Monogenity of Biquadratic Fields Related to Dedekind-Hasse’s Problem

Mamoona Sultan
National University of Computer & Emerging Sciences,
Peshawar, Khyber Pakhtunkhwa, the Islamic Republik of Pakistan
Email: p109957@nu.edu.pk

Yoshifumi Kôhno
Christ Church in Japan,
059-1433 Hokkaido Yuhutugun, Abiracyo Toasa 42, Japan
Email: yoshikohno080928@d1.dion.ne.jp

Toru Nakahara
Qarshi University,
8km from Thokar Niaz Baig, Canal Bank Road, Opposite Izmir Town, Lahore,
the Islamic Republik of Pakistan
Email: toru.nakahara@nu.edu.pk, toru.nakahara@qu.edu.pk, nakahara@ms.saga-u.ac.jp

Abstract. The aim of this paper is to determine the monogenity of imaginary, and real biquadratic fields $K$ over the field $Q$ of rational numbers and the relative monogenity of $K$ over its quadratic subfield $k$. To characterize such phenomena it is necessary to determine an integral basis of the field $K$ and to evaluate the relative norm of the different $d(\xi)$ with respect to $K/k$ of an integer $\xi$ in $K$. Here $d(\xi)$ is defined by $\prod_{\rho \in G \setminus \{1\}} (\xi - \xi^\rho)$, where $\xi - \xi^\rho$ denotes the partial different of an integer $\xi$ in $K$, and $G$ and $1$ denote the Galois group of $K/Q$ and the identity embedding of $K$, respectively. For the succinct proof of non-monogenity, we consider a single linear Diophantine equation consisted of the partial different with unit coefficients.

AMS (MOS) Subject Classification Codes: 11R04, 11R11, 11R29
Key Words: Monogenity, Biquadratic field, Discriminant, Integral basis

1. INTRODUCTION

In the 1960’s Hasse proposed to characterize an algebraic number field $K$ whose ring $Z_K$ of integers has a power integral basis or not. Let $p$ be a prime number and $\zeta_{p^r}$ be a primitive $p^r$th root of unity, which is a root of an irreducible cyclotomic polynomial $\Phi_{p^r}(x) = (x^{p^r} - 1)/(x^{p^r-1} - 1)$ over $Q$ with $\zeta_2 = -1$, $\zeta_3 = (-1 + \sqrt{-3})/2$, $\zeta_4 = \sqrt{-1}$ and $\zeta_{p^r} = \exp(2\pi i/p^r), p \geq 2, e \geq 1$.

