On a Problem of Hasse

By

Yasuo MOTODA*, Toru NAKAHARA1)** Syed Inayat Ali SHAH*** and
Tsuyoshi UEHARA1)†

Abstract

In this article we shall construct a new family of cyclic quartic fields $K$ with odd composite conductors, which give an affirmative solution to a Problem of Hasse(Problem 6 in [12, p. 529]); indeed our family consists of cyclic quartic fields whose ring $Z_K$ of integers are generated by a single element $\xi$ over $\mathbb{Z}$. We will find an integer $\xi$ in $K$ by the two different ways; one of which is based on an integral basis of $Z_K$ and the other is done on a field basis of $K$.

§1. Introduction

In the year 1966, Hasse’s problem was brought to Kyushu Univ. in Japan from Hamburg by K. Shiratani. Let $K$ be an algebraic number field of degree $n$ over the rationals $\mathbb{Q}$. Let $Z$ denote the ring of integers. It is called Hasse’s problem to characterize whether the ring $Z_K$ of integers in $K$ has a generator $\xi$ as $\mathbb{Z}$-free module, namely $Z_K$ coincides with

$$Z[1, \xi, \cdots, \xi^{n-1}],$$

which we denote by $Z[\xi]$. If $Z_K = Z[\xi]$, it is said that $Z_K$ has a power integral basis; it is also said that $K$ is monogenic. In this article, we consider the case of cyclic quartic...
fields $K$ with composite conductors over $Q$. In the case of cyclic quartic field $K$ with a prime conductor, $Z_K$ has no power integral basis except for $K = k_5$ or the maximal real subfield of $k_{16}$ as is shown by one of the author in [11]. Here, $k_n$ means the $n$-th cyclotomic field over $Q$. On the contrary, infinitely many monogenic cubic or biquadratic Dirichlet fields are found by D. S. Dummit - H. Kisilevsky in [1] and Y. Motoda in [6, 7]. In the case of biquadratic fields, M.-N. Gras - F. Tanoé [4] gave a necessary and sufficient condition for the fields to be monogenic. If $K$ is 2-elementary abelian extension of degree not less than 8, we proved in [8, 15] that $Z_K$ does not have any power integral basis except for the 24-th cyclotomic field $k_{24} = Q(\zeta_{24})$, which coincides with

$$Q(\zeta_4, \zeta_3, \zeta_8 + \zeta_8^{-1}),$$


§ 2. New examples of monogenic cyclic quartic fields based on integral bases of their rings of integers

A quarter of century ago, we found several monogenic cyclic quartic fields $K = Q(\eta)$ of composite conductor $D$ over $Q$ in [N1]. This result was obtained when we restricted ourselves to the associated Gaú period $\eta_X$ of $\varphi(D)$/4 terms with the character $\chi$ as a generator $\xi$ of $Z_K = Z[\xi]$, where $\chi = \chi_D$ is the quartic character with conductor $D$ and $\varphi(\cdot)$ denotes Euler’s function. We calculated the group index $[Z_K : Z[\xi]] = \sqrt{\frac{d_K(\xi)}{d_K}}$ of a number $\xi$ under the integral basis $\{1, \eta_X, \eta_X^\sigma, \eta_X^{\sigma^2}\}$, i.e., nearly the normal basis of $K/Q$, where $d_F, d_F(\alpha)$ and $\sigma$ denote the field discriminant of a field $F$, the discriminant of a number $\alpha$ with respect to $F/Q$ and a generator of the Galois group of $K/Q$, respectively.

In this section, we use a different integral basis from the previous one and seek a candidate $\xi$ of a generator of $Z_K$ using a linear combination of certain partial differenters of $\xi$. First we consider examples. Let $k_{15}$ be the cyclotomic field with conductor $5 \cdot \{-3\}$. Then all the proper subfields consists of three quartic fields $K_j$ and three quadratic ones $L_j$ (1 $\leq j \leq 3$), namely $K_1 = k_5, K_2 = Q(\sqrt{5}, \sqrt{-3}), K_3 = Q(\zeta_{15} + \zeta_{15}^{-1}), L_1 = Q(\sqrt{5}), L_2 = Q(\sqrt{-3}), L_3 = Q(\sqrt{-15})$. In the biquadratic field $K_2$, a prime number 2 remains prime in its subfield $L_1$. Then using Lemma 2, we see that $K_2$ is non-monogenic. The other five subfields are monogenic by [18]. Next we take the cyclotomic field $k_{371}$ with
On a Problem of Hasse

This field has three quartic subfields $K_j$ ($1 \leq j \leq 3$);

$$K_1 = \mathbb{Q}(\eta_{\chi_{53}}), \quad K_2 = \mathbb{Q}(\sqrt{53}, \sqrt{-7}), \quad K_3 = \mathbb{Q}(\eta_{\chi_{371}}).$$

In the field $K_2$, since 2 remains prime in the quadratic subfield $\mathbb{Q}(\sqrt{53})$ and is decomposed in $\mathbb{Q}(\sqrt{-7})$, i.e., its relative degree $f_{K_2}$ with respect to $K_2/\mathbb{Q}$ is 2, we see by Lemma 2 that $K_2$ is non-monogenic. However, since the relative degree $f_{K_1}$ with respect to $K_1/\mathbb{Q}$ is 4, we could not use Lemma 2 for $K_1$. Since the conductor of $K_1$ is a prime $> 5$, $K_1$ is also non-monogenic by the former work [11]. Now we shall show that $K_3$ is monogenic and this is a new example, which was not obtained by the previous method in [10].

