RIMS Kôkyûroku Bessatsu
B12 (2009), 209–221

On a Problem of Hasse

By

Yasuo Motoda*, Toru Nakahara[1)**] Syed Inayat Ali Shah*** and Tsuyoshi Uehara[1)†]

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 ξ over $\boldsymbol{Z}$. We will find an integer ξ 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 $\boldsymbol{Q}$. Let $\boldsymbol{Z}$ 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 ξ as $\boldsymbol{Z}$-free module, namely Z_K coincides with

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

which we denote by $\boldsymbol{Z}[\xi]$. If $Z_K = \boldsymbol{Z}[\xi]$, 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

Received May 12, 2008. Revised April 13, 2009.
2000 Mathematics Subject Classification(s): 11R04.
Key Words: Hasse's problem, Power integral basis, Partial Different
[1)] Partially supported by grant (♯18540040) from the Japan Society for the Promotion of Science.
*Yatsushiro National College of Technology, Yatsushiro 866-8501, Japan.
e-mail: `motoda@as.yatsushiro-nct.ac.jp`
**Faculty of Science and Engineering, Saga University 840-8502, Japan [Current address; National University of Computer & Emerging Sciences(NUCES]) Peshawar Campus, 160-Industrial Estate, Hayatabad, Peshawar, the Islamic Republic of Pakistan.]
e-mail: `toru.nakahara@nu.edu.pk, nakahara@ms.saga-u.ac.jp`
***Department of Sciences and Humanities, NUCES Peshawar Campus, [Current address; Islamia College University Peshawar, N.W.F.P., the Islamic Republic of Pakistan.]
e-mail: `inayat.shah@nu.edu.pk`
†Faculty of Science and Engineering, Saga University 840-8502, Japan.
e-mail: `uehara@ma.is.saga-u.ac.jp`

fields K with composite conductors over $\boldsymbol{Q}$. 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 $\boldsymbol{Q}$. 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 $k_{24} = \boldsymbol{Q}(\zeta_{24})$, which coincides with

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

where ζ_m denotes a primitive m-th root of unity. Besides the results referred above, there are works of I. Gaál, L. Robertson, S. I. A. Shah, T. Uehara [2, 16, 17, 13, 11] for monogenic fields, and ones of M. N. Gras and authors [3, 11, 9] for non-monogenic fields. An expository paper [5] by K. Győry and the frequentry updated tables [20, 21] by K. Yamamura are significant for future research on Hasse's problem.

§ 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 $K = \boldsymbol{Q}(\eta)$ of composite conductor D over $\boldsymbol{Q}$ in [N$_1$]. This result was obtained when we restricted ourselves to the assiciated Gauß period η_χ of $\varphi(D)/4$ terms with the character χ as a generator ξ of $Z_K = \boldsymbol{Z}[\xi]$, where $\chi = \chi_D$ is the quartic character with conductor D and $\varphi(\cdot)$ denotes Euler's function. We calculated the group index $[Z_K : \boldsymbol{Z}[\xi]] = \sqrt{\left|\frac{d_K(\xi)}{d_K}\right|}$ of a number ξ under the integral basis $\{1, \eta_\chi, \eta_\chi^\sigma, \eta_\chi^{\sigma^2}\}$, i.e., nearly the normal basis of $K/\boldsymbol{Q}$, where $d_F, d_F(\alpha)$ and σ denote the field discriminant of a field F, the discriminant of a number α with respect to $F/\boldsymbol{Q}$ and a generator of the Galois group of $K/\boldsymbol{Q}$, respectively.

In this section, we use a different integral basis from the previous one and seek a candidate ξ of a generator of Z_K using a *linear* combination of certain *partial* differents of ξ. 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 $(1 \leqq j \leqq 3)$, namely $K_1 = k_5, K_2 = \boldsymbol{Q}(\sqrt{5}, \sqrt{-3}), K_3 = \boldsymbol{Q}(\zeta_{15} + \zeta_{15}^{-1})$, $L_1 = \boldsymbol{Q}(\sqrt{5})$, $L_2 = \boldsymbol{Q}(\sqrt{-3}), L_3 = \boldsymbol{Q}(\sqrt{-15})$. 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 composite conductor $53 \cdot |-7|$. This field has three quartic subfields K_j $(1 \leqq j \leqq 3)$;

