ANNALES MATHÉMATIQUES

BLAISE PASCAL

Toru Nakahara

Hasse's problem for monogenic fields

Volume 16, n° 1 (2009), p. 47-56.

<http://ambp.cedram.org/item?id=AMBP_2009__16_1_47_0>

Publication éditée par le laboratoire de mathématiques de l'université Blaise-Pascal, UMR 6620 du CNRS Clermont-Ferrand — France

Annales mathématiques Blaise Pascal **16**, 47-56 (2009)

Hasse's problem for monogenic fields

Toru Nakahara

Abstract

In this article we shall give a survey of Hasse's problem for integral power bases of algebraic number fields during the last half of century. Specifically, we developed this problem for the abelian number fields and we shall show several substantial examples for our main theorem [7] [9], which will indicate the actual method to generalize for the forthcoming theme on Hasse's problem [15].

1. Introduction

In 1960's Hasse proposed to characterize number fields whose rings of integers have power integral bases. First, we define a power integral basis.

Definition 1.1. Let Z_K be the ring of integers in an algebraic number field K of extension degree n. When the ring Z_K is generated by a primitive element α in K, namely $Z_K = \mathbf{Z}[\alpha] = \mathbf{Z}[1, \alpha, \cdots, \alpha^{n-1}]$, we call that Z_K has a power basis or K is monogenic.

Let ζ_n be a primitive n-th root of unity. When K is any cyclotomic number field $k_n = \mathbf{Q}(\zeta_n)$, its maximal real subfield $\mathbf{Q}(\zeta_n + \zeta_n^{-1})$ or any quadratic number field $\mathbf{Q}(\sqrt{m})$ for a square-free $m \neq 0, 1$, the ring Z_K of integers has a power basis;

$$\mathbf{Z}[\zeta_n], \quad \mathbf{Z}[\zeta_n + \zeta_n^{-1}], \quad \mathbf{Z}[\omega]$$

respectively. Here

$$\omega = \frac{d + \sqrt{d}}{2}, \quad d = \begin{cases} m & \text{if } m \equiv 1 \pmod 4, \\ 4m & \text{if } m \equiv 2, 3 \pmod 4. \end{cases}$$

If K is a certain cubic cyclic quartic abelian or a maximal imaginary abelian subfield of a cyclotomic field k_n, such families of infinitely many

Partially supported by grant (♯16540029) from the Japan Society for the Promotion of Science.
Keywords: Power integral basis, monogenic fields, Hasse's problem.
Math. classification: 11R27, 11R29, 11R37.

fields have power integral bases [1, 2, 4, 10, 11, 12, 13, 14, 17]. On the other hand, Dedekind showed that a non-Galois cubic field $K = \mathbf{Q}(\theta)$ is non-monogenic, where θ is a root of $f(\theta) = \theta^3 - \theta^2 - 2\theta - 8 = 0$ with the discriminant $d(\theta) = -N_{K/\mathbf{Q}} f'(\theta) = -2^2 \cdot 503$. If K is non-monogenic, by Stickelberger's theorem the field discriminant $d(K)$ would equal to -503. In fact, we can seek for an integer η as a third generator of Z_K. Let $\eta = (\theta + \theta^2)/2 \notin \mathbf{Z}[\theta]$ Then $\theta\eta = \theta^2 + \theta + 4 \in \mathbf{Z}[\theta]$. Hence $\eta^2 + \eta = 2\theta^2 + 4\theta + 6$. Thus $\eta \in \bar{\mathbf{Z}}_K \cap K = Z_K$, where $\bar{\mathbf{Z}}_K$ is the integral closure of Z_K. Then

$$\begin{pmatrix} 1 \\ \theta \\ \eta \end{pmatrix} = M \begin{pmatrix} 1 \\ \theta \\ \theta^2 \end{pmatrix} \text{ with } M = \begin{pmatrix} 1 & & \\ & 1 & \\ & \frac{1}{2} & \frac{1}{2} \end{pmatrix}.$$

Hence $d(1, \theta, \eta) = (\det M)^2 d(1, \theta, \theta^2)$ namely, $d(1, \theta, \eta) = \frac{1}{4} \cdot (-4 \cdot 503) = -503$. Thus we have $Z_K = \mathbf{Z}[1, \theta, \eta]$.