Let $D = dd_1$ be a square free odd integer with $d = a^2 + 4b^2 \equiv -d_1 \equiv 1 \pmod{4}$ and $d = \prod_{j=1}^{r} p_j$ and $d_1 = \prod_{k=1}^{s} q_k$, the canonical factorizations of $d$ and $d_1$, respectively. Let $\delta = \prod_{j=1}^{r} \pi_j$ be the prime decomposition of a factor $\delta = a + 2bi$ of $d$ with $i = \sqrt{-1}$ in $k_4$, where $p_j = \pi_j \cdot \overline{\pi_j}$, $d = \delta \cdot \overline{\delta}$; here $\overline{\alpha}$ denotes the complex conjugate of $\alpha \in k_4$. Let $G$ be the Galois group of the cyclotomic extension $k_D/\mathbb{Q}$. We identify the group $G$ with the reduced residue group modulo $D$. Let $\chi_p(x) = \left(\frac{x}{\pi_j}\right)_4$ be a pure quartic character with conductor $p_j$ for $x \in G$, where $\left(\frac{x}{\pi_j}\right)_4$ means the quartic residue symbol modulo $\pi_j$ with normalized $\pi_j \equiv 1 \pmod{(1-i)^3}$ ($1 \leq j \leq r$). Then the quartic character $\chi_d$ is defined by $\prod_{j=1}^{r} \chi_{p_j}$, Let $\psi_{d}$ and $\psi_{d_1}$ denote the quadratic characters $\chi_d^2$ and $\prod_{k=1}^{s} \psi_{q_k}$ for the quadratic character $\psi_{q_k}$ with conductor $q_k$, respectively. Then $\chi = \chi_d \psi_{d_1}$ is a quartic character with conductor $dd_1$. Let $\tau(\chi) = \sum_{x \in G} \chi(x)\zeta_D^x$ be the Gauß sum attached with $\chi$. From the norm relation of the Gauß sum, Jacobi sum and the decomposition of $\tau(\chi)$, we have

$$\tau(\chi_p)\tau(\overline{\chi}_p) = \chi_p(-1)p,$$

$$\tau(\chi_p)^2/\tau(\chi_p^2) = -\chi_p(-1)\pi_p,$$

$$\tau(\chi) = \left(\prod_{j=1}^{r} \chi_{p_j}(d/p_j)\right) \left(\prod_{k=1}^{s} \psi_{q_k}(d_1/q_k)\right) \left(\prod_{j=1}^{r} \tau(\chi_{p_j})\right) \left(\prod_{k=1}^{s} \tau(\psi_{q_k})\right),$$

where $\overline{\chi}_p$ denotes the complex conjugate character of $\chi_p$. Then we can derive for $d = \delta \cdot \overline{\delta}$,
\[ \delta \equiv 1 \pmod{(1-i)^3}, \]
\[
\tau(\chi)\tau(\bar{\chi}) = \chi(-1)dd_1 = (-1)^sdd_1, \\
\tau(\chi)^2 = (-1)^{r+s}\psi_d(d_1)\delta d_1\sqrt{d}, \\
\tau(\chi^2) = (-1)^s\psi_d(d_1)\sqrt{d}. 
\]

Let \( H \) be the kernel of \( \chi \). Then the residue class group \( G/H \) is isomorphic to a cyclic subgroup \( < \chi > \) of order 4 of the character group \( X \) of \( G \). Let \( K \) denote the subfield of \( k_D \) associated with \( < \chi > \). Then we have \( K = Q(\eta) \).

**Lemma 2.1.** Being the same notation as above, it holds that
\[ Z_K = Z[1, \eta, \eta^\sigma, \eta^{\sigma^2}] = Z[1, \eta, \eta^\sigma, \eta + \eta^{\sigma^2}]. \]

**Proof.** Since the set \( \{ \eta, \eta^\sigma, \eta^{\sigma^2}, \eta^{\sigma^3} \} \) forms a normal basis of \( Z_K \), we have \( Z_K = Z[1, \eta, \eta^\sigma, \eta^{\sigma^2}] \) by \((-1)^{r+s} = \eta + \eta^\sigma + \eta^{\sigma^2} + \eta^{\sigma^3}\). Applying a suitable special linear transformation to a basis \( \{1, \eta, \eta^\sigma, \eta^{\sigma^2}\} \), we obtain the basis \( \{1, \eta, \eta^\sigma, \eta + \eta^{\sigma^2}\} \). \( \square \)

Now, we choose the integral basis \( \{1, \eta, \eta + \eta^{\sigma^2}, \eta^\sigma\} \) because the number \( \eta + \eta^{\sigma^2} \\
\{((-1)^{r+s} + \tau(\chi) + \tau(\chi^2) + \tau(\bar{\chi}))/4 \\
\tau(\chi)^\sigma = -i\tau(\chi), \quad \tau(\chi^2)^\sigma = -\tau(\chi^2), \quad \tau(\chi)^\sigma = i\tau(\chi).
\]

\[
Z_K = Z[1, \eta, \eta^\sigma, \eta^{\sigma^2}] = Z[1, \eta, \eta^\sigma, \eta + \eta^{\sigma^2}]. 
\]

By \( d_K = N_K(\mathfrak{d}_K) \), where \( f_\rho \) denotes the conductor of a character \( \rho \).

