Punjab University
Journal of Mathematics (ISSN 1016-2526)
Vol. 50(3)(2018) pp. 67-73

# On the Monogenity of Cyclic Sextic Fields of Composite Conductor

Mushtaq Ahmad
National University of Computer & Emerging Sciences, Peshawar Campus
the Islamic Republic of Pakistan.
Email: p097001@nu.edu.pk

Abdul Hameed
National University of Sciences and Technology (NUST), Islamabad.
the Islamic Republic of Pakistan
Email: hameed.lamp@mcs.edu.pk

Nadia Khan
National University of Computer & Emerging Sciences, Lahore Campus.
the Islamic Republic of Pakistan.
Email: p109958@nu.edu.pk

Toru NAKAHARA
University of Peshawar, Khyber Pakhtunkhuwa.
the Islamic Republic of Pakistan
Email: toru.nakahara@nu.edu.pk

Received: 24 July, 2017 / Accepted: 20 December, 2017 / Published online: 10 April, 2018

**Abstract.** The aim of this paper is to determine the monogenity of the family of cyclic sextic composite fields $K \cdot k$ over the field $\boldsymbol{Q}$ of rational numbers, where $K$ is a cyclic cubic field of prime conductor $p$ and $k$ a quadratic field with the field discriminant $d_k$ such that $(p, d_k) = 1$. Examples of our theorems are compared with the experiments by PARI/GP.

**AMS (MOS) Subject Classification Codes: 11R04; 11R16; 11R18**
**Key Words:** Monogenity · Cyclic sextic field · Conductor · Simplest cubic field

## 1. Introduction

Let $L$ be an algebraic number field over the field $\boldsymbol{Q}$ of rational numbers of the extension degree $[L : \boldsymbol{Q}] = n$. Let $Z_L$ be the ring of integers in $L$. Then $Z_L$ has an integral basis $\{\alpha_j\}_{1 \leqq j \leqq n}$ such that $Z_L = \boldsymbol{Z} \cdot \alpha_1 + \cdots + \boldsymbol{Z} \cdot \alpha_n$ as a $\boldsymbol{Z}$-module of rank $n$, where $\boldsymbol{Z}$ denotes the ring of rational integers. We call it Dedekind-Hasse's problem to determine monogenity of a number field $L$. [5, 13, 17].

**Definition.** If there exists an integer $\xi$ in a field $L$ such that

$$Z_L = \boldsymbol{Z} \cdot 1 + \boldsymbol{Z} \cdot \xi + \cdots + \boldsymbol{Z} \cdot \xi^{n-1} = \boldsymbol{Z}[\xi],$$

then the ring $Z_L$ is said to have a power integral basis or the field $L$ is monogenic.

Let $k$ be a quadratic field $\boldsymbol{Q}(\omega)$ with $\omega = \frac{1+\sqrt{5}}{2}$ and $K$ the simplest cubic field $\boldsymbol{Q}(\eta)$ introduced by D. Shanks with a root $\eta$ of a cubic equation $x^3 = ax^2 + (a+3)x + 1$, where the discriminant $d_K(\eta)$ of a number $\eta$ is defined by
$((\eta - \eta^{\sigma})(\eta - \eta^{\sigma^2})(\eta^{\sigma} - \eta^{\sigma^2}))^2$ with a non-trivial Galois action $\sigma$ of $K/\boldsymbol{Q}$, which is equal to $(a^2 + 3a + 9)^2$, specifically $7^2$ for $a = -1$ [14]. Then $Z_k = \boldsymbol{Z}[\omega]$, $Z_K = \boldsymbol{Z}[\eta]$ and the composite sextic field $K \cdot k$ are monogenic. On the other hand, for the sextic field $L' = K \cdot k'$ with the Eisenstein field $k' = \boldsymbol{Q}(e^{\frac{2\pi i}{3}})$, the monogenity could not be prolonged into $L'$, namely there does not exist an integer $\xi$ in $L'$ such that the module index $[Z_L : Z[\xi]] = 1$.
In this paper, we consider a generalization of the monogenity for the family of cyclic sextic composite fields by a cyclic cubic field of prime conductor $p$ and a quadratic field of the field discriminant $q$ with $(p, q) = 1$.

