $\frac{m-1}{8} = 2m_1 \equiv 0 \pmod 2$ and $\eta_7 = \omega\frac{1+\theta^2}{2}\frac{1+\theta}{2} = \eta_3\frac{1+\theta}{2}$, as follows:
$\eta_7\omega = \omega^2\frac{1+\theta^2}{2}\frac{1+\theta}{2} = (\omega+4m_1)\frac{1+\theta^2}{2}\frac{1+\theta}{2} = \eta_7 + m_1(1+\theta+\theta^2+\theta^3)$,
$\eta_7\theta^2 = \omega\frac{1+\theta^2}{2}\frac{1+\theta}{2}(\theta^2-1+1) = -\omega\omega^\sigma\frac{1+\theta}{2} + \eta_7 = 2m_1(1+\theta)+\eta_7 \equiv \eta_7$, and in the same way

$$\begin{aligned}\eta_7^2 &= \omega^2(\frac{1+\theta^2}{2})^2\cdot(\frac{1+\theta}{2})^2 = (4m_1+\omega)\{\frac{1+\theta^2}{2}-\frac{1-\theta^4}{4}\}\{\frac{1+\theta}{2}-\frac{1-\theta^2}{4}\}\\ &= (4m_1+\omega)\{\frac{1+\theta^2}{2}\}\{\frac{1+\theta}{2}\} + (4m_1+\omega)\{-\frac{1}{4}\omega^\sigma - \frac{1}{2}\omega^\sigma\frac{1+\theta}{2} + \frac{1}{2}\omega^\sigma\frac{1-\theta^2}{4}\}\\ &= m_1(1+\theta^2)(1+\theta) + \eta_7 + (4m_1\omega^\sigma - 4m_1)\{-\frac{1}{4} - \frac{1}{2}\frac{1+\theta}{2} + \frac{1}{2}\frac{1-\theta^2}{4}\}\\ &= m_1(1+\theta^2)(1+\theta) + \eta_7 + m_1\omega(1+1+\theta-\frac{1-\theta^2}{2})\\ &= m_1(1+\theta^2)(1+\theta) + \eta_7 + m_1\omega(1+\theta+\eta_3)\\ &= m_1(1+\omega+\theta^2+\eta_3+\theta+\omega\theta+\theta^3)+\eta_7\end{aligned}$$

□

Theorem 3. *With the same notation as above, let* $m \equiv 9 \pmod{16}$. *Then the pure octic field* $L = \mathbb{Q}(\theta)$ *with* $\theta = \sqrt[8]{m}$ *does not have a relative power integral basis over its quadratic subfield* k, *that is,* $\mathbb{Z}_L \neq \mathbb{Z}_k[\eta]$ *for any* $\eta \in \mathbb{Z}_L$ *if* $m \equiv 9 \pmod{16}$.

Proof: Suppose that L has a relative power integral basis over k, that is,

$$\mathbb{Z}_L = \mathbb{Z}_k[\eta] = Z_k[1, \eta, \eta^2, \eta^3] = \mathbb{Z}[1, \omega, \eta, \omega\eta, \eta^2, \omega\eta^2, \eta^3, \omega\eta^3]$$

holds for some integer $\eta \in \mathbb{Z}_L$. By Theorem 1 we have an integral basis

$$\mathbb{Z}_L = \mathbb{Z}_K[\theta] = \mathbb{Z}[1, \omega, \theta^2, \eta_3, \theta, \omega\theta, \theta^3, \eta_3\theta] \text{ with } \eta_3 = \omega\frac{1+\theta^2}{2}$$

Then there exists an 8×8 matrix A with coefficients in $\mathbb{Z}$ such that

$${}^t(1, \omega, \eta^2, \omega\eta^2, \eta, \omega\eta, \eta^3, \omega\eta^3) = A^t(1, \omega, \theta^2, \eta_3, \theta, \omega\theta, \theta^3, \eta_3\theta).$$

Therefore for $\eta = a_0 + a_1\omega + a_2\theta^2 + a_3\eta_3 + (b_0 + b_1\omega + b_2\theta^2 + b_3\eta_3)\theta$ with $a_j, b_j \in \mathbb{Z}, j = 0, 1, 2, 3$, we deduce the following congruences modulo $2\mathbb{Z}_L$ using Lemma 4 (i)