By \( \mathfrak{d}_K(\xi) = (\xi - \xi^\sigma)(\xi - \xi^{\sigma^2})(\xi - \xi^{\sigma^3}) \) we have
\[
\pm d_K(\xi) = N_K(\mathfrak{d}_K(\xi)) \\
= (\xi - \xi^\sigma)(\xi - \xi^{\sigma^2})(\xi - \xi^{\sigma^3}) \\
\times (\xi^\sigma - \xi^{\sigma^2})(\xi^\sigma - \xi^{\sigma^3})(\xi^\sigma - \xi) \\
\times (\xi^{\sigma^2} - \xi^{\sigma^3})(\xi^{\sigma^2} - \xi)(\xi^{\sigma^2} - \xi^\sigma) \\
\times (\xi^{\sigma^3} - \xi)(\xi^{\sigma^3} - \xi^\sigma)(\xi^{\sigma^3} - \xi^{\sigma^2}) \\
= \{(\xi - \xi^\sigma)(\xi - \xi^{\sigma^2})(\xi - \xi^{\sigma^3})\}^2 \{(\xi - \xi^{\sigma^2})(\xi - \xi^{\sigma^3})(\xi - \xi^\sigma)\}^2 \{(\xi - \xi^\sigma)(\xi - \xi^{\sigma^2})(\xi - \xi^{\sigma^3})\}^2 \sigma. 
\]
Here, we select $\xi = x\eta + z(\eta + \eta\sigma^2)$ with $y = 0$ and put

$$I = N_{K/k}(\mathfrak{d}_{K/k}(\xi)) = -(\xi - \xi\sigma^2)^2, \quad J = N_{K/k}(\mathfrak{d}_k(\xi)) = (\xi - \xi\sigma)(\xi - \xi\sigma)^2.$$  

Then it follows that $I = x^2(\eta - \eta\sigma^2)^2$. On the other hand, by the transitive law of the field different for $K \supset k \supset \mathbb{Q}$, we have

$$\mathfrak{d}_K = \mathfrak{d}_{K/k}\mathfrak{d}_k,$$

where $\mathfrak{d}_{K/k}$ is the relative different with respect to $K/k$, namely

$$\mathfrak{d}_{K/k} = <\alpha - \alpha\sigma^2; \forall \alpha \in \mathcal{O}_K>.$$

Thus, by $N_K(\mathfrak{d}_K) = N_K(\mathfrak{d}_{K/k})N_K(\mathfrak{d}_k)$, $N_K(\mathfrak{d}_K) = d_K = d^3d_1^2$ and $N_k(\mathfrak{d}_k) = d$, we obtain $N_K(\mathfrak{d}_{K/k}) = dd_1^2$, namely the relative discriminant

$$d_{K/k} \cong N_{K/k}(\mathfrak{d}_{K/k}) \cong \sqrt{d}d_1.$$

Here $\alpha \cong \beta$ means that both sides are equal to each other as ideals. Then

$I = x^2d_1\sqrt{d} \gamma$ for some integer $\gamma \in k$. Since the ‘obstacle’ factor $x^2\gamma$ should disappear, we have $x = \pm 1$. By virtue of $N_{K}(\mathfrak{d}_k(\xi))^2 \equiv 0 \pmod{d_K/d_{K/k}^2}$ and $d_K/d_{K/k}^2 = d_K/d_{K/k}^2 = d$, we obtain $J \equiv \mathfrak{d}_k(\xi)\mathfrak{d}_k(\xi)^{\sigma} \equiv 0 \pmod{\sqrt{d}}$. Next we consider the following linear relation of three partial differentials;

$$N_{K/k}(\mathfrak{d}_k(\xi)) - N_k(\mathfrak{d}_{K/k}(\xi)) - N_{K/k}(\mathfrak{d}_k(\xi)^{\sigma^{-1}}) = 0,$$

namely,

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

For $\xi$ to satisfy $\mathcal{O}_K = \mathbb{Z}[\xi]$, there must be such units $\epsilon_j$ in $k$ as

$$\epsilon_1\sqrt{d} + \epsilon_2\sqrt{dd_1} + \epsilon_3\sqrt{d} = 0.$$  

Here by $N_{K/k}(\mathfrak{d}_k(\xi)) = \mathfrak{d}_k(\xi)\mathfrak{d}_k(\xi)^{\sigma} \cong \sqrt{dd_1}$, we have $N_k(\mathfrak{d}_{K/k}(\xi)) = \mathfrak{d}_{K/k}(\xi)\mathfrak{d}_{K/k}(\xi)^{\sigma} \cong \sqrt{dd_1}$, because, for a ramified ideal $\mathfrak{L}$ in $K$, i.e., $\mathfrak{L}|dd_1$, $\mathfrak{L}^\sigma = \mathfrak{L}$ holds. Then we get