## 2. THEOREMS

We claim Theorem 2.1 and Theorem 2.3.

**Theorem 2.1.** *Let $L$ be a cyclic sextic composite field $K \cdot k$, where $K$ is a cyclic cubic field $K$ of prime conductor $p$ and $k$ a quadratic field of the field discriminant $d_k$ such that $(p, d_k) = 1$. Then*
(1) *For a fixed quadratic field $k$, there exist at most finitely many monogenic sextic cyclic fields $L$.*
(2) *For a fixed cyclic cubic field $K$, there exist at most finitely many monogenic sextic cyclic fields $L$.*

The proof of this theorem is based on the evaluation modulo the ramified prime ideals in $K$ and $k$ for the identity (2.1) of the sum of three products of two partial differents

$$(\xi - \xi^{\sigma})(\xi - \xi^{\sigma})^{\tau} - (\xi - \xi^{\tau})(\xi - \xi^{\tau})^{\sigma} - (\xi - \xi^{\sigma\tau})(\xi - \xi^{\sigma\tau})^{\tau} = 0. \tag{2. 1}$$

of a candidate number $\xi$ of a power integral basis $Z_L = \boldsymbol{Z}[\xi]$ [12]. This involves the followings.

**Theorem 2.2** [18]. *Let $L$ be a cyclic sextic field $K \cdot k_5^+$, where $K$ is a simplest cubic field of prime conductor $p$ and $k_5^+$ the maximal real subfield of conductor $5$. Then only two sextic cyclic fields $k_7^+ \cdot k_5^+$ and $k_9^+ \cdot k_5^+$ are monogenic.*

This has been proved in [9].

**Theorem 2.3.** *Let $L$ be a cyclic sextic composite field $K \cdot k_4$, where $K$ is a simplest cubic field of prime conductor $p$ and $k_4$ the Gauß field of conductor $4$. Then only two sextic cyclic fields $k_7^+ \cdot k_4$ and $k_9^+ \cdot k_4$ are monogenic.*

*Proof of Theorem* 2.1. Let $G(K) =< \sigma >$ and $G(k) =< \tau >$ . Then it holds that $Z_L = Z_K \cdot Z_k$, where $Z_K = \boldsymbol{Z}[1, \eta, \eta^{\sigma}] = \boldsymbol{Z}[\eta, \eta^{\sigma}, \eta^{\sigma^2}]$ holds, where $\eta$ denotes the Gauß period $\sum_{\rho \in H_K} \zeta^{\rho}$ of length $(p-1)/6$ for the Galois group $H_K$ corresponding to the cubic subfield $K$ for a primitive $p$th root $\zeta$ of unity and $Z_k = \boldsymbol{Z}[1, \omega]$ with $\omega = \frac{d_k + \sqrt{d_k}}{2}$. From $(p, d_k) = 1$, we may assume that the ring $Z_L$ has a power integral basis $\boldsymbol{Z}[\xi]$ for an integer $\xi$ such that

$$\xi = \alpha + \beta\omega \ \text{ with } \ \alpha, \beta \in Z_K.$$

Since it holds that $N_{L/K}(\xi - \xi^{\tau}) = N_{L/K}(\alpha + \beta\omega - \alpha - \beta\omega^{\tau}) = \beta^2 d_k$, $\beta$ should be a unit in $K$ since $\beta$ is an integer. Thus it holds that $(\gamma - \gamma^{\sigma j})^2 \equiv 0 (\text{mod } \mathbb{P})$ for $\gamma \in Z_K$ with $\gamma = a\eta + b\eta^{\sigma} + c\eta^{\sigma^2}$, $a, b, c \in \boldsymbol{Z}$ and $\mathfrak{P} \cap K = \mathbb{P}$, where $\mathfrak{P}$ and $\mathbb{P}$ denote the ramified prime ideal in $k_p$ and $K$ respectively [10]. Then it is deduced that $N_L((\xi - \xi^{\sigma})(\xi - \xi^{\sigma^2})(\xi - \xi^{\tau}))$ $= \pm p^2 \cdot p^2 \cdot d_k^3$. We consider the fundamental relation (2.1) for the partial factors $\xi - \xi^{\rho}$ of the different $\mathfrak{d}_L(\xi)$.