$$\begin{aligned}\eta^2 &\equiv a_0 + a_1\omega^2 + a_2\theta^4 + a_3\eta_3^2 + (b_0 + b_1\omega^2 + b_2\theta^4 + b_3\eta_3^2)\theta^2 \\ &\equiv (a_0 + a_2 + a_3 + b_3) + (a_1 + a_3 + b_1 + b_3)\omega + (a_3 + b_0 + b_2 + b_3)\theta^2 \\ &\quad + (a_3 + b_3)\eta_3 + 0 + 0 + 0 + 0 \pmod{2\mathbb{Z}_L} \text{ and} \\ \omega\eta^2 &\equiv (a_0 + a_2 + a_3 + b_3)\omega + (a_1 + a_3 + b_1 + b_3)\omega^2 + (a_3 + b_0 + b_2 + b_3)\omega\theta^2 \\ &\quad + (a_3 + b_3)\omega\eta_3 + 0 + 0 + 0 + 0 \\ &\equiv (a_3 + b_3) + (a_0 + a_1 + a_2 + a_3 + b_0 + b_1 + b_2 + b_3)\omega + (a_3 + b_3)\theta^2 \\ &\quad + (a_3 + b_3)\eta_3 + 0 + 0 + 0 + 0 \pmod{2\mathbb{Z}_L}.\end{aligned}$$

Then we obtain $\eta^2 \sim \eta^2 + \omega\eta^2 \equiv (a_0 + a_2) + (a_0 + a_2 + b_0 + b_2)\omega + (b_0 + b_2)\theta^2$ $\equiv a + (a+b)\omega + b\theta^2 \pmod 2$ with $a_0 + a_2 = a$ and $b_0 + b_2 = b$. Here for $\gamma, \delta \in L, \gamma \sim \delta$ means the corresponding row vectors of γ and δ with respect to an integral basis of L are equal to each other modulo an elementary row operation.

Consider the last row of the matrix A corresponding to the integer $\omega\eta^3$. We have $\omega\eta^3 = \omega \cdot \eta^2 \cdot \eta \equiv \omega\{a + (a + b)\omega + b\theta^2\}\eta \equiv \{a\omega + a\omega^2 + b\omega^2 + b\theta^2\omega^2\}\eta$ $\equiv \{a\omega + a\omega + b\omega + b\omega\}\eta \equiv 0 \pmod{2\mathbb{Z}_L}$. Thus we obtain $det(A) \equiv 0 \pmod 2$. Thereby $\mathbb{Z}_L$ has no relative power integral basis over $\mathbb{Z}_k$ for $m \equiv 9 \pmod{16}$. □

Theorem 4. *With the same notation as above, let* $m \equiv 1 \pmod{16}$. *Then the pure octic field* $L = \mathbb{Q}(\theta)$ *with* $\theta = \sqrt[8]{m}$ *is relatively non monogenic over its quadratic subfield* $k = \mathbb{Q}(\theta^4)$, *that is,* $\mathbb{Z}_L$ *does not have a power integral basis over* $\mathbb{Z}_k$.

Proof: Assume that $\mathbb{Z}_L = \mathbb{Z}_k[\eta] = \mathbb{Z}_k[1, \eta, \eta^2, \eta^3] = \mathbb{Z}[1, \omega, \eta, \omega\eta, \eta^2, \omega\eta^2, \eta^3, \omega\eta^3]$. Then there exists a representation matrix A of size 8 by 8 with coefficients in $\mathbb{Z}$ with respect to an integral basis $\{1, \omega, \theta^2, \eta_3, \theta, \omega\theta, \theta^3, \eta_7\}$ with $\eta_7 = \eta_3\frac{1+\theta}{2}$. Therefore for $\eta = a_0 + a_1\omega + a_2\theta^2 + a_3\eta_3 + b_0\theta + b_1\omega\theta + b_2\theta^3 + b_3\eta_7$ we have

$${}^t(1, \omega, \eta^2, \omega\eta^2, \eta, \omega\eta, \eta^3, \omega\eta^3) = A \cdot {}^t(1, \omega, \theta^2, \eta_3, \theta, \omega\theta, \theta^3, \eta_7),$$

with $a_j, b_j \in \mathbb{Z}$, $j = 0, 1, 2, 3$. Using Lemma 4 (ii) we compute the row vectors of A corresponding to the integers η^2 and $\omega\eta^2$ as follows:

$$\begin{aligned}\eta^2 &\equiv (a_0 + a_2 + m_1b_3) + (a_1 + b_1 + m_1b_3)\omega + (b_0 + b_2 + m_1b_3)\theta^2 \\ &\quad + (a_3 + m_1b_3)\eta_3 + m_1b_3\theta + m_1b_3\omega\theta + m_1b_3\theta^3 + b_3\eta_7 \pmod{2\mathbb{Z}_L}, \text{ and}\end{aligned}$$

$\omega\eta^2 \equiv (a_0+a_2+m_1b_3)\omega+(a_1+b_1+m_1b_3)\omega^2 +(b_0+b_2+m_1b_3)\omega\theta^2+(a_3+m_1b_3)\omega\eta_3$
$+m_1b_3\omega\theta + m_1b_3\omega^2\theta + m_1b_3\omega\theta^3 + b_3\omega\eta_7$
$\equiv m_1b_3 + (a_0 + a_1 + a_2 + b_0 + b_1 + b_2 +m_1b_3)\omega + m_1b_3\theta^2 + (a_3 + m_1b_3)\eta_3$
$+ m_1b_3\theta + m_1b_3\omega\theta + m_1b_3\theta^3 + b_3\eta_7$.