$$\begin{cases}
\epsilon_1 + \epsilon_2d_1 + \epsilon_3 = 0, \\
\bar{\epsilon}_1 + \bar{\epsilon}_2d_1 + \bar{\epsilon}_3 = 0,
\end{cases}$$

where $\bar{\epsilon}$ for $\epsilon \in k$ means the real conjugate of $\epsilon$ with respect to $K/\mathbb{Q}$. When we consider the simultaneous equation $(\ast)_0$ with coefficients $\epsilon_j, \bar{\epsilon}_j$, under the assumption that the rank of $(\ast)_0$ would be equal to 1, then we have $1 \pm d_1 \pm 1 = 0$, which is impossible by
$d_1 \geq 3$. Then the rank of $(*)_0$ is equal to 2. Without loss of generality, we may consider the equations dividing both sides of $(*)_0$ by $\epsilon_2$;

\[
(*) \quad \begin{cases}
    \epsilon_1 \cdot 1 + 1 \cdot d_1 + \epsilon_3 \cdot 1 = 0, \\
    \overline{\epsilon}_1 \cdot 1 + 1 \cdot d_1 + \overline{\epsilon}_3 \cdot 1 = 0,
\end{cases}
\]

with units $\epsilon_j = \frac{v_j + u_j\sqrt{d}}{2}$ in $k$. Thus we have the ratios

\[
1 : d_1 : 1 = \begin{vmatrix}
    \epsilon_3 \\
    \overline{\epsilon}_3 \\
    \epsilon_1 \\
    \overline{\epsilon}_1
\end{vmatrix}.
\]

Then by $1 : 1 = \overline{\epsilon}_3 - \epsilon_3 : \epsilon_1 - \overline{\epsilon}_1 = -u_3 : -u_1$ and $d_1 : 1 = \epsilon_3\overline{\epsilon}_1 - \overline{\epsilon}_3\epsilon_1 : \epsilon_1 - \overline{\epsilon}_1 = (v_3(-u_1) + u_3v_1)/2 : u_1$, we obtain $d_1 = -(v_3 + v_1)/2$. Since $\epsilon_3 = (v_3 + u_3\sqrt{d})/2$, $\epsilon_1 = (v_1 + u_1\sqrt{d})/2$ and $-u_3 = u_1$, we have $v_3 = \pm v_1$, and hence $v_3 = v_1$ by $d_1 \neq 0$. Then $d_1 = -v_1$. Thus $N_k(\epsilon) = (d_1^2 - u_1^2d)/4 = \pm 1$, namely $d_1^2 \pm 4 = u_1^2d$ holds. From $\mathfrak{d}_k(\xi) = (2z + (-1)^s\psi_{d_1}(d)\sqrt{d})/2 + (1 + i)\tau(\chi) + (1 - i)\tau(\overline{\chi})/4$, it follows that

\[
J = N_{K/k}(\mathfrak{d}_k(\xi)) = \mathfrak{d}_k(\xi)\mathfrak{d}_k(\xi)^{\sigma^2} = (2z \pm 1)^2d/4 - \{2i(\pm \sqrt{d})^{\pm 1}/4\} \sqrt{d}.
\]

Here we conclude that $(2z \pm 1)^2 \pm d_1$ is equal to $(2z \pm 1)^2 - d_1$, because $J$ is an integer in $k$. We choose $b = 1$ and the number $(2z \pm 1)^2 \pm 2$ as $d_1$. Then for $\varepsilon = (\pm d_1 \pm \sqrt{d})/2$ we see that $N_k(\varepsilon) = -1$, namely that $\varepsilon$ is a unit in $k$. Thus for square free numbers $d_1 = (2z + 1)^2 \pm 2$ and $d = d_1^2 + 4$, we obtain

\[
d_K(\xi) \cong N_K(\mathfrak{d}_K(\xi)) = (2z \pm 1)^2d_1^2 = d_1^2 + 4.
\]

where $I = N_{K/k}(\mathfrak{d}_K/k(\xi))$, $J = N_{K/k}(\mathfrak{d}_k(\xi))$ and $\sigma^2 Gal(K/Q) = Gal(K/Q)$. Therefore we verified the following Theorem.
Theorem 2.2. Let \( d_1 = (z + 1)^2 \pm 2 \) \( (z \in \mathbb{Z}) \) and \( d = d_1^2 + 4 \) be square free integers. Then the cyclic quartic field \( K = \mathbb{Q}(\eta) \) with conductor \( dd_1 \) is monogenic; namely its ring \( \mathbb{Z}_K \) of integers has a power integral basis \( \mathbb{Z}_K = \mathbb{Z}[\xi] \) for \( \xi = \eta + z\sqrt{d} \). Here \( \eta \) means the associated Gauß period of \( \varphi(dd_1)/4 \) terms with the quartic character \( \chi = \chi_d\psi_{d_1} \), where \( \chi_d \) denotes the quartic character with conductor \( d \) and \( \psi_{d_1} \) the quadratic one with conductor \( d_1 \).