(1) Since the three products in (2.1) are invariant by the action $\tau$, each of them belongs to $Z_K$. By $\xi - \xi^{\sigma} = \sum_{j=0}^{2} a_j(\eta^{\sigma^j} - \eta^{\sigma^{j+1}}) \equiv 0 (\text{mod } \mathfrak{P})$ and hence $(\xi - \xi^{\sigma})(\xi - \xi^{\sigma})^{\tau} \equiv 0 (\text{mod } \mathbb{P}^2)$, $\xi - \xi^{\tau} \cong \sqrt{d_k}$ and $(\xi - \xi^{\sigma\tau})(\xi - \xi^{\sigma\tau})^{\tau}$ should be a unit in $K$ by the assumption $Z_L = \boldsymbol{Z}[\xi]$. Here for $\alpha,\ \beta \in Z_F$ and an ideal $\mathfrak{A}$ in a field $F$, $\alpha \cong \beta$ or $\alpha \cong \mathfrak{A}$ means that both sides are equal to each other as ideals. Taking the norm from the cubic field $K$

$$N_K((\xi - \xi^{\sigma})(\xi - \xi^{\sigma})^{\tau} - (\xi - \xi^{\tau})(\xi - \xi^{\tau})^{\sigma}) = N_K((\xi - \xi^{\sigma\tau})(\xi - \xi^{\sigma\tau})^{\tau}), \quad (2.\ 2)$$

it follows that

$$d_k^3 \equiv \varepsilon (\text{mod } p) \text{ and hence } d_k^6 \equiv \pm 1 (\text{mod } p) \qquad (2.\ 3)$$

for a unit $\varepsilon$ in $k$. Then for a fixed quadratic subfield $k$, from (2.3) there exist at most finitely many monogenic sextic fields $L = K \cdot k$.

(2) Moreover by (2.2) it holds that

$$p \equiv \delta (\text{mod } d_k) \text{ and hence } p^2 \equiv \pm 1 (\text{mod } d_k) \qquad (2.\ 4)$$

for a unit $\delta$ in $k$. Then for a fixed cubic field $K$ of conductor $p$, from (2.4) there exist at most finitely many such monogenic sextic fields $L$. □

**Remark 2.1.** Let $k$ be the Gauß field and $\beta$ be a number $\frac{\alpha}{\alpha^{\tau}}$ with an integer $\alpha$ in $k \setminus \{\pm 1, \pm i, \pm 1 \pm i\}$. Then $N_k(\beta) = 1$, but $\beta$ is *not* a unit.

*Proof of Theorem* 2.3. By the formula (2.3) it follows that $-64 \equiv \pm 1$ or $\pm i$ $(\text{mod } p)$. Since $p$ is the conductor of a simplest cubic field, it deduces that $p = 7, 9$ or 13.

The case of $K = k_7^+$ of conductor 7. Put $\xi = \eta i$ and $\xi_{st} = \xi - \xi^{\sigma^s \tau^t}$. Then it holds that $\xi_{s0} = (\eta - \eta^{\sigma^s})i \cong \mathbb{P}$ and $\xi_{s1} = \eta i - \eta^{\sigma^s}(-i) = (\eta + \eta^{\sigma^s})i$ $(1 \leqq s \leqq 2)$. Since the Gauß period $\eta = \zeta_7 + \zeta_7^{-1}$ with $p = 7$ satisfies $f(x) = x^3 + x^2 - \frac{p-1}{3}x - \frac{cp+3p-1}{27}$ with $4p = c^2 + 27d^2$, $c \equiv 1 (\text{mod } 3), c > 0$, for $\eta_j = \eta^{\sigma j}$ $N_K(\eta_0 + \eta_1) = N_K(\eta_0)$

$+\sum_{0\leqq j\leqq 2}\eta_j\eta_{j+1}(\eta_j+\eta_{j+1}) + N_K(\eta_1) = 2N_K(\eta_0)+(-3N_K(\eta_0)) = -1$ [DK]. Then $\eta_0+\eta_j$ are units in $K$ for $1\leqq j\leqq 2$.