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

In the field K_2, since 2 remains prime in the quadratic subfield $\boldsymbol{Q}(\sqrt{53})$ and is decomposed in $\boldsymbol{Q}(\sqrt{-7})$, i.e., its relative degree f_{K_2} with respect to $K_2/\boldsymbol{Q}$ is 2, we see by Lemma 2 that K_2 is non-monogenic. However, since the relative degree f_{K_1} with respect to $K_1/\boldsymbol{Q}$ 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 $k_D/\boldsymbol{Q}$. We identify the group G with the reduced residue group modulo D. Let $\chi_p(x) = \left(\dfrac{x}{\pi_j}\right)_4$ be a pure quartic character with conductor p_j for $x \in G$, where $\left(\dfrac{\cdot}{\pi_j}\right)_4$ means the quartic residue symbol modulo π_j with normalized $\pi_j \equiv 1 \pmod{(1-i)^3}$ $(1 \leqq j \leqq r)$. Then the quartic character χ_d is defined by $\prod_{j=1}^{r} \chi_{p_j}$. Let ψ_d and ψ_{d_1} denote the quadratic characters χ_d^2 and $\prod_{k=1}^{s} \psi_{q_k}$ for the quadratic character ψ_{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 χ. From the norm relation of the Gauß sum, Jacobi sum and the decomposition of $\tau(\chi)$, we have

$$\begin{aligned}
\tau(\chi_p)\tau(\bar{\chi}_p) &= \chi_p(-1)p, \\
\tau(\chi_p)^2/\tau(\chi_p^2) &= -\chi_p(-1)\pi_p, \\
\tau(\chi) &= \left(\prod_{j=1}^{r} \chi_{p_j}(d/p_j)\right)\left(\prod_{k=1}^{s} \psi_{q_k}(d_1/q_k)\right)\left(\prod_{j=1}^{r} \tau(\chi_{\pi_j})\right)\left(\prod_{k=1}^{s} \tau(\psi_{q_k})\right),
\end{aligned}$$

where $\overline{\chi}_p$ denotes the complex conjugate character of χ_p. Then we can derive for $d = \delta \cdot \overline{\delta}$,

$\delta \equiv 1 \,(\mathrm{mod}\ (1-i)^3)$,

$$\tau(\chi)\tau(\bar{\chi}) = \chi(-1)dd_1 = (-1)^s dd_1,$$
$$\tau(\chi)^2 = (-1)^{r+s}\psi_d(d_1)\delta d_1\sqrt{d},$$
$$\tau(\chi^2) = (-1)^s\psi_d(d_1)\sqrt{d}.$$

Let H be the kernel of χ. Then the residue class group G/H is isomorphic to a cyclic subgroup $<\chi>$ of order 4 of the character group $\mathfrak{X}$ of G. Let K denote the subfield of k_D associated with $<\chi>$. Then K is a cyclic quartic extension over $\boldsymbol{Q}$, whose Galois group $Gal(K/\boldsymbol{Q})$ is isomorphic to G/H. Let $\eta = \eta_\chi = \sum_{x\in H}\zeta_D^x$ be the associated Gauß period of $\varphi(D)/4$ terms with the character χ of conductor D. Then we have $K = \boldsymbol{Q}(\eta)$. Fix an element $\sigma \in G$ such that $\chi(\sigma) = i$. Then we get

$$\eta = ((-1)^{r+s} + \tau(\chi) + \tau(\chi^2) + \tau(\overline{\chi}))/4$$
$$\tau(\chi)^\sigma = -i\tau(\chi), \quad \tau(\chi^2)^\sigma = -\tau(\chi^2), \quad \tau(\overline{\chi})^\sigma = i\tau(\overline{\chi}).$$

Lemma 2.1. *Being the same notation as above, it holds that*

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

Proof. Since the set $\{\eta,\eta^\sigma,\eta^{\sigma^2},\eta^{\sigma^3}\}$ forms a normal basis of Z_K, we have $Z_K = \boldsymbol{Z}[1,\eta,\eta^\sigma,\eta^{\sigma^2}]$ 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 $\{1,\eta,\eta^\sigma,\eta+\eta^{\sigma^2}\}$. □