§3. A new family of monogenic cyclic quartic fields based on bases of the fields

Let \( K \) be a cyclic quartic extension \( \mathbb{Q}(\theta) \) over \( \mathbb{Q} \) associated to the character \( \chi = \chi_d\psi_{d_1} \), where \( \chi_d \) is a quartic and \( \psi_{d_1} \) is a quadratic character. Then \( K \) has a quadratic subfield \( k = \mathbb{Q}(\sqrt{d}) \) with the field discriminant \( d \). In this article, we restrict ourselves within an odd factor \( d \equiv 5 \) (mod 8) of the conductor \( dd_1 \) of \( K \). It is because \( \mathbb{Z}_K \) has no power basis if \( d \equiv 1 \) (mod 8). Indeed, the prime 2 is completely decomposed in \( k \) in this case, and hence the relative degree \( f \) of 2 with respect to \( K/\mathbb{Q} \) is at most 2. Thus by Lemma 2 of [17], \( \mathbb{Z}_K \) has no power basis. Since \( K \) is a quadratic extension of \( k \), we can choose an integer \( \sqrt{\frac{a + b\sqrt{d}}{2}} \) for \( a, b \in \mathbb{Z}, a \equiv b \) (mod 2) as a generator \( \theta \) for the field \( K \).

Here we use the following lemmas.

Lemma 3.1 ([17]). Let \( \ell \) be a prime number and let \( F/\mathbb{Q} \) 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 two conditions is satisfied, then the ring \( \mathbb{Z}_F \) of integers in \( F \) has no power integral basis, i.e., \( F \) is non-monogenic:

1. \( e\ell^f < n \) and \( f = 1 \);
2. \( e\ell^f \leq n + e - 1 \) and \( f \geq 2 \).

Lemma 3.2 ([6, 19]). Being the same notation as above, the field \( \mathbb{Q}\left(\sqrt{(a + b\sqrt{d})/2}\right) \) is a cyclic quartic extension over \( \mathbb{Q} \) if and only if there exists an integer \( j \in \mathbb{Z} \) such that

\[
\frac{a^2 - b^2d}{4} = j^2d;
\]

hence \( a \equiv 0 \) (mod \( d \)) in this case.

Let \( G \) be the Galois group \( < \sigma > \) of the cyclic quartic extension \( K/\mathbb{Q} \) with a generator \( \sigma \). We may suppose

\[
\theta^\sigma = \sqrt{\frac{a - b\sqrt{d}}{2}} \quad \text{and} \quad \theta^{\sigma^2} = -\theta.
\]
Proposition 3.3. Let \( d(1, \sqrt{d}, \theta, \theta^\sigma) \) be the discriminant of a basis \( \{1, \sqrt{d}, \theta, \theta^\sigma\} \) of the field \( K \), where \( \theta = \sqrt{\frac{a+b\sqrt{d}}{2}} \), \( \theta^\sigma = \sqrt{\frac{a-b\sqrt{d}}{2}} \) and \( \theta^{\sigma^2} = -\theta \). Then it holds that

\[
d(1, \sqrt{d}, \theta, \theta^\sigma) = \begin{vmatrix} 1 & \sqrt{d} & \theta & \theta^\sigma \\ 1 & -\sqrt{d} & \theta^\sigma & -\theta \\ 1 & \sqrt{d} & -\theta & -\theta^\sigma \\ 1 & -\sqrt{d} & -\theta^\sigma & \theta \end{vmatrix}^2 = 64a^2d.
\]

On the other hand, we obtain the field discriminant \( d_K \) by the next lemma.

Lemma 3.4 ([18]). For the field discriminant \( d_K \) of the cyclic quartic field \( K \) associated to quartic character \( \chi = \chi_d\psi_{d_1} \), it holds that

(1) \( d_K = f_1f_Xf\chi^2f\chi^3 = d^3d_1^2 \),

where \( f_\rho \) and \( I \) denote the conductor of a character \( \rho \) and the principal character, respectively;

(2) \( d_K = \text{N}_{k}(d_{K/k})d_{k}^{2} = d^{3}d_{1}^{2} \),

where \( k \) denotes the quadratic subfield \( \mathbb{Q}(\sqrt{d}) \) of \( K \), \( d_{K/k} \) the relative discriminant with respect to \( K/k \) and \( \text{N}_{k} \) the norm of an ideal in \( k \) with respect to \( k/\mathbb{Q} \), respectively.

Lemma 3.5 ([6]). Being the same notation as above, for a number \( \xi = x+y\sqrt{d}+z\theta+w\theta^\sigma \) of the field \( K \), \( x, y, z, w \in \mathbb{Q} \), it holds that \( \xi \in Z_{K} \) if and only if the following two conditions hold:

(IT) \( \text{Tr}_{K/k}(\xi) = 2(x+y\sqrt{d}) \in Z_K \),

(IN) \( N_{K/k}(\xi) = \left\{x^2+y^2d-(z^2+w^2)\frac{a}{2}\right\} + \left\{2xy-(z^2-w^2)\frac{b}{2}-2zwj\right\}\sqrt{d} \in Z_K \).