The case of $K=k_9^+=\boldsymbol{Q}(\eta)$. The Gauß period $\eta=\zeta_9+\zeta_9^{-1}$ satisfies $x^3-3x+1=0$. Put $\xi=\eta i$. Then $\xi_{j0}\cong\mathbb{P}$ and $\xi_{j1}=(\eta+\eta_j)i$. Then by $N_K(\eta+\eta^\sigma)=-N_K(\eta_0)=-(-1)$ $\eta_0+\eta_j$ are units in $K$. On the other hand, it holds that $\eta-\eta^\sigma=\zeta+\zeta^{-1}-(\zeta^2+\zeta^{-2})$ $=(1-\zeta)\zeta^{-2}(\zeta^3-1)\cong\mathfrak{P}\mathfrak{P}^3$, $\mathfrak{d}_L(\eta i)\cong(\eta-\eta^\sigma)(\eta^\sigma-\eta)^{\sigma^2})(\eta-\eta^\tau)\cong\mathfrak{P}^8(2i)$, and hence $d_{L/k}(\eta i)\cong\mathfrak{P}^{24}(2i)^3\cong 3^4(-2^3)$. Therefore it is deuced that $d_L\cong(3^4)^2(-2^3)^2$ $\cong d_K^{[L:K]}\cdot d_k^{[L:k]}=d_L$. Thus the sextic field $k_4\cdot k_9^+$ is monogenic.

The case of $K=\boldsymbol{Q}(\eta)$ of conductor $p=13$ with the Gauß period $\eta=\sum_{\rho\in\mathrm{Gal}(K/\boldsymbol{Q})}\zeta^\rho$, where $\eta$ satisfies $x^3+x^2-4x+1=0$. Assume that $Z_L=\boldsymbol{Z}[\xi]$ for a suitable integer $\xi=\alpha+\beta i$ in $L$ with $\alpha,\beta\in Z_K$. Then by $\xi-\xi^\sigma\equiv 0(\mathrm{mod}\ \mathfrak{d}_K)$ and $\xi-\xi^\tau\equiv 0(\mathrm{mod}\ \mathfrak{d}_k)$, $\xi-\xi^{\sigma\tau}$ should be a unit in $L$. However for the partial factor $\xi_{\sigma\tau}=\xi-\xi^{\sigma\tau}=\alpha+\beta i-(\alpha^\sigma+\beta^\sigma(-i))$, it should be deduced that $N_{L/K}(\xi_{\sigma\tau})=(\alpha-\alpha^\sigma)^2+(\beta+\beta^\sigma)^2=E$ with a unit $E$ in $K$. Put $\pi_\sigma=\alpha-\alpha^\sigma$ and $\beta_\sigma=\beta+\beta^\sigma$. Then $1=N_K(E)=N_K(N_{L/K}(\xi_{\sigma\tau}))$ $=(\pi_\sigma^2+\beta_{\sigma\tau}^2)(\pi_\sigma^2+\beta_{\sigma\tau}^2)^\sigma\ (\pi_\sigma^2+\beta_{\sigma\tau}^2)^{\sigma^2}\geqq 2^3\sqrt{(\pi_\sigma\beta_\sigma)(\pi_\sigma\beta_\sigma)^\sigma(\pi_\sigma\beta_\sigma)^{\sigma^2}}$ $=2^3\sqrt{N_K(\pi_\sigma)N_K(\beta_\sigma)}>2^3$ because of $\pi_\sigma\equiv 0(\mathrm{mod}\ \mathbb{P})$. This is a contradiction. Then the sextic field $k_4\cdot K$ is non-monogenic. □

**Remark 2.2.** On the family of cyclic sextic fields $L$ of prime power conductor, it is proved that there does not exist any monogenic field $L$ except for the three fields, the 7th cyclotomic field, 9th one and the maximal real subfield of 13th one [8].