Now, we choose the integral basis $\{1,\eta,\eta+\eta^{\sigma^2},\eta^\sigma\}$ because the number $\eta+\eta^{\sigma^2} = \{(-1)^{r+s}+\tau(\chi^2)\}/2 = \{(-1)^{r+s}+\sqrt{d}\}/2$ belongs to $k = \boldsymbol{Q}(\sqrt{d})$. Assume that we have $Z_K = \boldsymbol{Z}[\xi]$ for $\xi = x\eta + y\eta^\sigma + z(\eta+\eta^{\sigma^2})$. Then for the candidate ξ of a power integral basis, the different $\mathfrak{d}_K(\xi)$ of ξ should be equal to the field different $\mathfrak{d}_K$. By Hasse's Conductor-Discriminant formula, we have $d_K = \prod_{\rho\in<\chi>} f_\rho = 1\cdot dd_1\cdot d\cdot dd_1 = d^3d_1^2$ and $d_K = \mathrm{N}_K(\mathfrak{d}_K)$, where f_ρ denotes the conductor of a character ρ.
By $\mathfrak{d}_K(\xi) = (\xi-\xi^\sigma)(\xi-\xi^{\sigma^2})(\xi-\xi^{\sigma^3})$ we have

$$\begin{aligned}
\pm d_K(\xi) &= N_K(\mathfrak{d}_K(\xi)) \\
&= (\xi-\xi^\sigma)(\xi-\xi^{\sigma^2})(\xi-\xi^{\sigma^3}) \\
&\times (\xi^\sigma-\xi^{\sigma^2})(\xi^\sigma-\xi^{\sigma^3})(\xi^\sigma-\xi) \\
&\times (\xi^{\sigma^2}-\xi^{\sigma^3})(\xi^{\sigma^2}-\xi)(\xi^{\sigma^2}-\xi^\sigma) \\
&\times (\xi^{\sigma^3}-\xi)(\xi^{\sigma^3}-\xi^\sigma)(\xi^{\sigma^3}-\xi^{\sigma^2}) \\
&= \{(\xi-\xi^\sigma)(\xi-\xi^\sigma)^{\sigma^2}\}^2\{(\xi-\xi^{\sigma^2})(\xi-\xi^{\sigma^2})^\sigma\}^2\left[\{(\xi-\xi^\sigma)(\xi-\xi^\sigma)^{\sigma^2}\}^2\right]^\sigma.
\end{aligned}$$

Here, we select $\xi = x\eta + z(\eta + \eta^{\sigma^2})$ with $y = 0$ and put

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

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

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

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

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

Here $\alpha \cong \beta$ means that both sides are equal to each other as ideals. Then $I = x^2 d_1 \sqrt{d} \cdot \gamma$ for some integer $\gamma \in k$. Since the 'obstacle' factor $x^2\gamma$ should disappear, we have $x = \pm 1$. By virtue of $\mathrm{N}_K(\mathfrak{d}_k(\xi))^2 \equiv 0 \pmod{d_K/d_{K/k}^2}$ and $d_K/d_{K/k}^2 = d^3 d_1^2/(dd_1^2) = d^2$, we obtain $J \cong \mathfrak{d}_k(\xi)\mathfrak{d}_k(\xi)^{\sigma^2} \equiv 0 \pmod{\sqrt{d}}$. Next we consider the following linear relation of three partial differents;

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

namely,

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

For ξ to satisfy $Z_K = \boldsymbol{Z}[\xi]$, there must be such units ε_j in k as

$$\varepsilon_1\sqrt{d} + \varepsilon_2\sqrt{d}d_1 + \varepsilon_3\sqrt{d} = 0.$$