Let K be a cyclic quartic extension field over $\mathbf{Q}$ with prime conductor. Then, before a quarter of a century, K has no power integral basis except for the 5-th cyclotomic field $\mathbf{Q}(\zeta_5)$ (see [10]).

Next we quote a criterion for non-monogenic phenomena.

Lemma 1.2 ([14, 17])**.** *Let ℓ be a prime number and let $F/\mathbf{Q}$ 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 conditions is satisfied, then Z_F has no power integral basis, i.e. F is non-monogenic;*

(1) $e\ell^f < n$ *if* $f = 1$;

or

(2) $e\ell^f \leqq n + e - 1$ *if* $f \geqq 2$.

Any cyclic extension F over $\mathbf{Q}$ with prime degree $\ell = [F : \mathbf{Q}] \geqq 5$ is non-monogenic except for the maximal real subfield F of the $(2\ell + 1)$-th cyclotomic field with prime conductor $2\ell + 1$, by M.-N. Gras [3] and it is proved by us that some type of imaginary extension has no power integral basis [17, 8, 16].

Finally we will propose a few open problems concerning Hasse's problem.

2. The rank $r \leq 2$ or $r \geq 4$

In the case of any quadratic field $K = \mathbf{Q}(\sqrt{a})$ $(r = 1)$, where $a \neq 0, 1$ square-free, is monogenic. Namely, the ring Z_K of integers in K, $Z_K = \mathbf{Z}[1, \omega]$, where ω is defined in the Section 1.

If K is a biquadratic extension field $(r = 2)$, the author showed that there exist infinitely many monogenic fields and non-monogenic ones within the estimation of the field indices:

$$\tilde{m}(K) = \min_{\text{primitive } \alpha \in K} \{\mathrm{Ind}(\alpha)\}, \text{ where } \mathrm{Ind}(\alpha) = \sqrt{\left|\frac{d_K(\alpha)}{d_K}\right|}$$

for the discriminant $d_K(\alpha)$ of a number α and the field discriminant d_K [11]. M. N. Gras and T. Tanoé obtained a necessary and sufficient condition such that $F = \mathbf{Q}(\sqrt{a_1}, \sqrt{a_2})$ is a monogenic biquadratic field [4]. Specifying their result, Y.Motoda proved that there exist infinitely many such fields [5].

Applying Lemma 1.2 for the prime number $\ell = 2$, by the ideal decomposition of a principal ideal (2) in K, we obtain for any such a field K of higher rank $r \geqq 4$.

Proposition 2.1 ([7]). *Let $a_1, a_2, \cdots, a_r$ be square-free rational integers and F be the field $\mathbf{Q}(\sqrt{a_1}, \sqrt{a_2}, \cdots, \sqrt{a_r})$ of degree $2^r, r \geqq 4$. Then F is non-monogenic.*

Next we obtained the followings for the octic field over $\mathbf{Q}$ whose Galois group is 2-elementary abelian.

Theorem 2.2 ([15]). *Let $F = \mathbf{Q}(\sqrt{a_1}, \sqrt{a_2}, \sqrt{a_3})$ be any octic field over $\mathbf{Q}$. Then F is non-monogenic except for the field $\mathbf{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{-3})$, namely the cyclotomic field $\mathbf{Q}(\zeta_{24})$ of conductor 24.*

In this article we explain the basic idea and show prospective examples for the theorem.

3. The rank r=3

If an octic field $\mathbf{Q}(\sqrt{a_1}, \sqrt{a_2}, \sqrt{a_3})$ with $a_j \equiv 1 \pmod 4$, that is, K has an odd conductor, then we have $e \cdot \ell^f \leqq 1 \cdot 2^2 < 8$ by Lemma 1.2 since prime number (2) is not ramified in K and the inert group T with respect to 2 in the Galois group $G(K/\mathbf{Q})$ is cyclic, hence the order f of T is less or equal to 2. Thus K is non-monogenic. On the other hand, we have in the case $a_1 \equiv 3 \pmod 4$, $a_2 \equiv a_3 \equiv 1 \pmod 4$, $e = 2$ and $f \leqq 2$ with rspect to (2). Then