Then for the Eisenstein field $k_3 = Q(\zeta_3) = Q(\sqrt{-3})$, the Gauß field $k_4 = Q(\sqrt{-1})$ and a
cycloptic field \(k_{p^e} = \mathbb{Q}(\zeta_{p^e})\), it is known that \(Z_{k_3} = \mathbb{Z}[1, \zeta_3], Z_{k_4} = \mathbb{Z}[1, \sqrt{-1}]\) and \(Z_{k_{p^e}} = \mathbb{Z}[1, \zeta, \cdots, \zeta^{p-1}(p-1)^{-1}]\) with \(\zeta = \zeta_{p^e}\) as a \(\mathbb{Z}\) – free module of rank \((p - 1)!\) [15]. Each of the fields is called monogenic. For an algebraic number field \(K\) over the rationals \(\mathbb{Q}\), \(Z_K\) denotes the ring of integers in \(K\). Let \(\mathbb{Q} \subset F \subset K\) be an algebraic number field tower. It is said that a field \(K\) is relatively monogenic in the relative field extension \(K/F\) of degree \(n\) or equivalently, \(Z_K\) has a power integral basis of rank \(n\) over \(Z_F\) if for a suitable integer \(\alpha \in Z_K, Z_K\) coincides with the \(Z_F\)-module \(Z_F[\alpha] = Z_F \cdot 1 + Z_F \cdot \alpha + \cdots + Z_F \cdot \alpha^{n-1}\) of rank \(n\) over \(Z_F\). In the case of \(F = \mathbb{Q}\), we say that \(K\) is monogenic or \(Z_K\) has a power integral basis [4]. Then to determine the monogenity of \(Z_K = Z_F[\alpha]\) with a suitable integer \(\alpha\) or \(Z_K \neq Z_F[\beta]\) for any integer \(\beta\) in \(F\) is called Dedekind-Hasse’s problem. Let \(d_F\) and \(d_F(\alpha)\) denote the field discriminant and the discriminant of a number \(\alpha\) in \(F\) and the Index \(\text{Ind}_F(\alpha)\) of a number \(\alpha\) is defined by \(\sqrt{|d_F(\alpha)/d_F|}\). It is known that Dedekind’s example of a cubic field \(K = \mathbb{Q}(\theta)\) is non-monogenic, where \(\theta\) satisfies a cubic irreducible equation; \(x^3 - x^2 - 2x - 8 = 0\) with the discriminant \(d_K(\theta) = \{(\theta - \theta^2)(\theta - \theta^3)(\theta^2 - \theta^3)^2\} = 2^2 \cdot (-503)\) of \(\theta\) and a non-trivial conjugate map \(\sigma\) on \(K\) [3]. In fact, \(\{1, \theta, \eta\}\) with \(\eta = \theta(\theta - 1)/2\) is an integral basis of \(K\) and it holds that \(\theta^4 \in \mathbb{Z}[\theta, \eta]\) for any element \(\zeta = \zeta(1, \theta, \eta)\) and \(\eta^2 = (\theta, \theta - 1)\). Here the field discriminant \(d_K\) is defined by \(\det(B)\). Hence \(d_K(\theta) = \det(A)^2 d_K\). Here the field discriminant \(d_K\) is defined by \(\det\left(\begin{smallmatrix} \sigma \eta & \eta^2 & \eta^6 \\ 1 & \sigma & \sigma^2 \\ 0 & 1 & 0 \end{smallmatrix}\right)\) and \(\text{Ind}_K(\theta) = |\det(A)| = 2\). Then it follows that the ring \(\mathbb{Z}[1, \theta, \eta^2]\) is a proper subring of \(Z_K\). Moreover for any integer \(\xi = x + y\theta + z\eta\), we know that \(\text{Ind}_K(\xi) \equiv 0 \pmod{2}\), namely \(Z_K\) has no power integral basis. In this paper we consider the problem on a family of imaginary, and real biquadratic fields \(K = \mathbb{Q}(\sqrt{DM}, \sqrt{DN})\), where \(DMN\) is a square free integer with \(1 \leq |D|, 1 < N, M\) as an analogue of a work by Y. Motoda [9].

**Theorem 1.1.** Let \(K\) be a biquadratic field \(\mathbb{Q}(\sqrt{DM}, \sqrt{DN})\), where \(DMN\) is square free with \(DM \equiv DN \equiv 3, MN \equiv 1 \pmod{4}\) and \(1 \leq |D|, 1 < N, 1 < M\). Then \(K\) has an integral basis \(\mathbb{Z}[1, \sqrt{DM}, \sqrt{DN}]\) with the field discriminant \(d_K = 2^3 D^2 M^2 N^2\) and \(Z_K\) has a relative power integral basis \(Z_k[1, \sqrt{DM}]\) over \(Z_k\) with a quadratic subfield \(k = \mathbb{Q}(\omega)\) and \(\omega = \frac{1 + \sqrt{MN}}{2}\). But, if \(4D \pm M \pm N \neq 0\) holds, then \(Z_K\) has no power integral basis.

**Corollary 1.2.** There exist infinitely many non-monogenic biquadratic fields.

**Corollary 1.3.** Using the same notation as in Theorem 1.1, there exist monogenic biquadratic fields for \(D = \pm 1, M = N = \pm 4\).

Our theorem gives a negative solution to the problem 6 in [11]. An explicit integral basis of any biquadratic field \(K\) is shown in K. S. Williams using evaluation modulo powers of 2 without the process of a relative extension \(K/k/\mathbb{Q}\) for a quadratic subfield \(k\) of \(K\) [16]. On the family of imaginary biquadratic fields \(K\) with \(D < 0\) a complete classification of monogenity has been given by G. Nyul using the evaluation of the full norm of the different \(d_K(\xi)\) for any element \(\xi \in K\) [12]. On the contrary, based on the works of M.-N. Gras, F. Tanoè, it is shown that there exist infinitely many real monogenic biquadratic fields not depending on Dirichlet’s theorem on arithmetic progression [9, 4]. We prove our theorem by the consideration of the relative norm with respect to \(K/k\) of partial differents \(\xi - \xi^p\) of the different \(\partial(\xi)\) of an integer \(\xi\), and a single linear Diophantine equation consisted of three relative norms of the partial differents with unit coefficients. Here \(\partial(\xi)\)
is defined by \( \prod_{\rho \in G \setminus \{1\}} (\xi - \xi^\rho) \) with Galois group \( G \) of \( K/Q \) and the identity embedding \( i \) of \( K \) for a family of certain biquadratic fields. Related works are found in [1, 2, 5, 6, 8, 10, 13, 14].