Here by $N_{K/k}(\mathfrak{d}_k(\xi)) = \mathfrak{d}_k(\xi)\mathfrak{d}_k(\xi)^{\sigma^2} \cong \sqrt{d}d_1$, we have $N_k(\mathfrak{d}_{K/k}(\xi)) = \mathfrak{d}_{K/k}(\xi)\mathfrak{d}_{K/k}(\xi)^{\sigma}$ $\cong \sqrt{d}d_1$, because, for a ramified ideal $\mathfrak{L}$ in K, i.e., $\mathfrak{L}|dd_1$, $\mathfrak{L}^{\sigma} = \mathfrak{L}$ holds. Then we get

$$(*)_0 \qquad \begin{cases} \varepsilon_1 + \varepsilon_2 d_1 + \varepsilon_3 = 0, \\ \bar{\varepsilon}_1 + \bar{\varepsilon}_2 d_1 + \bar{\varepsilon}_3 = 0, \end{cases}$$

where $\bar{\varepsilon}$ for $\varepsilon \in k$ means the real conjugate of ε with respect to $K/\boldsymbol{Q}$. When we consider the simultaneous equation $(*)_0$ with coefficients $\varepsilon_j, \bar{\varepsilon}_j$, under the assumption that the rank of $(*)_0$ would be equal to 1, then we have $1 \pm d_1 \pm 1 = 0$, which is impossible by

$d_1 \geqq 3$. Then the rank of $(*)_0$ is equal to 2. Without loss of generality, we may consider the equations dividing both sides of $(*)_0$ by ε_2;

$$(*) \qquad \begin{cases} \varepsilon_1 \cdot 1 + 1 \cdot d_1 + \varepsilon_3 \cdot 1 = 0, \\ \bar{\varepsilon}_1 \cdot 1 + 1 \cdot d_1 + \bar{\varepsilon}_3 \cdot 1 = 0, \end{cases}$$

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

$$1 : d_1 : 1 = \begin{vmatrix} 1 & \varepsilon_3 \\ 1 & \bar{\varepsilon}_3 \end{vmatrix} : \begin{vmatrix} \varepsilon_3 & \varepsilon_1 \\ \bar{\varepsilon}_3 & \bar{\varepsilon}_1 \end{vmatrix} : \begin{vmatrix} \varepsilon_1 & 1 \\ \bar{\varepsilon}_1 & 1 \end{vmatrix}.$$

Then by $1 : 1 = \bar{\varepsilon}_3 - \varepsilon_3 : \varepsilon_1 - \bar{\varepsilon}_1 = -u_3 : -u_1$ and $d_1 : 1 = \varepsilon_3\bar{\varepsilon}_1 - \overline{\varepsilon_3\bar{\varepsilon}_1} : \varepsilon_1 - \bar{\varepsilon}_1$ $= (v_3(-u_1) + u_3v_1)/2 : u_1$, we obtain $d_1 = -(v_3 + v_1)/2$. Since $\varepsilon_3 = (v_3 + u_3\sqrt{d})/2$, $\varepsilon_1 = (v_1 + u_1\sqrt{d})/2$ 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 $N_k(\varepsilon_1) = (d_1^2 - u_1^2 d)/4 = \pm 1$, namely $d_1^2 \pm 4 = u_1^2 d$ holds. From $\mathfrak{d}_k(\xi) = (2z + (-1)^s\psi_{d_1}(d)\sqrt{d})/2 + \{(1+i)\tau(\chi) + (1-i)\tau(\bar{\chi})\}/4$, it follows that

$$\begin{aligned} J =& N_{K/k}(\mathfrak{d}_k(\xi)) = \mathfrak{d}_k(\xi)\mathfrak{d}_k(\xi)^{\sigma^2} \\ =& [(2z \pm 1)\sqrt{d}/2 + \{(1+i)\tau(\chi) + (1-i)\tau(\bar{\chi})\}/4] \\ \times& [(2z \pm 1)\sqrt{d}/2 - \{(1+i)\tau(\chi) + (1-i)\tau(\bar{\chi})\}/4] \\ =& (2z \pm 1)^2 d/4 - \{2i\tau(\chi)^2 - 2i\tau(\bar{\chi})^2 + 4\tau(\chi)\tau(\bar{\chi})\}/(16) \\ =& (2z \pm 1)^2 d/4 - \{2i(\pm\delta d_1\sqrt{d}) - 2i(\pm\bar{\delta} d_1\sqrt{d}) + 4(\pm d d_1)\}/(16) \\ =& (2z \pm 1)^2 d/4 - \{\pm 8bd_1\sqrt{d}) + 4(\pm dd_1)\}/(16) \\ =& \left\{\pm bd_1/2 + [\{(2z \pm 1)^2 - d_1\}/4]\sqrt{d})\right\}\sqrt{d}. \end{aligned}$$