Theorem 3.6. Let \( \chi = \chi_d\psi_{d_1} \) be the composite quartic character with a quartic \( \chi_d \) with odd conductor \( d \) and a quadratic \( \psi_{d_1} \) with odd conductor \( d_1 \). Then a cyclic quartic field \( K = \mathbb{Q}(\theta) \) with \( \theta = \sqrt{\frac{a+b\sqrt{d}}{2}} \) for square free integers \( a \) and \( b \) is monogenic, namely \( Z_K = \mathbb{Z}[\xi] \) for some \( \xi = x+y\sqrt{d}+z\theta+w\theta^\sigma \), \( x, y, z, w \in \mathbb{Q} \) and a generator \( \sigma \) of the Galois group of \( K/\mathbb{Q} \), if and only if the following three conditions are satisfied:

(1) For \( a = dd_1a_0, \ b = d_1b_0, \ d \equiv 5 (\text{mod } 8), \ -d_1 \equiv 1 (\text{mod } 4) \), it holds that \( \frac{da_0^2-b_0^2}{4} = j_0^2 \) and \( a_0, b_0, j_0 \) are rational integers;

(2) \( \text{Tr}_{K/k}(\xi) = 2(x+y\sqrt{d}) \) belongs to \( Z_k \), and

\[
N_{K/k}(\xi) = \left\{x^2+y^2d-(z^2+w^2)\frac{dd_1a_0}{2}\right\} + \left\{2xy-(z^2-w^2)\frac{d_1b_0}{2}-2zwd_1j_0\right\}\sqrt{d} \text{ belongs to } Z_k;
\]

(3) For \( X = (z^2-w^2)j_0-zwb_0 \) and \( Y = 4y^2-(z^2+w^2)d_1a_0 \), it holds that \( X = \pm \frac{1}{4} \) and \( 2d_1X - Y\sqrt{d} \) is a unit in \( k \).
Proof. First we immediately see that the assertion (2) holds if and only if $\xi \in \mathbb{Z}_K$. We now assume $\xi \in \mathbb{Z}_K$. We notice that the assertion $Z_K = \mathbb{Z}[\xi]$ if and only if $\pm d_K = d_K(\xi)$. For the different $d_K(\xi) = (\xi - \xi^\sigma)(\xi - \xi^\sigma^2)(\xi - \xi^\sigma^3)$, it holds that

$$d_K(\xi) = N_K(d_K(\xi)) = N_K(d_K/\mathfrak{d}_K(\xi) \cdot N_K(d_k(\mathfrak{d}_k(\xi))).$$

We put

$$(I) = N_k(d_{K/k}(\xi)) = (\xi - \xi^\sigma^2)(\xi - \xi^\sigma^3)^\sigma, \quad (II) = N_{K/k}(d_k(\xi)) = (\xi - \xi^\sigma)(\xi - \xi^\sigma)^\sigma^2.$$

Then, it follows that

$$N_K(d_{K/k}(\xi)) = N_k(N_{K/k}(d_{K/k}(\xi)) = N_k(d_K(\xi))$$
$$= N_{K/k}(N_k(d_K(\xi)))$$
$$= N_{K/k}((\xi - \xi^\sigma^2)(\xi - \xi^\sigma)^\sigma)$$
$$= (I)^2$$

and

$$N_K(d_k(\xi)) = N_{K/k}(N_k(d_k(\xi))) = N_{K/k}(d_k(\xi))$$
$$= N_{K/k}(N_{K/k}(d_k(\xi)))$$
$$= (\xi - \xi^\sigma)(\xi - \xi^\sigma^2^)(\xi - \xi^\sigma^3)^\sigma,$$

$$= (II)(II)^\sigma.$$

Specifically,

$$d_{K/k}(\theta) = N_{K/k}(d_{K/k}(\theta)) = (\theta - \theta^\sigma^2)(\theta - \theta^\sigma^2)^\sigma^2 = (\theta - (-\theta))(\theta - (-\theta))^\sigma^2 = 4\theta\theta^\sigma^2.$$

Then by Lemma 3, it holds that

$$\frac{d_K(\theta)}{d_K(\theta)^4} = N_k(d_{K/k}(\theta)) = (4\theta\theta^\sigma^2)(4\theta\theta^\sigma^2)^\sigma = 2^4(\theta\theta^\sigma)(\theta\theta^\sigma)^\sigma^2$$
$$= 2^4\sqrt{a^2 - b^2d} \left((-1)^2 \sqrt{a^2 - b^2d}\right) = 2^4 j^2d.$$
because \( K = \mathbb{Q}(\theta) \) is a cyclic quartic field. For a generator \( \xi = x + y\sqrt{d} + z\theta + w\theta^\sigma \) of \( Z_K \) in \( \mathbb{Q}(\theta) \) we have

\[
(I) = 2(z\theta + w\theta^\sigma) \cdot 2(z\theta^\sigma + w\theta^\sigma^2) \\
= 2^2(z^2\theta\theta^\sigma + zw(\theta\theta^\sigma^2 + (\theta^\sigma)^2) + w^2\theta^\sigma \theta^\sigma^2) \\
= 2^2(z^2j\sqrt{d} + zw\left(-\frac{a + b\sqrt{d}}{2} + \frac{a - b\sqrt{d}}{2}\right) + w^2(-j\sqrt{d})) \\
= 2^2(-zwb\sqrt{d} + (z^2 - w^2)j\sqrt{d}) \\
= 2^2Xd_1\sqrt{d} \text{ with } X = (z^2 - w^2)j_0 - zwb_0
\]