We reduce $\eta^2 \sim \eta^2 + \omega\eta^2 \equiv (a_0 + a_2) + (a_0 + a_2 + b_0 + b_2)\omega + (b_0 + b_2)\theta^2$
$\equiv a + (a + b)\omega + b\theta^2 \pmod{2\mathbb{Z}_L}$ with $a = a_0 + a_2$ and $b = b_0 + b_2$.
Consider the 8th row of A corresponding to $\omega\eta^3$. By Lemma 4(ii) we have
$\omega\eta^3 = \omega\eta^2 \cdot \eta \equiv [a\omega + (a+b)\omega^2 + b\omega\theta^2]\eta \equiv [a\omega + (a+b)\omega + b\omega]\eta \equiv 0 \pmod{2\mathbb{Z}_L}$,
so that $det(A) \equiv 0 \pmod 2$.
Thus $\mathbb{Z}_L$ has no relative power integral basis over $\mathbb{Z}_k$ for $m \equiv 1 \pmod{16}$. ∎

Theorem 5. *With the same notation as above, let the square-free integer m satisfy $m \equiv 1 \pmod{16}$ with $m = 1 + 16m_1, m_1 \in \mathbb{Z}$. If the pure octic field $L = \mathbb{Q}(\sqrt[8]{m})$ has a relative power integral basis over the quartic subfield K, that is, there exists $\eta \in \mathbb{Z}_L$ such that $\mathbb{Z}_L = \mathbb{Z}_K[\eta]$ for $\eta = \alpha + b_0\theta + b_1\omega\theta + b_2\theta^2 + b_3\eta_7$ with $\alpha \in \mathbb{Z}_K$, then the necessary congruence conditions are*

$$b_1 + m_1 \equiv 0,\ b_0 + b_2 \equiv 1 \text{ and } b_3 \equiv 1 \pmod 2.$$

Proof: Assume that $\mathbb{Z}_L = \mathbb{Z}_K[\eta] = \mathbb{Z}[1, \omega, \theta^2, \eta_3, \eta, \omega\eta, \theta^2\eta, \eta_3\eta]$ for some $\eta \in \mathbb{Z}_L$. Put $\eta = \alpha + \beta\theta + b_3\eta_7$ with $\alpha = a_0 + a_1\omega + a_2\theta^2 + a_3\eta_3$ and $\beta = b_0 + b_1\omega + b_2\theta^2 \in \mathbb{Z}_K$. Then using the congruence relations modulo $2\mathbb{Z}_L$ in Lemma 4 (ii), we deduce that $\omega\eta \equiv m_1b_3 + (a_0 + a_1 + a_2)\omega + m_1b_3\theta^2 + a_3\eta_3 + m_1b_3\theta + (b_0 + b_1 + b_2)\omega\theta + m_1b_3\theta^3 + b_3\eta_7 \pmod{2\mathbb{Z}_L} \equiv m_1b_3\theta + (b_0 + b_1 + b_2)\omega\theta + m_1b_3\theta^3 + b_3\eta_7 \pmod{(\mathbb{Z}_K, 2\mathbb{Z}_L)}$. Similarly it is deduced that
$\theta^2\eta \equiv b_2\theta + b_1\omega\theta + b_0\theta^3 + b_3\eta_7 \pmod{(\mathbb{Z}_K, 2\mathbb{Z}_L)}$ and
$\eta_3\eta \equiv m_1b_3 + m_1b_3\omega\theta + m_1b_3\eta_7 \pmod{2Z_L}$. Thus we have
${}^t(1, \omega, \theta^2, \eta_3, \eta, \omega\eta, \theta^2\eta, \eta_3\eta) = \begin{pmatrix} E_4 & O_4 \\ A_4 & B \end{pmatrix} {}^t(1, \omega, \theta^2, \eta_3, \theta, \omega\theta, \theta^3, \eta_7)$ with a suitable 4×4 matrix A_4 and $B = \begin{pmatrix} b_0 & b_1 & b_2 & b_3 \\ m_1b_3 & b_0 + b_1 + b_2 & m_1b_3 & b_3 \\ b_2 & b_1 & b_0 & b_3 \\ m_1b_3 & m_1b_3 & m_1b_3 & b_3 \end{pmatrix}$.