## 3. Examples comparing experiments due to PARI/GP

Among several softwares for Mathematics, PARI/GP is an important tool to work in Number Theory and related areas [4]. It is a free software implemented by Université Bordeaux, France and can be used through MS Windows and Linux. Recently, (ex) PhD scholars in Pakistan have completed their main papers on Algebraic Number Theory [2, 6, 18, 15]. In the initial stage of their research and to verify the validity of claims, PARI/GP is making an indispensable role. Here we would show a prospective experiment, by which a new theorem will be developed and the related future work is proposed.

Let $K$ the simplest cubic field $\boldsymbol{Q}(\eta)$ introduced by D. Shanks with a root $\eta$ of a cubic equation $x^3=ax^2+(a+3)x+1$, where the discriminant $d_K(\eta)$ of a number $\eta$ is defined by $((\eta-\eta^\sigma)(\eta-\eta^{\sigma^2})(\eta^\sigma-\eta^{\sigma^2}))^2$, which is equal to $(a^2+3a+9)^2$, specifically $7^2$ for $a=-1$ [14]. Then $Z_k=\boldsymbol{Z}[\omega]$ and $Z_K=\boldsymbol{Z}[\eta]$ hold.

**Example 3.1.** In Theorem 2.2, let $L$ be the composite abelian sextic extension field $K\cdot k$, where $K$ is the simplest cubic field $\boldsymbol{Q}(\eta)$ of conductor 7 with the Gauß period $\eta$ and $k$ is a quadratic field $\boldsymbol{Q}(\omega)$ with $\omega=\frac{1+\sqrt{5}}{2}$. Then the monogenity of the subfield $K$

is lifted up to $L$. The sextic field $L$ is generated by $\xi = \eta\omega$, which satisfies $(\xi/\omega)^3 = -(\xi/\omega)^2 + 2(\xi/\omega) + 1$ namely
$\left\{\frac{(\xi^3-2\xi-1)^2}{-\xi^2+2\xi+2}\right\}^2 - \frac{\xi^3-2\xi-1}{-\xi^2+2\xi+2} - 1 = 0$ by $\xi^3 - 2\xi - 1 = \omega(-\xi^2 + 2\xi + 2)$ for $\omega = \frac{1+\sqrt{5}}{2}$.
We examine the fact for the sextic field $L$.

```
\\ Then PARI/GP gives a power integral basis
gp> nfbasis((x^3-2*x-1)^2-(x^3-2*x-1)*(-x^2+2*x+2)-(-x^2+2*x+2)^2)
%1=[1,x,x^2,x^3,x^4,x^5],
\\ the field discriminant d_{L} of the sectic field L
gp> nfdisc((x^3-2*x-1)^2-(x^3-2*x-1)*(-x^2+2*x+2)-(-x^2+2*x+2)^2)
%2=300125  \\ and the prime number decomposition of d_{L}
gp> factor(300125)
%3=[5 3], [7 4] \\ namely
d_{L}=5^3\cdot 7^4=d_{k}^{[L:k]}\cdot d_{K}^{[L:K]}
with d_{k}=5 and d_{K}=7^2.
```

Since the fields $K$ and $k$ are linearly disjoint, that is $K \cap k = \boldsymbol{Q}$ by $\gcd(d_K, d_k) = 1$. the ring $Z_L$ of the composite field $L$ coincides with $Z_K \cdot Z_k = \boldsymbol{Z}[1, \eta, \eta^2] \cdot \boldsymbol{Z}[1, \omega] = \boldsymbol{Z}[1, \eta, \eta^2, \omega, \eta\omega, \eta^2\omega]$. Thus for $\xi = \eta\omega$ the representation matrix $A$ of $\{1, \xi, \xi^2, \xi^3, \xi^4, \xi^5\}$ with respect to $\{1, \eta, \eta^2, \omega, \eta\omega, \eta^2\omega\}$ is equal to