and

\[
(II) = (2y\sqrt{d} + z(\theta - \theta^\sigma) + w(\theta + \theta^\sigma))(2y\sqrt{d} - z(\theta - \theta^\sigma) - w(\theta + \theta^\sigma)) \\
= 4y^2d - \{z(\theta - \theta^\sigma) + w(\theta + \theta^\sigma)\}^2 \\
= 4y^2d - \{z^2(\theta^2 + (\theta^\sigma)^2 - 2\theta\theta^\sigma) + w^2(\theta^2 + (\theta^\sigma)^2 + 2\theta\theta^\sigma) + zw(\theta^2 - (\theta^\sigma)^2)\} \\
= 4y^2d - \{z^2(a - 2j\sqrt{d}) + w^2(a + 2j\sqrt{d}) + 2zw(b\sqrt{d})\} \\
= \{4y^2 - (z^2 + w^2)a_0d_1\}d - 2\{z^2j - w^2j - zwb\}\sqrt{d} \\
= (Y\sqrt{d} - 2Xd_1)\sqrt{d}
\]

with \( Y = 4y^2 - (z^2 + w^2)a_0d_1, \quad X = (z^2 - w^2)j_0 - zwb_0 \).

Hence, \( d_K(\xi) = d_K \) if and only if two numbers \( 2^2X \) and \( Y\sqrt{d} - 2d_1X \) are units in \( k \), that is,

\[
(z^2 - w^2)j_0 - zwb_0 = \pm \frac{1}{4}, \\
(4y^2 - (z^2 + w^2)a_0d_1)\sqrt{d} - 2((z^2 - w^2)j_0 - zwb_0)d_1 = \text{a unit in } k.
\]

\[\square\]

§ 4. The density of certain monogenic fields

Finally we construct certain monogenic cyclic quartic fields \( K \) associated to the characters of the form \( \chi = \chi_d\psi_{d_1} \) where \( \chi_d \) is a quartic character with conductor \( d \) and \( \psi_{d_1} \) a quadratic character with conductor \( | -d_1 | \). Let \( < \sigma > \) be the Galois group of \( K/\mathbb{Q} \) and \( \theta = \sqrt{\frac{a + b\sqrt{d}}{2}} \) be a primitive element of \( K \) over \( \mathbb{Q} \). Here we can put \( a = dd_1a_0, \ b = d_1b_0 \) and \( j = d_1j_0 \) by the previous section. For a number \( \xi = x + y\sqrt{d} + z\theta + w\theta^\sigma \), we select

\[
x = y = \frac{d_2}{4}, d_2 \equiv 1 \pmod{2}, \ z = \frac{1}{2}, \ w = 0, j_0 = 1, \ a_0 = -1, \ -d_1 = -d_2^2 \pm 2, \ d = d_1^2 + 4.
\]
On a Problem of Hasse

Then by

\[ Y = 4y^2 - (z^2 + w^2)a_0d_1 \equiv \frac{1}{2} \pmod{1}, \]
\[ 2X = 2((z^2 - w^2)j_0 - zwb_0) = \frac{1}{2}, \]

it holds that \( Y\sqrt{d} - 2Xd_1 \in \mathbb{Z}_k \).

We estimate the density \( \Delta \) of square free numbers \( d_1 = d_2^2 - 2 \) and \( d = d_1^2 + 4 \). Assume \( d_2^2 - 2 \equiv D_2^2 - 2 \equiv 0 \pmod{p^2} \) for an odd prime \( p \) with \( d_2 \leq D_2 \) and \( d_2 \equiv D_2 \equiv 1 \pmod{2} \). Then \((d_2 - D_2)(d_2 + D_2) \equiv 0 \pmod{p^2} \). If \( d_2 - D_2 \equiv d_2 + D_2 \equiv 0 \pmod{p} \), then \( 2d_2 \equiv 0 \pmod{p} \), and hence \( d_2 \equiv 0 \pmod{p} \); so \(-2 \equiv -d_2^2 \equiv 0 \pmod{p} \), which is a contradiction. Thus only either one of \( D_2 \equiv d_2 \) or \(-d_2 \pmod{p^2} \) holds. Let \( I_t = (tp^2, (t + 1)p^2) \) be the unique interval of the form which contains \( d_2 \), and \( J_t \) be the set \( \{D_2; p^2 | (D_2^2 - 2), D_2 \in I_t \} \). Then \( J_t = \{d_2, (2t + 1)p^2 - d_2 \} \) for \( tp^2 < (2t + 1)p^2 - d_2 < (t + 1)p^2 \). However, since \((2t + 1)p^2 - d_2 \equiv 0 \pmod{2} \), it holds that \( \# J_t = \# \{d_2\} = 1 \).