2. INTEGRAL BASES

Let \( K \) be a biquadratic field \( Q(\sqrt{DM}, \sqrt{DN}) \) with a square free \( DMN, 1 \leq |D|, 1 < N, 1 < M \) and \( DM \equiv DN \equiv 3 \pmod{4}, MN \equiv 1 \pmod{4} \). Let \( k \) be a quadratic subfield \( Q(\sqrt{DM}) \).

Then it holds that \( K = k[1, \omega] = Q[1, \sqrt{DM}, \omega, \gamma_0] \) with \( \omega = \frac{1 + \sqrt{MN}}{2} \) and \( \gamma_0 = \sqrt{DM} \omega = \frac{\sqrt{DM} + \sqrt{DN}}{2} \).

Let \( k = Q(\sqrt{DM}), k_1 = Q(\sqrt{MN}) \) and \( k_2 = Q(\sqrt{DN}) \) be the quadratic subfields of \( K \).

Let \( G = \text{Gal}(K/Q) \) be the Galois group of \( K \) over \( Q \) generated by embeddings \( \sigma \) and \( \tau \). Let \( H_k = \langle \sigma \rangle, H_k = \langle \tau \rangle \) and \( H_k = \langle \sigma \tau \rangle \) be the Galois subgroups corresponding to subfields \( k, k_1 \) and \( k_2 \) of \( K \), respectively. Then it holds that

\[
\begin{align*}
\sigma : \sqrt{DM} & \mapsto \sqrt{DM}, \quad \sqrt{MN} \mapsto -\sqrt{MN}, \quad \sqrt{DN} \mapsto -\sqrt{DN}, \\
\tau : \sqrt{DM} & \mapsto -\sqrt{DM}, \quad \sqrt{MN} \mapsto \sqrt{MN}, \quad \sqrt{DN} \mapsto -\sqrt{DN}, \\
\sigma \tau : \sqrt{DM} & \mapsto -\sqrt{DM}, \quad \sqrt{MN} \mapsto -\sqrt{MN}, \quad \sqrt{DN} \mapsto \sqrt{DN}.
\end{align*}
\]

First we show that an integral basis of \( k \). Let \( \xi = \sqrt{DM} + \sqrt{MN} \in Z_k \cap k \), and hence \( a, b \in Z \) holds by \( Z_k \cap k = Z_k = Z[1, \sqrt{DM}] \).

Put \( \xi_1 = \xi - a - b \sqrt{DM} \) with \( a, b \in Z \). Then \( \xi_1 = \omega + d \gamma_0 \in Z_k \) holds. If we choose \( d = 0 \), then \( c \in Z \). Put \( \xi_2 = \xi_1 - c \omega \) with \( c \in Z \). By \( \xi_2 = d \sqrt{DM} + e \sqrt{DN} = d \sqrt{DM} + e \sqrt{DN} \), \( \xi_2 = d \sqrt{DM} + \sqrt{DN} = d \sqrt{DM} + \sqrt{DN} \), which is denoted by \( \xi_3 \) should belong to \( Z_k \) as \( d \sqrt{DN} \in Z \).

Put \( \gamma = \sqrt{DM} + \sqrt{DN} \). Thus by \( T_{K/k}(\xi) = c \gamma + d \gamma = dv \sqrt{DM} \in Z_k, d \in Z \) is deduced. Here, \( T_{K/k}(\cdot) \) means the relative trace with respect to \( K/k \). Put \( Z'_k = Z[1, \sqrt{DM}, \omega, \gamma] \). Therefore if \( \xi \in Z_K \), it holds that \( \xi \in Z'_k \), namely \( Z'_K \subseteq Z'_k \).

