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 $\mathbb{Q}$ 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 $\mathbb{Q}$ of rational numbers of the extension degree $[L : \mathbb{Q}] = n$. Let $\mathcal{O}_L$ be the ring of integers in $L$. Then $\mathcal{O}_L$ has an integral basis $\{\alpha_j\}_{1 \leq j \leq n}$ such that $\mathcal{O}_L = \mathbb{Z} \cdot \alpha_1 + \cdots + \mathbb{Z} \cdot \alpha_n$ as a $\mathbb{Z}$-module of rank $n$, where $\mathbb{Z}$ 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
$$Z_L = Z \cdot 1 + Z \cdot \xi + \cdots + Z \cdot \xi^{n-1} = Z[\xi],$$
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 $\mathbb{Q} (\omega)$ with $\omega = 1 + \sqrt{5}$ and $K$ the simplest cubic field $\mathbb{Q} (\eta)$ 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

$$(\eta - \eta^\tau)(\eta - \eta^\sigma)(\eta^\sigma - \eta^\tau^2))^2$$
with a non-trivial Galois action $\sigma$ of $K/\mathbb{Q}$, which is equal to $(a^2 + 3a + 9)^2$, specifically $7^2$ for $a = -1$ [14]. Then $Z_k = Z[\omega]$, $Z_K = Z[\eta]$ 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 $k' = \mathbb{Q}(e^{2\pi i/3})$, 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 different

$$(\xi - \xi^\sigma)(\xi - \xi^\sigma^\tau) - (\xi - \xi^\tau)(\xi - \xi^\sigma)(\xi - \xi^\tau^\sigma)(\xi - \xi^\sigma^\tau)^\tau = 0.$$  \hspace{1cm} (2.1)

of a candidate number $\xi$ of a power integral basis $Z_L = Z[\xi]$ [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 $k^+_5 \cdot k^+_5$ and $k^+_5 \cdot k^+_5$ 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 $k_2^+ \cdot k_4$ and $k_3^+ \cdot k_4$ are monogenic.

Proof of Theorem 2.1. Let $G(K) = \leq \sigma >$ and $G(k) = \leq \tau >$. Then it holds that $Z_L = Z_K \cdot Z_k$, where $Z_K = Z[1, \eta, \eta^\sigma] = Z[\eta, \eta^\sigma, \eta^\sigma^2]$ holds, where $\eta$ denotes the Gauß period $\sum_{\rho \in H_K} (\rho^p)^{\leq 0}$ 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 $Z_k = Z[1, \omega]$ with $\omega = \frac{d_{\eta} + \sqrt{\Delta_k}}{2}$. From $(p, d_k) = 1$, we may assume that the ring $Z_L$ has a power integral basis $Z[\xi]$ for an integer $\xi$ such that

$$\xi = \alpha + \beta \omega \text{ with } \alpha, \beta \in \mathbb{Z}_K.$$ 

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

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

$$N_{K}((\xi - \xi^T)(\xi - \xi^T)^T - (\xi - \xi^T)(\xi - \xi^T))^T = N_{K}((\xi - \xi^T)(\xi - \xi^T)^T)^T, \quad (2.2)$$

it follows that

$$d_k^2 \equiv \epsilon \pmod{p} \text{ and hence } d_k^2 \equiv \pm 1 \pmod{p} \quad (2.3)$$

for a unit $\epsilon$ 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

$$p \equiv \delta \pmod{d_k} \text{ and hence } p^2 \equiv \pm 1 \pmod{d_k} \quad (2.4)$$

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 $L$. \hfill \square

Remark 2.1. Let $k$ be the Gauß field and $\beta$ be a number $\frac{\alpha}{\alpha}$ 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 $-64 \equiv \pm 1 \pmod{p}$. Since $p$ is the conductor of a simplest cubic field, it deduces that $p = 7, 9$ or 13.

The case of $K = k_2^+$ of conductor 7. Put $\xi = \eta$ and $\xi_{st} = \xi - \xi^\sigma \cdot T$. Then it holds that $\xi_{s0} = (\eta - \eta^\sigma) i \equiv P$ and $\xi_{s1} = \eta - \eta^\sigma (-i) = (\eta + \eta^\sigma^2) i (1 \leq s \leq 2)$. Since the Gauß period $\eta = \zeta_7 + \zeta_7^{-1}$ with $p = 7$ satisfies $f(x) = x^3 + x^2 - \frac{4}{\zeta_7}x + \frac{4}{\zeta_7^2}$ with $4p = c^2 + 27d^2, c \equiv 1 \pmod{3}, c > 0$, for $\eta_j = \eta^\sigma_j N_K(\eta_0 + \eta_1) = N_K(\eta_0)$
where $K$ will be developed and the related future work is proposed. Example 3.1. In Theorem 2.2, let $L$ be the composite abelian sextic extension field $K \cdot k$ of conductor 7 with the Gauß period $\eta$ and $k$ is a quadratic field $Q(\omega)$ with $\omega = \frac{1 + \sqrt{5}}{2}$. Then the monogeny of the subfield $K$.