$$e \cdot \ell^f = 2 \cdot 2^1 < 8 \quad \text{if } f = 1,$$

$$e \cdot \ell^f = 2 \cdot 2^2 \leqq 8 + 2 - 1 \quad \text{if } f = 2.$$

Then without loss of generality, for any octic field K, it is enough for us to investigate

$$K = \mathbf{Q}\left(\sqrt{4a_1}, \sqrt{4a_2}, \sqrt{a_3}\right)$$

where $a_1 = mn \equiv 3 \pmod 4$, $a_2 = dn \equiv 2 \pmod 4$, $a_3 = d_1m_1n_1\ell \equiv 1 \pmod 4$, $d = d_1d_2$, $m = m_1m_2$, $n = n_1n_2$, $d_2 \equiv 2 \pmod 4$, $d_1, m_1, n_1 \geqq 1$ and $dmn\ell$ is square-free.

Let $k = \mathbf{Q}\left(\sqrt{d_1m_1n_1\ell}\right)$ and $L = \mathbf{Q}\left(\sqrt{4mn}, \sqrt{4dn.}\right)$. When k and L are linearly disjoint, namely $d_1m_1n_1 = 1$, it is known that any such an octic field $K = kL$ is non-monogenic except for $K = \mathbf{Q}\left(\sqrt{-4}, \sqrt{8}, \sqrt{-3}\right) = \mathbf{Q}(\zeta_{24})$ (see [6]).

In general, for $d_1m_1n_1 \geqq 1$ we obtain

Theorem 3.1 ([15]). *Let*

$$K = \mathbf{Q}\left(\sqrt{4mn}, \sqrt{4dn}, \sqrt{d_1m_1n_1l}\right)$$

where $a_1 = mn \equiv 3 \pmod 4$, $a_2 = dn \equiv 2 \pmod 4$, $a_3 = d_1m_1n_1 \equiv 1 \equiv 3 \pmod 4$, $d = d_1d_2$, $m = m_1m_2$ $n = n_1n_2$ $d_2 \equiv 2 \pmod 4$, $d_1, m_1, n_1 \geqq 1$ *and* $dmnl$ *is square-free. Then* K *is non-monogenic except for the* 24*-th cyclotomic number field* $\mathbf{Q}(\zeta_{24})$.

In this section, we show a prospective example for Theorem 3.1. We consider the octic field

$$K = \mathbf{Q}\left(\sqrt{4 \cdot 3}, \sqrt{4 \cdot 2}, \sqrt{21}\right),$$

where $m = m_1m_2 = 3, n = n_1n_2 = 1, d = d_1d_2 = 2$ and $d_1m_1n_1\ell = 1 \cdot 3 \cdot 1 \cdot 7$. Then K contains seven quadratic subfields;

$$
\begin{aligned}
k_1 &= \mathbf{Q}(\sqrt{4\cdot mn}) = \mathbf{Q}(\sqrt{4\cdot 3}),\\
k_2 &= \mathbf{Q}(\sqrt{4\cdot dn}) = \mathbf{Q}(\sqrt{4\cdot 2}),\\
k_3 &= \mathbf{Q}(\sqrt{4\cdot mn\cdot dn}) = \mathbf{Q}(\sqrt{4\cdot 6}),\\
k_4 &= \mathbf{Q}(\sqrt{d_1m_1n_1\ell}) = \mathbf{Q}(\sqrt{21}),\\
k_5 &= \mathbf{Q}(\sqrt{4mn\cdot d_1m_1n_1\ell}) = \mathbf{Q}(\sqrt{4\cdot 7}),\\
k_6 &= \mathbf{Q}(\sqrt{4dn\cdot d_1m_1n_1\ell}) = \mathbf{Q}(\sqrt{4\cdot 42}),\\
k_7 &= \mathbf{Q}(\sqrt{4mn\cdot 4dn\cdot d_1m_1n_1\ell}) = \mathbf{Q}(\sqrt{4\cdot 14}),
\end{aligned}
$$

and seven biquadratic subfields;