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 2 & -1 & 2 & 4 & -2 \\ -2 & -2 & 6 & -3 & -3 & 9 \\ 9 & 15 & 12 & 15 & -25 & -20 \end{pmatrix}$$

which is equivalent to

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 2 & 0 & 2 & 0 & -1 \\ 0 & -2 & 0 & -3 & 0 & 3 \\ 0 & 15 & 0 & 15 & 0 & -8 \end{pmatrix}$$

and hence whose determinant is equal to 1, namely the matrix A belongs to $SL_6(\boldsymbol{Z})$.
Then our result and the output of PARI/GP coincide with each other.

**Example 3.2.** In Theorem 2.3, let $L''$ be the composite field $K \cdot k_4$ of the simplest cubic field $K = \boldsymbol{Q}(\eta)$ of conductor 7 and the Gauss field $k_4 = \boldsymbol{Q}(i)$. Then the ring of integers in $L''$ is generated by $\xi = \eta i$. Also PARI/GP gives a power integral basis by $\xi^3 + 2\xi = -i(\xi^2 + 1)$.

```
gp> nfbasis((x^3+2*x)^2+(x^2+1)^2)
%1=[1,x,x^2,x^3,x^4,x^5],
\\ the field discriminant d_{L^{\prime}} of
the sextic field L^{\prime\prime}
%% the sectic field L^{\prime}
gp> nfdisc((x^3-2*x-1)^2-(x^3-2*x-1)*(-x^2+2*x+2)-(-x^2+2*x+2)^2)
%2=300125  \\ and the prime number decomposition of d_{L}
gp> factor(-153664)
```

```
%3=[5 3], [7 4] \\ namely
d_{L^{\prime\prime}}=(-4)^3\cdot 7^4
=d_{k}^{[L^{\prime\prime}:k]}\cdot d_{K}^{[L^{\prime\prime}:K]}
with d_{k}=-4 and d_{K}=7^2.
```

Using the same notation as in the proof of Theorem 2.3, from $\mathfrak{d}_{L''}(\eta i) = (\eta i - \eta^{\sigma} i)(\eta i - \eta^{\sigma^2} i)(\eta i - \eta(-i))\,(\eta i - \eta^{\sigma}(-i))\,(-1)(\eta i - \eta^{\sigma}(-i))^{\sigma^2}$, it is deduced that $\mathfrak{d}_{L''} \cong \mathbb{P}\cdot\mathbb{P}\cdot 2i$. In fact, for $f(x) = x^3+x^2-2x-1 = (x-\eta)(x-\eta^{\sigma})(x-\eta^{\sigma^2})$ it holds that $(-2/2)\eta(-\eta - \eta^{\sigma})(\eta - \eta^{\sigma^2}) = (2/2)(\eta - 1)(\eta + 1) \cong 1$ by $f(-\eta) = \eta^3 + \eta^2 + 2\eta - 1 = 2(\eta^2 - 1)$, because of $f(1) = -1$ and $f(-1) = 1$. Thus each of the $4$th factor $(\eta i - \eta^{\sigma}(-i))$ and the $5$th $(-1)(\eta i - \eta^{\sigma}(-i))^{\sigma^2}$ of $\mathfrak{d}_{L''}(\eta i)$ is a unit in $L''$. Then our result coincides with the output of PARI/GP.

Based on the experiments, we propose future works.