Conversely for any \( \xi = s + t \sqrt{DM} + u \omega + v \gamma \in Z'_K \) with \( s, t, u, v \in Z \), we have \( T_{K/k}(\xi) = \xi + \xi' = 2s + 2t \sqrt{DM} + u + v \sqrt{DM} \in Z_k \) and \( N_{K/k}(\xi) = \xi \xi' = 2 \xi' \).

\[
(2s + t \sqrt{DM} + u + v \sqrt{DM})^2 = (u \sqrt{MN} + v \sqrt{DN})^2 = (u^2 + v^2 DM + 2uv \sqrt{DM}) - (u^2 + v^2 DN + 2uv \sqrt{DN}) \equiv 0 \pmod{4Z_k}.
\]

Here, \( N_{K/k}(\cdot) \) means the relative norm with respect to \( K/k \). In fact, because of \( u^2 + v^2 (1-MN) + 2uv(1-N) \equiv 0 \pmod{4} \) and \( 2uv(1-N) \equiv 0 \pmod{4} \), we obtain \( \xi \in K \cap \bar{Z} = Z_k \). Here \( \bar{Z} \) denotes the ring of integral closure over \( Q \). Thus \( Z'_K \subseteq Z_K \) holds. Then for a biquadratic field \( K \), \( Z_K \) coincides with \( Z[1, \sqrt{DM}, \sqrt{DM} + \sqrt{DN}] \). □

3. RELATIVE MONOGENICITY OF A BIA QUADRATIC FIELD OVER A QUADRATIC SUBFIELD

Assume that \( Z_K = Z_{k_1}[1, \omega] \) over \( Z_{k_1} \), for \( Z_{k_1} = Z[1, \omega] \) and \( \eta = a + b \sqrt{DM} \) with \( a, b \in Q \).

Thus \( Z_K = Z[1, \sqrt{DM}, a + b \sqrt{DM}] \) is a free module of rank 4 over \( Q \). Then we show that \( Z_K \) has a relative integral basis over \( Z_{k_1} \). Let \( d_K(\alpha, \beta, \gamma, \delta) \) be the discriminant \( \det (\alpha^t \beta^t \gamma^t \delta) \) for a column vector \( \mu = (\mu, \mu^\sigma, \mu^\tau, \mu^\sigma \tau) \).

Then by \( d_K(\alpha, \beta, \gamma, \delta) = d_K(\alpha, \beta, \gamma, \delta) \), it follows that
\[d_K(1, \omega, a + b\sqrt{DM}, a\omega + b\sqrt{DM} + \sqrt{DN})\]
\[= d_K(1, \omega, b\sqrt{DM}, b\sqrt{DM} + \sqrt{DN})\]
\[= b^{2+\frac{1}{2}} d_K(1, \omega, \sqrt{DM}, \sqrt{DM} + \sqrt{DN})\]
\[= b^4 d_K(1, \omega, (2^2D\sqrt{MN})^2\sqrt{DN})\]
\[= b^4 M^2 N^2.\]

Thus for \(\eta = a + b\sqrt{DM}\) with \(a = 0, b = 1\), \(Z_K\) has a relative power integral basis \(\{1, \eta\}\) over \(Z_{k_1}\).

4. Monogeneity of a Biquadratic Field

Let \(K\) be an imaginary, or real biquadratic field \(Q(\sqrt{DM}, \sqrt{DN})\) with positive square free relatively prime integers \(|D| \geq 1, N > 1, M > 1\) and \(DM \equiv DN \equiv 3, MN \equiv 1 \pmod{4}\). Let \(k = Q(\sqrt{DM})\) and \(k_2 = Q(\sqrt{DN})\) be quadratic subfields of \(K\) and \(k_1 = Q(\sqrt{MN})\) be a real one. Let \(G(K/Q)\) be the Galois group \(G\) of \(K\) over \(Q\) generated by embeddings \(\sigma\) and \(\tau\). Let the subfields \(k, k_1, k_2\) of \(K\) have corresponding Galois subgroups \(H_k = < \sigma >, H_{k_1} = < \tau >\) and \(H_{k_2} = < \sigma \tau >\) in \(G\), respectively. Let \(X\) denote the character group corresponding to \(G(K/Q)\) generated by \(\chi\) and \(\lambda\), which denote primitive characters of order 2 defined by \(\chi(\sigma) = -1, \chi(\tau) = 1\) and \(\lambda(\sigma) = \lambda(\tau) = -1\). By virtue of Hasse’s conductor-discriminant formula, the field discriminant \(d_K\) of \(K\) coincides with
\[
\prod_{\psi \in X} f_{\psi} = f_{\psi} \cdot f_{k} \cdot f_{\lambda} \cdot f_{\lambda^2} = 1 \cdot 2^2|DM| \cdot 2^2|DN| \cdot MN = 2^4 \cdot D^2 \cdot M^2 \cdot N^2,
\]
where \(f_{\psi}\) denote the conductor corresponding to a character \(\psi\) of \(X\) with the principal character \(\chi^0\) [7, 15]. Assume that the field \(K\) has a power integral basis for some suitable integer \(\xi = a + b\sqrt{DM} + c\sqrt{MN} + d\sqrt{DN}\) in \(K\) such that
\[Z_K = Z[\xi] = Z[1, \xi, \xi^2, \xi^3].\]