$$
\begin{array}{ll}
L_1 = k_1k_2 = \mathbf{Q}(\sqrt{4\cdot 3}, \sqrt{4\cdot 2}), & L_2 = k_3k_5 = \mathbf{Q}(\sqrt{4\cdot 6}, \sqrt{4\cdot 7}),\\
L_3 = k_2k_4 = \mathbf{Q}(\sqrt{4\cdot 2}, \sqrt{21}), & L_4 = k_4k_5 = \mathbf{Q}(\sqrt{21}, \sqrt{4\cdot 7}),\\
L_5 = k_3k_7 = \mathbf{Q}(\sqrt{4\cdot 6}, \sqrt{4\cdot 14}), & L_6 = k_6k_7 = \mathbf{Q}(\sqrt{4\cdot 42}, \sqrt{4\cdot 14}),\\
L_7 = k_4k_7 = \mathbf{Q}(\sqrt{21}, \sqrt{4\cdot 14}). &
\end{array}
$$

Let $G =< \tau, \sigma, \rho >$ be the Galois group of the octic extension K over $\mathbf{Q}$, where three automorphisms are defined by

$$
\begin{array}{llll}
\tau: & \sqrt{3}\mapsto -\sqrt{3}, & \sqrt{2}\mapsto \sqrt{2}, & \sqrt{21}\mapsto \sqrt{21},\\
\sigma: & \sqrt{3}\mapsto \sqrt{3}, & \sqrt{2}\mapsto -\sqrt{2}, & \sqrt{21}\mapsto \sqrt{21},\\
\rho: & \sqrt{3}\mapsto \sqrt{3}, & \sqrt{2}\mapsto \sqrt{2}, & \sqrt{21}\mapsto -\sqrt{21}.
\end{array}
$$

Let $G(L/M)$ be the Galois group of an extension field L over an algebraic number field M. Denote $G(L/\mathbf{Q})$ by $G(L)$ and $G(K)$ by G. Then we have

$$
\begin{array}{ll}
G(k_1)\cong G/<\sigma,\rho>\cong<\tilde{\tau}>, & G(k_2)\cong G/<\tau,\rho>\cong<\tilde{\sigma}>,\\
G(k_3)\cong G/<\tau\sigma,\rho>\cong<\tilde{\tau}>, & G(k_4)\cong G/<\tau,\sigma>\cong<\tilde{\rho}>,\\
G(k_5)\cong G/<\tau\rho,\sigma>\cong<\tilde{\tau}>, & G(k_6)\cong G/<\tau,\sigma\rho>\cong<\tilde{\sigma}>,\\
G(k_7)\cong G/<\tau\sigma,\tau\rho>\cong<\tilde{\tau}>, &
\end{array}
$$

and

$$
\begin{array}{lllllll}
G(L_1) & \cong & G/\{<\sigma,\rho>\cap<\tau,\rho>\} & \cong & G/<\rho> & \cong & <\tilde{\tau},\tilde{\sigma}>,\\
G(L_2) & \cong & G/\{<\tau\sigma,\rho>\cap<\tau\rho,\sigma>\} & \cong & G/<\tau\sigma\rho> & \cong & <\tilde{\tau},\tilde{\rho}>,\\
G(L_3) & \cong & G/\{<\tau,\rho>\cap<\tau,\sigma>\} & \cong & G/<\tau> & \cong & <\tilde{\sigma},\tilde{\rho}>,\\
G(L_4) & \cong & G/\{<\tau,\sigma>\cap<\tau\rho,\sigma>\} & \cong & G/<\sigma> & \cong & <\tilde{\tau},\tilde{\rho}>,\\
G(L_5) & \cong & G/\{<\tau\sigma,\rho>\cap<\tau\rho,\tau\sigma>\} & \cong & G/<\tau\sigma> & \cong & <\tilde{\tau},\tilde{\rho}>,\\
G(L_6) & \cong & G/\{<\tau,\sigma\rho>\cap<\tau\sigma,\tau\rho>\} & \cong & G/<\sigma\rho> & \cong & <\tilde{\tau},\tilde{\sigma}>,\\
G(L_7) & \cong & G/\{<\tau,\sigma>\cap<\tau\sigma,\tau\rho>\} & \cong & G/<\tau\sigma> & \cong & <\tilde{\tau},\tilde{\rho}>,
\end{array}
$$

where for a subgroup H of G and $\alpha\in G$, $\tilde{\alpha}$ means a coset αH in the residue class group G/H.