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 ε 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

$$\begin{aligned} d_K(\xi) \cong& N_K(\mathfrak{d}_K(\xi)) \\ \cong& N_K(\mathfrak{d}_{K/k}(\xi) \cdot N_{K/k}(\mathfrak{d}_k(\xi))) \\ \cong& N_K(\mathfrak{d}_{K/k}(\xi)) \cdot N_K(N_{K/k}(\mathfrak{d}_k(\xi))) \\ \cong& N_k(I) \cdot N_K(J) \\ \cong& dd_1^2 \cdot (\sqrt{d})^4 = d^3 d_1^2, \end{aligned}$$

where $I = N_{K/k}(\mathfrak{d}_{K/k}(\xi))$, $J = N_{K/k}(\mathfrak{d}_k(\xi))$ and $\sigma^2 Gal(K/\boldsymbol{Q}) = Gal(K/\boldsymbol{Q})$. Therefore we verified the following Theorem.

Theorem 2.2. *Let $d_1 = (z+1)^2 \pm 2$ $(z \in \boldsymbol{Z})$ and $d = d_1^2 + 4$ be square free integers. Then the cyclic quartic field $K = \boldsymbol{Q}(\eta)$ with conductor dd_1 is monogenic; namely its ring Z_K of integers has a power integral basis $Z_K = \boldsymbol{Z}[\xi]$ for $\xi = \eta + z\sqrt{d}$. Here η means the associated Gauß period of $\varphi(dd_1)/4$ terms with the quartic character $\chi = \chi_d \psi_{d_1}$, where χ_d denotes the quartic character with conductor d and ψ_{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 $\boldsymbol{Q}(\theta)$ over $\boldsymbol{Q}$ associated to the character $\chi = \chi_d \psi_{d_1}$, where χ_d is a quartic and ψ_{d_1} is a quadratic character. Then K has a quadratic subfield $k = \boldsymbol{Q}(\sqrt{d})$ with the field discriminant d. In this article, we restrict ourselves within an odd factor $d \equiv 5 \pmod 8$ of the conductor dd_1 of K. It is because Z_K has no power basis if $d \equiv 1 \pmod 8$. Indeed, the prime 2 is completely decomposed in k in this case, and hence the relative degree f of 2 with respect to $K/\boldsymbol{Q}$ is at most 2. Thus by Lemma 2 of [17], 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 $a, b \in \boldsymbol{Z}$, $a \equiv b \pmod 2$ as a generator θ for the field K. Here we use the following lemmas.

Lemma 3.1 ([17]). *Let ℓ be a prime number and let $F/\boldsymbol{Q}$ be a Galois extension of degree $n = efg$ with ramification index e and the relative degree f with respect to ℓ. If one of the following two conditions is satisfied, then the ring 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) $e\ell^f \leqq n + e - 1$ *and* $f \geqq 2$.

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

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

hence $a \equiv 0 \pmod d$ in this case.

Let G be the Galois group $< \sigma >$ of the cyclic quartic extension $K/\boldsymbol{Q}$ with a generator σ. 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*

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

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) $$d_K = f_I f_\chi f_{\chi^2} f_{\chi^3} = d^3 d_1^2,$$

where f_ρ and I denote the conductor of a character ρ and the principal character, respectively;

(2) $$d_K = \mathrm{N}_k(d_{K/k}) d_k^2 = d^3 d_1^2,$$

where k denotes the quadratic subfield $\boldsymbol{Q}(\sqrt{d})$ of K, $d_{K/k}$ the relative discriminant with respect to K/k and N_k the norm of an ideal in k with respect to $k/\boldsymbol{Q}$, 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, $x, y, z, w \in \boldsymbol{Q}$, it holds that $\xi \in Z_K$ if and only if the following two conditions hold*:

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

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

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

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

(2) *$T_{r_{K/k}}(\xi) = 2(x + y\sqrt{d})$ belongs to $\boldsymbol{Z}_k$, and $N_{K/k}(\xi) = \left\{x^2 + y^2 d - (z^2 + w^2)\dfrac{dd_1a_0}{2}\right\} + \left\{2xy - (z^2 - w^2)\dfrac{d_1b_0}{2} - 2zwd_1j_0\right\}\sqrt{d}$ 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 $\xi \in Z_K$. We now assume $\xi \in Z_K$. We notice that the assertion $Z_K = \boldsymbol{Z}[\xi]$ if and only if $\pm d_K = d_K(\xi)$. For the different $\mathfrak{d}_K(\xi) = (\xi - \xi^\sigma)(\xi - \xi^{\sigma^2})(\xi - \xi^{\sigma^3})$, it holds that

$$d_K(\xi) = N_K(\mathfrak{d}_K(\xi)) = N_K(\mathfrak{d}_{K/k}(\xi) \cdot N_{K/k}(\mathfrak{d}_k(\xi))).$$

We put

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

Then, it follows that

$$\begin{aligned} N_K(\mathfrak{d}_{K/k}(\xi)) &= N_k(N_{K/k}(\mathfrak{d}_{K/k}(\xi)) = N_k(d_{K/k}(\xi)) \\ &= N_{K/k}(N_k(\mathfrak{d}_{K/k}(\xi)) \\ &= N_{K/k}((\xi - \xi^{\sigma^2})(\xi - \xi^{\sigma^2})^\sigma) \\ &= \text{(I)}^2 \end{aligned}$$

and

$$\begin{aligned} N_K(\mathfrak{d}_k(\xi)) &= N_{K/k}(N_k(\mathfrak{d}_k(\xi))) = N_{K/k}(d_k(\xi)) \\ &= N_k(N_{K/k}(\mathfrak{d}_k(\xi))) \\ &= (\xi - \xi^\sigma)(\xi - \xi^\sigma)^{\sigma^2}(\xi - \xi^\sigma)^\sigma(\xi - \xi^\sigma)^{\sigma^3}, \\ &= \text{(II)}\text{(II)}^\sigma. \end{aligned}$$

Specifically,

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

Then by Lemma 3, it holds that

$$\frac{d_K(\theta)}{d_k(\theta)^4} = N_k(d_{K/k}(\theta)) = (4\theta\theta^{\sigma^2})(4\theta\theta^{\sigma^2})^\sigma = 2^4(\theta\theta^\sigma)(\theta\theta^\sigma)^{\sigma^2}$$

$$= 2^4\sqrt{\frac{a^2 - b^2 d}{4}}\left((-1)^2\sqrt{\frac{a^2 - b^2 d}{4}}\right) = 2^4 j^2 d.$$

Since $\gcd(d(1,\ \sqrt{d}, \theta,\ \theta^\sigma),\ N_k(d_{K/k}(\theta)) = \gcd(2^6 a^2 d,\ 2^4 j^2 d) \equiv 0 \pmod{d_{K/k}^2}$ for $d_{K/k}^2 = \frac{d_K}{d_k^2} = \frac{d^3 d_1^2}{d^2} = dd_1^2$, we have $\gcd(a^2 d,\ j^2 d) \equiv 0 \pmod{dd_1^2}$. Then we can put $a = dd_1 a_0$, $j = d_1 j_0, a_0, j_0 \in \boldsymbol{Z}$ together with $d(1,\ \sqrt{d}, \theta,\ \theta^\sigma) \equiv 0 \pmod{d_K}$, and hence by $\frac{a^2 - b^2 d}{4} = j^2 d$ in Lemma 3, we get $b = d_1 b_0$. Therefore we obtain the assertion (1), because $K = \boldsymbol{Q}(\theta)$ is a cyclic quartic field. For a generator $\xi = x + y\sqrt{d} + z\theta + w\theta^\sigma$ of Z_K in $\boldsymbol{Q}(\theta)$ we have

$$\begin{aligned}
(\mathrm{I}) &= 2(z\theta + w\theta^\sigma)\cdot 2(z\theta^\sigma + w\theta^{\sigma^2})\\
&= 2^2(z^2\theta\theta^\sigma + zw(\theta\theta^{\sigma^2} + (\theta^\sigma)^2) + w^2\theta^\sigma\theta^{\sigma^2})\\
&= 2^2(z^2 j\sqrt{d} + zw\left(-\frac{a+b\sqrt{d}}{2} + \frac{a-b\sqrt{d}}{2}\right) + w^2(-j\sqrt{d}))\\
&= 2^2(-zwb\sqrt{d} + (z^2-w^2)j\sqrt{d})\\
&= 2^2 X d_1\sqrt{d} \quad \text{with} \quad X = (z^2-w^2)j_0 - zwb_0
\end{aligned}$$