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 $K$ be the simplest cubic field $Q(\eta)$ 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 $((\eta - \eta^\sigma)(\eta - \eta^\sigma^\tau)(\eta^\sigma - \eta^\sigma^\tau))^2$, which is equal to $(a^2 + 3a + 9)^2$, specifically $7^2$ for $a = -1$ [14]. Then $Z_k = Z[\omega]$ and $Z_K = Z[\eta]$ hold.

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

\[
\begin{align*}
\left\{ \begin{array}{l}
\xi^3 - 2\xi - 1 \\
-\xi^2 + 2
\end{array} \right\} = 0 \quad \text{by} \quad \xi^3 - 2\xi - 1 = \omega(-\xi^2 + 2\xi + 2) \quad \text{for} \quad \omega = \frac{1+\sqrt{5}}{2}.
\end{align*}
\]

We examine the fact for the sextic field \( L \).

\[
\text{Then PARI/GP gives a power integral basis}
\]

\[
gp> \text{nfbasis}((x^3-2*x-1)^2-(x^3-2*x-1)*(x^2+2*x+2)-(x^2+2*x+2)^2)
\]

\[
%1=[1,x,x^2,x^3,x^4,x^5],
\]

\[
\text{the field discriminant} \ d_{L} \ \text{of the sextic field} \ L
\]

\[
gp> \text{nfdisc}((x^3-2*x-1)^2-(x^3-2*x-1)*(x^2+2*x+2)-(x^2+2*x+2)^2)
\]

\[
%2=300125 \ \text{\ and the prime number decomposition of} \ d_{L}
\]

\[
gp> \text{factor}(300125)
\]

\[
%3=[5 3], \ [7 4] \ \text{\ namely}
\]

\[
d_{L}=5^3\cdot 7^4=d_{k}^{[L:k]}\cdot d_{K}^{[L:K]}
\]

\[
\text{with} \ d_{k}=5 \ \text{and} \ d_{K}=7^2.
\]

Since the fields \( K \) and \( k \) are linearly disjoint, that is \( K \cap k = Q \) by \( \gcd(d_{K}, d_{k}) = 1 \), the ring \( Z_{L} \) of the composite field \( L \) coincides with \( Z_{K} \cdot Z_{k} = Z[1, \eta, \eta^2, \omega, \eta \omega, \eta^2 \omega] \). 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

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

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 \( SL_6(Z) \).

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 \( K = Q(\eta) \) of conductor 7 and the Gauss field \( k_4 = Q(i) \). Then the ring of integers in \( L'' \) is generated by \( \xi = \eta i \). Also PARI/GP gives a power integral basis by \( \xi^3 + 2\xi = -i(\xi^2 + 1) \).

\[
gp> \text{nfbasis}((x^3+2*x)^2+(x^2+1)^2)
\]

\[
%1=[1,x,x^2,x^3,x^4,x^5],
\]

\[
\text{the sextic field} \ L'' \ \text{of} \ L
\]

\[
gp> \text{nfdisc}((x^3-2*x-1)^2-(x^3-2*x-1)*(x^2+2*x+2)-(x^2+2*x+2)^2)
\]

\[
%2=300125 \ \text{\ and the prime number decomposition of} \ d_{L}
\]

\[
gp> \text{factor}(-153664)
\]
Applying the monogenic property of an algebraic number field, investigate the field discriminants of quadratic fields $\Delta_{Q} = \Delta_{K} = -4$ and $\Delta_{K} = 7^{2}$. Using the same notation as in the proof of Theorem 2.3, from $\Delta_{L''}(\eta_{i}) = (\eta_{i} - \eta_{i}^{2})(\eta_{i}^{2} - \eta_{i}^{3}i)(\eta_{i}^{2} - \eta_{i}^{3})(-1)(\eta_{i}^{2} - \eta_{i}^{3})(-i))^{2}$, it is deduced that $\Delta_{L''} \cong P \cdot P^{2}$. In fact, for $f(x) = x^{3} + x^{2} - 2x - 1 = (x - \eta)(x - \eta^{2})(x - \eta^{3})$, it holds that $(-2/2)\eta(-\eta - \eta^{2})(\eta - \eta^{2}) = (2/2)(\eta + 1) \cong 1$ 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 4th factor $(\eta_{i} - \eta^{2}(-i))$ and the 5th $(\eta_{i} - \eta^{2}(-i))^{2}$ of $\Delta_{L''}(\eta_{i})$ 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 $[L : Q] = 12$ or does not, where $K$ is a cyclic cubic field of prime conductor $p$ and $F$ a biquadratic field $Q(\sqrt{d_q}, \sqrt{d_l})$ with $(p, d_q \cdot d_l) = 1$. Here $d_q$ and $d_l$ with $(d_q, d_l) = 1$ denote the field discriminants of quadratic fields $Q(\sqrt{d_q})$ and $Q(\sqrt{d_l})$, respectively [12, 8, 1].

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

REFERENCES