• Characterize whether there exists a monogenic composite abelian field $L = K \cdot F$ of degree $[L : \boldsymbol{Q}] = 12$ or does not, where $K$ is a cyclic cubic field of prime conductor $p$ and $F$ a biquadratic field $\boldsymbol{Q}(\sqrt{d_q}, \sqrt{d_\ell})$ with $(p,\ d_q \cdot d_\ell) = 1$ Here $d_q$ and $d_\ell$ with $(d_q, d_\ell) = 1$ denote the field discriminants of quadratic fields $\boldsymbol{Q}(\sqrt{d_q})$ and $\boldsymbol{Q}(\sqrt{d_\ell})$, respectively [12, 8, 1].

• Applying the monogenic property of an algebraic number field, investigate an excellent code in the Coding Theory [16].

## References


[1] S. Ahmad, T. Nakahara and A. Hameed, *On certain pure sextic fields related to a problem of Hasse*, International Journal of Algebra and Computation **26**, No. 3 (2016) 577–583. DOI: 10.1142/S0218196716500259.

[2] S. Ahmad, T. Nakahara and S. M. Husnine, *On Power Bases for Certain Pure Sextic Fields*, International Journal of Number Theory (Singapore **10**, No. 8 (2014) 2257–2265. DOI: 10.1142/S1793042114500778.

[3] D. Dummit and H. Kisilevsky, *Indices in cyclic cubic fields in: Number Theory and Algebra*, Collection of Papers Dedicand O. Taussky-Todd, Academic Press, New York/San Francisco/London, (1977) 29-42.

[4] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, Springer-Verlag, Berlin, **138**, (1993) xii+534 pp. 1996(3rd corrected printing).

[5] I. Gaál, *Diophantine equations and power integral bases, new computational methods*, Birkhäuser Boston, Inc.,Boston, 2002.

[6] A. Hameed and T. Nakahara, *Integral bases and relative monogenity of pure octic fields*, Bull. Math. Soc. Sci. Math. Roumanie **58**, No. 4 (2015) 419–433.

[7] N. Khan, S.-i. Katayama, T. Nakahara and T. Uehara, *Monogeneity of totally real algebraic extension fields over a cyclotomic field*, J. of Number Theory, **158**, (2016) 348–355.

[8] N. Khan and T. Nakahara, *On cyclic sextic fields of prime power conductor related a problem of Hasse*, submitted.

[9] N. Khan, S.-i. Katayama, T. Nakahara and H. Sekiguchi, *The Gauß Sum and its Application to Number Theory*, Accepted in J. of Basic and Applied Sciences.

[10] H.-W. Leopoldt, *Uber die Hauptordnung der ganzen Elemente eienes abelishen Zahlkörpers*, J. Reine Angew. Math. **201**, (1959) 119-149.

[11] Y. Motoda, S. Inayat A. Shah and T. Nakahara, *On a Problem of Hasse for Certain Imaginary Abelian Fields*, J. of Number Theory, **96**, No. 2 (2002) 326-334.

[12] Y. Motoda and T. Nakahara, *Power integral bases in algebraic number fields whose galois groups are* $2$*-elementary abelian*, Archiv der Mathematik, Basel **83**, (2004) 309–316.

[13] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer-Verlag, $3^{\mathrm{rd}}$ ed. Berlin-Heidelberg-New York; PWM-Polish Scientific Publishers, Warszawa 2007.

[14] D. Shanks, *The simplest cubic fields*, Mathematics of Computation, **28**, No. 128 (1974) 1137–1152.

[15] M. Sultan and T. Nakahara, *On certain octic biquartic fields related to a problem of Hasse*, Monatshefte für Mathematik **176**, No. 1 (2015) 153–162, DOI 10.1007/s00605—014-0670-y.

[16] T. Uehara and K. H. Park, *Construction of evaluation codes from Hermitian curves*, Kyushu J. Math. **61**, No. 2 (2007) 415–429.

[17] K. Yamamura, *Bibliography on monogenity for the ring of integrs in algebraic number fields*, Up to dated in August, 2015, 135 papers are included.

[18] M. Sultan, Y. Kôhno and T. Nakahara, *Monogenity of Biquadratic Fields Related to Dedekind-Hasse's Problem*, Punjab Univ. j. math. **47**, No. 2 (2015) 77-82.