and

$$\begin{aligned}
(\mathrm{II}) &= (2y\sqrt{d} + z(\theta-\theta^\sigma) + w(\theta+\theta^\sigma))(2y\sqrt{d} - z(\theta-\theta^\sigma) - w(\theta+\theta^\sigma))\\
&= 4y^2 d - \{z(\theta-\theta^\sigma) + w(\theta+\theta^\sigma)\}^2\\
&= 4y^2 d - \{z^2(\theta^2 + (\theta^\sigma)^2 - 2\theta\theta^\sigma) + w^2(\theta^2 + (\theta^\sigma)^2 + 2\theta\theta^\sigma) + 2zw(\theta^2 - (\theta^\sigma)^2)\}\\
&= 4y^2 d - \{z^2(a - 2j\sqrt{d}) + w^2(a + 2j\sqrt{d}) + 2zw(b\sqrt{d})\}\\
&= \{4y^2 - (z^2+w^2)a_0 d_1\}d - 2\{z^2 j - w^2 j - zwb\}\sqrt{d}\\
&= (Y\sqrt{d} - 2Xd_1)\sqrt{d}\\
&\text{with } \; Y = 4y^2 - (z^2+w^2)a_0 d_1, \quad X = (z^2-w^2)j_0 - zwb_0.
\end{aligned}$$

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,

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

□

§ 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 χ_d is a quartic character with conductor d and ψ_{d_1} a quadratic character with conductor $|-d_1|$. Let $<\sigma>$ be the Galois group of $K/\boldsymbol{Q}$ and $\theta = \sqrt{\frac{a+b\sqrt{d}}{2}}$ be a primitive element of K over $\boldsymbol{Q}$. 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

$$x = y = \frac{d_2}{4}, d_2 \equiv 1 \pmod 2),\; z = \frac{1}{2},\; w = 0, j_0 = 1,\; a_0 = -1,\; -d_1 = -d_2^2 \pm 2,\; d = d_1^2 + 4.$$

Then by

$$Y = 4y^2 - (z^2 + w^2)a_0 d_1 \equiv \frac{1}{2} \pmod{1},$$
$$2X = 2((z^2 - w^2)j_0 - zwb_0) = \frac{1}{2},$$

it holds that $Y\sqrt{d} - 2Xd_1 \in \boldsymbol{Z}_k$.

We estimate the density Δ 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 $d_2 \leqq D_2$ 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 $\mathrm{I}_t = (tp^2, (t+1)p^2)$ be the unique interval of the form which contains d_2, and J_t be the set $\{D_2; p^2 \mid (D_2^2 - 2), D_2 \in \mathrm{I}_t\}$. 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 $\sharp J_t = \sharp\{d_2\} = 1$.

Hence, for odd primes p

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

we denote the last value by δ_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 $p = \pi\bar{\pi}$ 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 $d_2 \leqq D_2$; in the same way as above, we obtain

$$\lim_{N\to\infty} \frac{\sharp\{d = d_1^2 + 4 < N; d : \text{has a square factor} > 2\}}{N}$$
$$= \lim_{N\to\infty} \frac{1}{N}\sharp\{d; d < N,\ p^2|d\}$$
$$< \lim_{N\to\infty} \frac{1}{N} \sum_{d<N,\ p^2|d} \frac{N}{p^2} = \sum_{(\frac{-1}{p})=1} \frac{1}{p^2};$$

we denote the last value by δ.