Then we obtain $det(B) \equiv \begin{vmatrix} b_0 + b_2 & 0 & b_0 + b_2 & 0 \\ 0 & b_0 + b_1 + b_2 + m_1b_3 & 0 & 0 \\ b_2 & b_1 & b_0 & b_3 \\ m_1b_3 & m_1b_3 & m_1b_3 & b_3 \end{vmatrix} \pmod 2$
$\equiv (b_0 + b_2)b_3(b_0 + b_1 + b_2 + m_1b_3)(b_0 + b_2) \pmod 2$.
If $b_3 \not\equiv 0 \pmod 2$ and $b_0 + b_2 \not\equiv 0 \pmod 2$, then $det(B) \equiv 1 \cdot 1 \cdot (1 + b_1 + m_1) \cdot 1 \pmod 2$. Thus it is deduced that $det(A) \equiv 1 \pmod 2$ if $b_1 + m_1 \equiv 0$, $b_0 + b_2 \equiv 1$ and $b_3 \equiv 1 \pmod 2$. ∎

Acknowledgements. We express our sincere gratitude to the referee for his(her) substantial notices to improve this paper and Prof. K. S. Williams (Carleton

Univ. Canada) for his valuable comments. We also thank Prof S. M. Husnine (NUCES, Lahore Campus) for his ceaseless encouragement and Prof. Ken Yamamura (National Defense Academy of Japan) for his *Bibliography on monogenity of orders of algebraic number fields*, *Dec. 2011, updated ed.*, [112 papers with MR# are included]. The second author is partially supported by grant (♯20540019) from the Japan Society for the Promotion of Science.

References

[1] Şabin Alaca and Kenneth S. Williams, *Introductory algebraic number theory*, Cambridge University Press, 2004, www.Cambridge.org/9780521832502.

[2] David S. Dummit and Hershy Kisilevsky, *Indices in cyclic cubic fields*, in: Number Theory and Algebra, Collection of Papers Dedicated to H. B. Mann. A. E. Ross and O. Taussky-Todd, Academic Press, New York/San Francisco/London, 1977, 29–42

[3] Takeo Funakura, *On integral bases of pure quartic fields*, Math. J. Okayama Univ., **26** (1984), 27–41

[4] István Gaál, *Diophantine equations and power integral bases*, New Computational Methods, Boston-Basel-Berlin, Birkhäuser, 2002.

[5] István Gaál, Michael Pohst and Peter Olajos, *Power integral bases in orders of composite fields*, Experiment. Math., **11(1)**(2002), 87–90

[6] Kálmán Győry, *Discriminant form and index form equations*, Algebraic Number Theory and Diophantine Analysis (F. Halter-Koch and R. F. Tichy. Eds.), Walter de Gruyter, Berlin-New York (2000), 191–214

[7] Abdul Hameed, Toru Nakahara, Syed. M. Husnine and Shahzad Ahmad, *On existence of canonical number system in certain classes of pure algebraic number fields*, J. Prime Research in Mathematics, **7** (2011), 19–24

[8] John A. Hymo and Charles J. Parry, *On Relative Integral Basis for Pure Quartic Fields*, Indian J. Pure appl. Math., **23(5)** (1992), 359–376

[9] J. G. Huard, Blair K. Spearman and Kenneth S. Williams, *Integral Bases for Quartic Fields with Quadratic Subfields*, J. Number Theory, **51** (1995), 87–102

[10] Yasuo Motoda, Toru Nakahara, Syed I. A. Shah and Tsuyoshi Uehara, *On a problem of Hasse for certain imaginary abelian fields*, RIMS Kôkyûroku Bessatsu, **B12** (2009) 209–221

[11] Władysław Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer-Verlag, Third edition, Berlin-Heidelberg-New York; PWM-Polish Scientific Publishers, Warszawa, 2007.

[12] Blair K. Spearman and Kenneth S. Williams, *Relative Integral Bases for Quartic Fields over Quadratic Subfields*, Acta Math. Hungar., **70(3)** (1996), 185–192

[13] Blair K. Spearman and Kenneth S. Williams, The index of cyclic quartic field, *Monatsh. Math.*, **140** (2003), 19–70

[14] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, Berlin-Heidelberg-New York; 1982

Received: 24.06.2014
Revised: 03.09.2015
Accepted: 05.09.2015

(1) National University of Computer Emerging Sciences,
Lahore Campus,
the Islamic Republic of Pakistan
E-mail: abdul.hameed@lhr.nu.edu.pk
(2) National University of Computer Emerging Sciences,
Peshawar Campus,
the Islamic Republic of Pakistan
E-mails: toru.nakahara@nu.edu.pk
toru.nakahara@qu.edu.pk