Assume the ring Z_K has a power basis; $Z_K = Z[\xi]$ for a suitable primitive integer in K. Then the different

$$\mathfrak{d}_K(\xi) = (\xi - \xi^\tau)(\xi - \xi^\sigma)(\xi - \xi^\rho)(\xi - \xi^{\tau\sigma})(\xi - \xi^{\tau\rho})(\xi - \xi^{\sigma\rho})(\xi - \xi^{\tau\sigma\rho})$$

of a number ξ is equal to the field different $\mathfrak{d}_K$ of the field K. Then it holds that

$$(d_K(\xi)) = (N_K(\mathfrak{d}_K(\xi))) = \mathrm{N}_K(\mathfrak{d}_K) = (d_K),$$

where for a number α and an ideal $\mathfrak{a}$ in an algebraic number field $F/\mathbf{Q}$, $N_F(\alpha)$ and $\mathrm{N}_F(\mathfrak{a})$ mean the norm map of α and of $\mathfrak{a}$ with respect to $F/\mathbf{Q}$, respectively and for a number β in K, (β) means the principal ideal generated by β. We denote the discriminant of a number α and of a field F by $d_F(\alpha)$ and d_F, respectively.

By Hasse's discriminant-conductor formula, we have

$$d_K = \prod_{j=1}^{7} d_{k_j} = (4\cdot 3)(4\cdot 2)(4\cdot 6)(21)(4\cdot 7)(4\cdot 42)(4\cdot 14) = 2^{16}\cdot 3^4\cdot 7^4,$$

We consider the following identity whose terms are fixed by the subgroup $<\sigma,\rho>= H_{k_1}$ in G;

$$(\xi - \xi^\sigma)(\xi - \xi^\sigma)^\rho - (\xi - \xi^\rho)(\xi - \xi^\rho)^\sigma + (\xi - \xi^{\sigma\rho})(\xi - \xi^{\sigma\rho})^\sigma = 0. \quad (3.1)$$

Since the difference $\xi - \xi^\sigma$ is divisible by the relative different $\mathfrak{d}_{K/L_4}$, the product $(\xi - \xi^\sigma)(\xi - \xi^\sigma)^\rho$ is divisible by $\mathfrak{d}_{K/L_4}\cdot\mathfrak{d}^\rho_{K/L_4}$ By the transitive law of different,

$$\mathfrak{d}_K = \mathfrak{d}_{L_4}\cdot\mathfrak{d}_{K/L_4},$$

we have $\mathrm{N}_K\mathfrak{d}_K = \mathrm{N}_{K/L_4}(\mathrm{N}_{L_4}(\mathfrak{d}_{L_4}))\mathrm{N}_{L_4}(\mathrm{N}_{K/L_4}(\mathfrak{d}_{K/L_4}))$, where for a field tower $\mathbf{Q}\subset F\subset L$ of algebraic number fields, $N_{L/F}$ means the relative norm map with respect to L/F and we denote the relative discriminant $\mathrm{N}_{L/F}\mathfrak{d}_{L/F}$ by $d_{L/F}$. Then we obtain $(d_K) = (d_{L_4})^2(d_{K/L_4})^4$, namely $2^{16}\cdot 3^4\cdot 7^4 = (2^4\cdot 3^2\cdot 7^2)^2(d_{K/L_4})^4$. Then $(2^2) = d_{K/L_4}$, hence $(2)(2) = \mathfrak{d}_{K/L_4}(\mathfrak{d}_{K/L_4})^\rho$. In the same way since the differences $\xi - \xi^\rho$, $\xi - \xi^{\sigma\rho}$ are divisible by $\mathfrak{d}_{K/L_1}$, $\mathfrak{d}_{K/L_6}$, respectively, we have $(7) = d_{K/L_1}$ and $(1) = d_{K/L_6}$, hence $(7) = \mathfrak{d}_{K/L_1}\mathfrak{d}^\sigma_{K/L_1}$ and $(1) = \mathfrak{d}_{K/L_6}\mathfrak{d}^\sigma_{K/L_6}$.