Let Δ be the density

$$\lim_{N\to\infty} \frac{\sharp\{d = d_1^2 + 4 < N; d \text{ and } d_1 \text{ are square free}\}}{N}.$$

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 $\sum_{p \geqq 3} \frac{1}{p^2} < \frac{19}{72}$, 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 $3 \not| d$ and $3 \not| d_2$; namely, the prime number 3 does not appear in the both summations $\sum_{(\frac{2}{p})=1} \frac{1}{p^2}$ and $\sum_{(\frac{-1}{p})} \frac{1}{p^2}$. Then the evaluation of $\sum_{p \geqq 5} \frac{1}{p^2} = \sum_{p \geqq 3} \frac{1}{p^2} - \frac{1}{3^2}$ 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;

$$53 \cdot \mid -7 \mid_{z_-=1} = 371, \quad 533 \cdot \mid -23 \mid_{z_-=2} = 13 \cdot 41 \cdot \mid -23 \mid = 12259,$$
$$2213 \cdot \mid -47 \mid_{z_-=3} = 104011.$$

Two monogenic fields with conductors,

$$5 \cdot \mid -1 \mid_{z_-=0} = 5, \; 13 \cdot \mid -3 \mid_{z_+=0} = 39$$

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 Diskriminantenteiler) 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 (Yume Jyuwa) [Ten Stories of Dreams] by 夏目漱石 (Natsume Soseki) during the Conference [Algebraic Number Theory and Related Topics 2007].

References

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

[2] Gaal, I. and Robertson, L., Power integral bases in prime-power cyclotomic fields, *J. Number Theory*, **120** (2006), 372–384.

[3] Gras M.-N., Non monogénéité de l'anneau des entiers de degré premier $\ell \geq 5$, *J. Number Theory*, **23** (1986), 347–353.

[4] Gras M.-N. and Tanoé F., Corps biquadratiques monogènes, *Manuscripta Math.*, **86** (1995), 63–77.

[5] Győry K., 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.

[6] Y. Motoda, Notes on Quartic Fields, *Rep. Fac. Sci. Engrg. Saga Univ. Math.*, **32**-1 (2003), 1–19, Appendix and corrigenda to "Notes on Quartic Fields", *ibid.*, **37**-1(2008), 1–8.

[7] Motoda Y., Power Integral Bases for Certain Abelian Fields, *Saga Univ.*, Ph. D. Thesis 2004, pp. 31,
`http://dlwww.dl.saga-u.ac.jp/contents/diss/GI00000879/motodaphd.pdf`

[8] Motoda Y. and Nakahara T., Power integral bases in algebraic number fields whose Galois groups are 2-elementary abelian, *Arch. Math.*, **83** (2004), 309–316.

[9] Motoda Y., Nakahara T. and Shah S. I. A., On a problem of Hasse for certain imaginary abelian fields, *J. Number Theory*, **96** (2002), 326–334.

[10] Nakahara T., On Power integral bases in the ring of integers in quartic abelian fields [in Japanese], *RIMS Kôkyûroku, Kyoto Univ. Experimental Number Theory*, **371** (1979), 31–46.

[11] Nakahara T., On Cyclic biquadratic fields related to a problem of Hasse, *Monatsh. Math.*, **94** (1982), 125–132.

[12] Narkiewich W, Elementary and Analytic Theory of Algebraic Numbers, *Springer-Verlag* 3rd *ed.*, 2007, Berlin-Heidelberg-New York; PWM-Polish Scientific Publishers, Warszawa.

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

[14] Park K., Motoda Y. and Nakahara T., On integral bases of certain real octic abelian fields, *Rep. Fac. Sci. Engrg. Saga Univ. Math.*, **34**-1 (2005), 1–15.

[15] Park K., Nakahara T. and Motoda Y., On integral bases of the octic 2-elementary abelian extension fields, *submitted*.

[16] Robertson L., Power bases for cyclotomic integer rings, *J. Number Theory*, **69** (1998), 98–118.

[17] Shah S. I. A. and Nakahara T., Monogenesis of the rings of integers in certain imaginary abelian fields, *Nagoya Math. J.*, **168** (2002), 85–92.

[18] Washington L. C., Introduction to cyclotomic fields, *Graduate texts in mathematics* 2nd *ed.*, **83**, 1997, Springer-Verlag, New York-Heidelberg-Berlin.

[19] Williams K. S., Integers of biquadratic fields, *Canad. Math. Bull.*, **13** (1970), 519-526.

[20] Yamamura K., Bibliography on monogenuity of orders of algebraic number fields, Dec. 2007*, updated ed.*, [91 papers with MR# are included].

[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].