For an algebraic number field tower \(Q \subset F \subset L\) with the Galois group \(G = G(L/Q)\), the field different \(\mathfrak{d}_L\) is defined as an ideal
\[\beta - \beta^p; \forall \beta \in Z_L, \forall p \in G(L/Q)\]
of \(L\), and the relative field different \(\mathfrak{d}_{L/F}\) as an ideal
\[\gamma - \gamma^p; \forall \gamma \in Z_L, \forall p \in G(L/F)\]
of \(L/F\). By the assumption \(Z_K = Z[\xi]\), it holds that
\[\mathfrak{d}_K(\xi) = (N_K(\mathfrak{d}_K(\xi))) = (N_K(\mathfrak{d}_K)) = (d_K),\]
where \(a\) means the principal ideal generated by a number \(a\) in \(K\) and \(N_F(a), N_P(a)\) are the norms of \(a\) and of \(a\) with respect to \(F/Q\), respectively. Hence for the biquadratic field \(K\), the different \(\mathfrak{d}_K(\xi)\) of an element \(\xi \in Z_K\) is given by \((\xi - \xi^\sigma)(\xi - \xi^\sigma^T)(\xi - \xi^\sigma T)\).

Thus it holds that
\[N_K(\mathfrak{d}_K(\xi)) = N_K((\xi - \xi^\sigma)(\xi - \xi^\sigma T)(\xi - \xi^\sigma T)) = N_K(N_K((\xi - \xi^\sigma)(\xi - \xi^\sigma T)(\xi - \xi^\sigma T))) = N_K(((\xi - \xi^\sigma)(\xi - \xi^\sigma)(\xi - \xi^\sigma T))((\xi - \xi^\sigma T)(\xi - \xi^\sigma T)(\xi - \xi^\sigma T)))\]
\[= (\xi - \xi^\sigma)(\xi - \xi^\sigma T)(\xi - \xi^\sigma T)(\xi - \xi^\sigma)(\xi - \xi^\sigma T)(\xi - \xi^\sigma T).
\]
Proof of Corollary 1.2. Put $N = 8D_0t + M_0$ with a valuable $t$ ($1 \leq t$) for $D = D_0 > 0$, $M = M_0 > 0$ and $(8D_0, M_0) = 1$. Then there exist infinitely many prime numbers $N$ by Dirichlet’s theorem.
Proof of Corollary 1.3. Let $D = \pm 1$, $N - M = 4D$, and $b = c = 0$, $d = 1$. Then by (4.1), (4.2) and (4.3), we obtain that the product is equal to $(M \cdot 4(\pm 1) \cdot N)^2 = 2^4 D^2 M^2 N^2$. □

Remark 4.1. By the next work it will be investigated on monogenity for a complete classification of the real biquadratic fields $\mathbb{Q}(\sqrt{DM}, \sqrt{DN})$ such that

(i) $D \equiv M \equiv N \equiv 1$ or 3 (mod 4)

(ii) $DM \equiv DN \equiv 2$ (mod 4) and $MN \equiv 3$ (mod 4)

and

(iii) $DM \equiv DN \equiv 2$ (mod 4) and $MN \equiv 1$ (mod 4).

5. ACKNOWLEDGEMENTS

The authors deeply thank the referee for his/her remarks to improve this paper and Prof. M. Showkat Raheem Chowdhury [UMT, Lahore] for his kind notices.

REFERENCES