Since the number ξ generates a power basis, then using the identity (3.1) we obtain

$$7E_1 + 2^2E_2 + 1E_3 = 0$$

for suitable units $E_j (1 \leqq j \leqq 3)$ in the fixed field $F_{<\sigma,\rho>} = k_1 = \mathbf{Q}(\sqrt{4\cdot 3})$ with notations $7 = l$, $2^2 = 2d_2$, $1 = d_1$, for three partial products in the equation (3.1), because it should follow that $(\xi-\xi^{\rho})(\xi-\xi^{\rho})^{\sigma}=d_{K/L_1}$, $(\xi-\xi^{\sigma})(\xi-\xi^{\sigma})^{\rho}=d_{K/L_4}$, $(\xi-\xi^{\sigma\rho})(\xi-\xi^{\sigma\rho})^{\sigma}=d_{K/L_6}$ as ideals.

With general notations $7=\ell$, $2^2=2d_2$, $1=d_1$, we have

$$\ell E_1+\ 2d_2E_2\ +\ d_1E_3\ =\ 0\quad\text{in}\quad \mathbf{Q}\left(\sqrt{4mn}\right), \tag{3.2}$$

$$\ell \bar{E}_1+\ 2d_2\bar{E}_2\ +\ d_1\bar{E}_3\ =\ 0\quad\text{in}\quad \mathbf{Q}\left(\sqrt{4mn}\right). \tag{3.3}$$

If the rank $r_{4\cdot 3}$ of the equations (3.2), (3.3) in $\mathbf{Q}(\sqrt{4\cdot 3})$ is one, we have $\ell\pm 2d_2\pm d_1=0$ i.e. $\ell=\pm 2d_2\pm d_1<2d_2+d_1=5$, which is impossible. Then the rank $r_{4\cdot 3}$ is two. By $E_j=\varepsilon^{e_j}$, let $e_1=\min_{1\leqq j\leqq 3}\{e_j\}$. Thus $\ell+2d_2\varepsilon^{e}+d_1\varepsilon^{f}=0$ and $e,f\geqq 0$ holds.

Put

$$\varepsilon^{g}=u_g+v_g\sqrt{3}.$$

Then, for *unknown* valuables ℓ, $2d_2$ and d_1, it holds that

$$2d_2:d_1=\begin{vmatrix}\varepsilon^{f} & 1\\ \bar{\varepsilon}^{f} & 1\end{vmatrix}:\begin{vmatrix}1 & \varepsilon^{e}\\ 1 & \bar{\varepsilon}^{e}\end{vmatrix}=2v_f\sqrt{3}:-2v_e\sqrt{3}.$$

Hence, $2d_2/d_1=4/1=v_f/-v_e$, namely $|v_f|=4|v_e|$.

$$\ell:d_1=\begin{vmatrix}\varepsilon^{e} & \varepsilon^{f}\\ \bar{\varepsilon}^{e} & \bar{\varepsilon}^{f}\end{vmatrix}:\begin{vmatrix}1 & \varepsilon^{e}\\ 1 & \bar{\varepsilon}^{e}\end{vmatrix}=\varepsilon^{e}\cdot\bar{\varepsilon}^{e}\begin{vmatrix}1 & \varepsilon^{f-e}\\ 1 & \bar{\varepsilon}^{f-e}\end{vmatrix}:\begin{vmatrix}1 & \varepsilon^{e}\\ 1 & \bar{\varepsilon}^{e}\end{vmatrix}=-2v_{f-e}:-2v_e.$$

Hence, $\ell/d_1=7/1=v_{f-e}/v_e$, namely $|v_{f-e}|=7|v_e|$ and $f-e>e$, which is a contradiction to $0<|v_{f-e}|<|v_f|=4|v_e|$.

Then the equations (3.2), (3.3) are impossible in $\mathbf{Q}(\sqrt{3})$. Therefore the octic field $\mathbf{Q}(\sqrt{3},\sqrt{2},\sqrt{21})$ is non-monogenic.