Hence, for odd primes \( p \)

\[
\lim_{N \to \infty} \frac{\# \{d_1 = d_2^2 - 2 < N; d_1 \text{ odd square free} \}}{N} > \lim_{N \to \infty} \frac{1}{N} \left( N - \# \{d_1; d_1 < N, p^2|d_1\} - \# \{d_1; d_1 < N, 2|d_1\} \right) > 1 - \sum_{(\frac{2}{p})=1} \frac{1}{p^2} - \frac{1}{2};
\]

we denote the last value by \( \delta_1 \) where \( \frac{1}{2} \) means the the density of even \( d_2 \). For \( d = d_1^2 + 4 \), we have \( p \mid d \) if and only if \((\frac{-1}{p}) = 1 \) if and only if \( p \equiv 1 \pmod{4} \). In the ring of Gaussian integers, \( p \mid d = d_1^2 + 4 \) if and only if \( p = p\bar{\pi} \) for a prime \( \pi = a + ib \) and its conjugate \( \bar{\pi} = a - ib \). Suppose that \( d \equiv 0 \pmod{p^2} \). Then since \( d_1^2 + 4 = (d_1 + 2i)(d_1 - 2i) = (d_2^2 - 2 + 2i)(d_2^2 - 2 - 2i) \), if \( d_1 \equiv 0 \pmod{p^2} \), then \( \pi^2 \mid d_2^2 - 2 + 2i \), because \( (d_2^2 - 2, 2) = 1 \).

Assume \( d_2^2 - 2 + 2i \equiv D_2^2 - 2 + 2i \pmod{\pi^2} \) and \( d_2 \leq D_2 \); in the same way as above, we obtain

\[
\lim_{N \to \infty} \frac{\# \{d = d_1^2 + 4 < N; d \text{ has a square factor } > 2 \}}{N} = \lim_{N \to \infty} \frac{1}{N} \# \{d; d < N, p^2|d\} < \lim_{N \to \infty} \frac{1}{N} \sum_{d < N, \ p^2|d} \frac{N}{p^2} = \sum_{(\frac{\pi}{p})=1} \frac{1}{p^2};
\]

we denote the last value by \( \delta \).

Let \( \Delta \) be the density

\[
\lim_{N \to \infty} \frac{\# \{d = d_1^2 + 4 < N; d \text{ and } d_1 \text{ are square free} \}}{N}.
\]
Then $\Delta > \delta_1 - \delta = \left(1 - \frac{1}{2} - \sum_{(\frac{2}{p})=1} \frac{1}{p^2}\right) - \sum_{(\frac{-1}{p})=1} \frac{1}{p^2}. By virtue of the evaluation

$$\sum_{p\geq 3} \frac{1}{p^2} < \frac{19}{72},$$

which is due to Lemma 7 in [6], we obtain $\Delta > \frac{1}{2} - (\frac{19}{72} - \frac{1}{3^2}) \times 2 = \frac{7}{36} > 0.$ Indeed, from the fact $(\frac{-1}{3}) = (\frac{2}{3}) = -1$, it follows that $3 \nmid d$ and $3 \nmid d_2$; namely, the prime number 3 does not appear in the both summations $\sum_{(\frac{2}{p})=1} \frac{1}{p^2}$ and $\sum_{(\frac{-1}{p})=1} \frac{1}{p^2}$. Then the evaluation of $\sum_{p\geq 5} \frac{1}{p^2} = \sum_{p\geq 3} \frac{1}{p^2} - \frac{1}{3^2}$ is bounded by the value $\frac{19}{72} - \frac{1}{3^2}.$ Contrary to the cyclic quartic fields with prime conductors, we obtain

**Theorem 4.1.** There exist infinitely many monogenic cyclic quartic fields with odd composite conductors over the rationals.

**Example 4.2.** Using the parameter $z$ in Theorem 1, several conductors of new monogenic cyclic quartic fields are given as follows;

$$53 \cdot |z_{-1}=1 = 371, 533 \cdot |z_{-2}=13 \cdot 41 \cdot |z_{-3}=12259,$$

$$2213 \cdot |z_{-3}=104011.$$ Two monogenic fields with conductors,

$$5 \cdot |z_{-0}=5, 13 \cdot |z_{+0}=39$$

coincide with the members of the former experiments [10].

**Acknowledgement.** The authors would like to express their gratitude to Prof. Yuichiro Taguchi [Kyushu Univ.] for his valuable comments to §2, a referee for many notices with linguistic remarks and Prof. Ken Yamamura [National Defense Academy of Japan] for remarks on Theorem 1 and updated reference tables on monogenuity and the non-essential discriminant factor (außerwesentlicher Diskriminantenanteiler) of an algebraic number field. Finally the authors would express thanks to Prof. Noriyuki Suwa[Chuo Univ.] for his ceaseless encouragements to find a new phenomenon in Mathematics introducing us a short novel 夢十話[Ten Stories of Dreams] by 夏目漱石 during the Conference [Algebraic Number Theory and Related Topics 2007].

**References**


[13] Nakahara T. and Uehara T., Monogenesis of the Rings of Integers in Certain Abelian Fields, Preprint,


[21] Yamamura K., Bibliography on außerwesentlicher diskriminantenteiler or common index divisors in algebraic number fields, Dec. 2007, updated ed., [47 papers with MR# are included].