However we could not always determine the monogenesis of the quartic subfields in K from the following necessary condition (3.4). In fact we can find an integral power basis for the field $L_1=k_1k_2=\mathbf{Q}(\sqrt{4\cdot 3},\sqrt{4\cdot 2})$ as follows.

We can confirm that the ring Z_{L_1} of integers in L_1 has an integral power basis $\mathbf{Z}[1,\alpha,\beta,(\alpha+1)\beta/2]$ for $\alpha=\sqrt{3}$ and $\beta=\sqrt{2}$. We select an integer $\xi=\beta-(\alpha+1)\beta/2$. Then it holds that

$$d_{L_1}(\xi)=3^2\cdot 2^8=1\cdot(4\cdot 3)(4\cdot 2)(4\cdot 6)=d_{L_1}.$$

Then the field L_1 is monogenic. In fact, the identity $(-6)-(-4)-(-2)=0$ holds for $(\xi-\xi^{\tau})(\xi-\xi^{\tau})^{\sigma}=-6$, $(\xi-\xi^{\sigma})(\xi-\xi^{\sigma})^{\tau}=-4$ and $(\xi-\xi^{\tau\sigma})(\xi-\xi^{\tau\sigma})^{\sigma}=-2$.

Next we consider the second quartic subfield $L_2 := \mathbf{Q}(\sqrt{4\cdot 6}, \sqrt{4\cdot 7})$ in K. Since the Galois group $G(L_2/\mathbf{Q})$ coincides with $< \tau, \varrho >$, we have for an integer $\xi \in Z_{L_2}$,

$$(\xi - \xi^{\tau})(\xi - \xi^{\tau})^{\varrho} - (\xi - \xi^{\varrho})(\xi - \xi^{\varrho})^{\tau} - (\xi - \xi^{\tau\varrho})(\xi - \xi^{\tau\varrho})^{\varrho} = 0 \qquad (3.4)$$

For three quadratic subfields

$$k_3 = \mathbf{Q}(\sqrt{4\cdot 6}), \quad k_5 = \mathbf{Q}(\sqrt{4\cdot 7}), \quad k_6 = \mathbf{Q}(\sqrt{4\cdot 42}),$$

in L_2, we calculate each of the relative discriminants

$$\begin{aligned} \pm d_{L_2/k_3} &= \sqrt{d_{L_2}/d_{k_3}^2} &= \sqrt{2^8\cdot 3^2\cdot 7^2/(2^3\cdot 3)^2} &= 2\cdot 7, \\ \pm d_{L_2/k_5} &= \sqrt{d_{L_2}/d_{k_5}^2} &= \sqrt{2^8\cdot 3^2\cdot 7^2/(2^2\cdot 7)^2} &= 2^2\cdot 3, \\ \pm d_{L_2/k_6} &= \sqrt{d_{L_2}/d_{k_6}^2} &= \sqrt{2^8\cdot 3^2\cdot 7^2/(2^3\cdot 3\cdot 7)^2} &= 2. \end{aligned}$$

If the ring Z_{L_2} has an integral power basis, which is generated by ξ, then the equation (3.4) should hold. However since

$$2 \pm 2\cdot 7 \pm 2^2\cdot 3 = 2 - 14 + 12 = 0!$$

would happen, we can not deduce a contradiction. But, on the first partial different $(\xi - \xi^{\tau})(\xi - \xi^{\tau})^{\rho}$ for any integer $\xi = a\alpha + b\beta + c\gamma$ in Z_{L_2}, we have the value $(2a+c)^2\cdot 6 - (2b)^2\cdot 7 = 2[3(2a+c)^2 - 14b^2]$. Then we consider the Diophantine equation $3X^2 - 14Y^2 = \pm 1$. Assume that this equation has an integral solution. Then in the case of $-1, Y^2 \equiv -1 \pmod 3$; which is impossible. In the case of $+1$, it holds that $X_1^2 - 3\cdot 2\cdot 7Y^2 = 3$ with $X_1 = 3X$. Since 3 is a quadratic non-residue modulo 7, this case is also impossible. Then we obtain that $|(\xi - \xi^{\tau})(\xi - \xi^{\tau})^{\rho}| > 2$. Namely the integral closure Z_{L_2} in the second quartic subfield has no integral power basis.

Problems.

- Characterize Hasse's Problem for the cyclic quartic fields over the rationals $\mathbf{Q}$.
- Let the fields K run through all the real octic fields whose Galois groups are 2-elementary abelian. Then evaluate the values of

$$\inf_K \tilde{m}(K) \quad \text{and} \quad \inf_K m(K),$$

respectively. Here, $\tilde{m}(K)$ denotes the field index of K and $m(K)$ the common index $\gcd(\mathrm{Ind}(\alpha); \alpha \in Z_K)$ for the integral closure Z_K of the field K.

Acknowledgement. I wish to express my gratitude Prof. Mohammed Ayadi for his courteous invitation to CIANTA 2006 at Oujda.

References

[1] D. S. Dummit & H. Kisilevsky – Indices in cyclic cubic fields, in *Number theory and algebra*, Academic Press, New York, 1977, p. 29–42.

[2] I. Gaál – *Diophantine equations and power integral bases*, Birkhäuser Boston Inc., Boston, MA, 2002, New computational methods.

[3] M.-N. Gras – Non monogénéité de l'anneau des entiers des extensions cycliques de $\mathbf{Q}$ de degré premier $l \geq 5$, *J. Number Theory* **23** (1986), no. 3, p. 347–353.

[4] M.-N. Gras & F. Tanoé – Corps biquadratiques monogènes, *Manuscripta Math.* **86** (1995), no. 1, p. 63–79.

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

[6] Y. Motoda & T. Nakahara – Monogenesis of algebraic number fields whose galois groups are 2-elementary abelian, *Proceedings of the 2003 Nagoya Conference "Yokoi-Chowla Conjecture and Related Problems", Edited by S.-I. Katayama, C. Levesque and T. Nakahara, Furukawa Total Pr.Co. Saga* (2004), p. 91–99.

[7] ———, Power integral bases in algebraic number fields whose galois groups are 2-elementary abelian, *Arch. Math.* **83** (2004), p. 309–316.

[8] Y. Motoda, T. Nakahara & S. Shah – On a problem of Hasse for certain imaginary abelian fields, *J. Number Theory* **96** (2002), p. 326–334, [cf. http://dlwww.dl.saga-u.ac.jp/contents/diss/GI00000879/motodaphd.pdf].

[9] Y. Motoda, K. Park & T. Nakahara – On power integral bases of the 2-elementary abelian extension fields, *Trends in Mathematics* **9-1** (2006), p. 55–63.

[10] T. Nakahara – On cyclic biquadratic fields related to a problem of Hasse, *Mh. Math.* **94** (1982), p. 125–132.

[11] ———, On the indices and integral bases of non-cyclic but abelian biquadratic fields, *Arch. Math.* **41** (1983), p. 504–508.

[12] ———, On the indices and integral bases of abelian biquadratic fields, *RIMS Kōkyūroku, Distribution of values of arithmetic functions* **517** (1984), p. 91–100.

[13] ———, On the minimum index of a cyclic quartic field, *Arch. Math.* **48** (1987), p. 322–325.

[14] ———, A simple proof for non-monogenesis of the rings of integers in some cyclic fields, in *Advances in number theory (Kingston, ON, 1991)*, Oxford Sci. Publ., Oxford Univ. Press, New York, 1993, p. 167–173.

[15] K. PARK, Y. MOTODA & T. NAKAHARA – On integral bases of certain octic abelian fields, Submitted.

[16] S. SHAH – Monogenesis of the ring of integers in a cyclic sextic field of a prime conductor, *Rep. Fac. Sci. Engrg. Saga Univ. Math.* **29-1** (2000), p. 1–10.

[17] S. SHAH & T. NAKAHARA – Monogenesis of the rings of integers in certain imaginary abelian fields, *Nagoya Math. J.* **168** (2002), p. 85–92.

TORU NAKAHARA
Department of Mathematics, Faculty of
Science and Engineering, Saga University,
Saga 840-8502, Japan.
Current address:
NUCES, Peshawar Campus,
160-Industrial Estate, Hayatabad,
Peshawar, N.W.F.P.
The Islamic Republic of Pakistan
nakahara@ms.saga-u.ac.jp,
toru.nakahara@nu.edu.pk