数理解析研究所講究録
517巻 1984年 91-100

On the indices and integral bases of abelian biquadratic fields

By

Toru Nakahara

1. Introduction. Let K be an algebraic number field over the rationals Q with finite degree. Z and $\mathcal{O}_K$ denote the ring of rational integers and the integer ring of K respectively. If $\mathcal{O}_K = Z[\alpha]$ for some number α in K, it is called that $\mathcal{O}_K$ has a power basis. For a number ξ in $\mathcal{O}_K$ we denote by $\mathrm{Ind}\,\xi$ the group index $(\mathcal{O}_K : Z[\xi])$ if ξ is a primitive element of K and 0 otherwise. Then the index $m(K)$ of any field K is defined by g.c.d. $\{\mathrm{Ind}\,\xi\ ;\ \xi \in \mathcal{O}_K\}$. The minimum index $\tilde{m}(K)$ of any K is defined by $\min\{\mathrm{Ind}\,\eta\ ;\ \eta \in \mathcal{O}_K,\ Q(\eta) = K\}$. In §2 we shall give an estimate of the index $m(K)$ without using the decomposition theory of primes when K is any abelian biquadratic field. In §3 we shall investigate some relations between $m(K)$ and an integral basis related to a problem of Hasse and construct such a field K that the minimum index $\tilde{m}(K)$ is greater than any given integer N applying a method of M. Hall[2].

2. An estimate of the indices. By [8] it is well known that if a prime p divides the index $m(K)$, then p is smaller than the degree $[K : Q]$.

In our situation we obtain more precisely the next lemma.

Lemma 1. For any abelian biquadratic field K over Q it holds that if the number $2^e 3^{e'}$ exactly divides the index $m(K)$, then $e \leqq 2$ and $e' \leqq 1$. Especially if the discriminant $d(K)$ of a field K is even, then $e = 0$.

Proof. i) The cyclic cases. Let χ be a biquadratic character with odd conductor n determined by the biquadratic residue symbol. k_n denotes the n-th cyclotomic field $Q(\zeta_n)$, herein $\zeta_n = \exp(2\pi i/n)$. Let G be the Galois group of k_n/Q. The group $<\chi>$ is a cyclic subgroup with order 4 of the character group of G. Let K denote the subfield of k_n corresponding to the kernel H of χ. Then we have $K = Q(\eta)$ with the Gauss period $\eta = \sum_{x \in H} \zeta_n^x$. We fix an element σ in G such that $\chi(\sigma) = i$, and denote $\sigma(\xi)$, $\sigma^2(\xi)$, $\sigma^3(\xi)$ by ξ', ξ'', ξ''' respectively for ξ in K.

First we consider the case of odd conductor n. Since the set $\{1, \eta, \eta', \eta''\}$ makes an integral basis of K, it is enough for computation of the $\operatorname{Ind}\xi$ to choose $\xi = x\eta + y\eta' + z\eta''$ for ξ in K. Let $n = \ell m$ be square-free for odd integers $\ell = a^2 + 4b^2$, m where any prime factor of ℓ is congruent to 1 modulo 4 and $\lambda = a + 2bi \equiv 1 \bmod 2(1 - i)$. Then by using the Gauss sum $\tau(\chi) = \sum_{x \in G} \chi(x)\zeta_n^x$ attached to χ and the Jacobi sum $\tau(\chi)^2/\tau(\chi^2)$ we obtain $\operatorname{Ind}\xi = \sqrt{|d(\xi)/d(K)|} = |cN\alpha_n|$, where $\alpha_n = (cm + d\sqrt{\ell})/2$, $c = ((x - z)^2 - y^2)b - (x - z)ya$, $d = ((x - y + z)^2 - \chi(-1) \times ((x - z)^2 + y^2)m)/2$. Herein $d(\xi)$, N mean the discriminant of a number ξ, the norm with respect to $Q(\sqrt{\ell})/Q$ respectively.

i)$_1$ If $\ell \equiv 1 \bmod 8$ and $b \equiv 0, 4 \bmod 8$ (resp. $b \equiv \pm 2 \bmod 8$), then for $\xi = 2\eta + \eta' - \eta''$ (resp. $2\eta \pm \eta'$ from $\chi(-1) = \begin{cases} 1, \\ -1, \end{cases}$ $\left.\begin{matrix} m \equiv 1 \bmod 4 \\ m \equiv -1 \bmod 4 \end{matrix}\right\}$) we have $\operatorname{Ind}\xi \equiv 4 \bmod 8$. i)$_2$ If $\ell \equiv 5 \bmod 8$, then for $\xi = \eta + \eta' - \eta''$ we get $\mathrm{Ind}\,\xi \equiv 1 \bmod 2$. i)$_3$ If $m \equiv 0 \bmod 3$ and $a \equiv 0 \bmod 3$ (resp. $a \not\equiv 0 \bmod 3$), then we choose $\xi = \eta$ (resp. $\eta + \eta'$). Thus we have $\mathrm{Ind}\,\xi \not\equiv 0 \bmod 3$. i)$_4$ If $m \not\equiv 0 \bmod 3$ and $a \equiv 0 \bmod 3$, then $b \not\equiv 0 \bmod 3$ and for $\xi = \eta$ $4N\alpha_n \equiv b^2|1 - 2\chi(-1)m| \bmod 9$ holds. When $1-2\chi(-1)m \equiv 0 \bmod 9$, we reset $\xi = 2\eta + 3\eta'$. Then $4N\alpha_n \equiv b^2|1 - 8\chi(-1)m| \not\equiv 0 \bmod 9$. i)$_5$ The case of $m \not\equiv 0$ and $a \not\equiv 0 \bmod 3$. For $\xi = \eta$ if $4^2N\alpha_n \equiv |4b^2m^2 - (1-\chi(-1)m)^2\ell| \equiv 0 \bmod 9$ holds, then we reset $\xi = 2\eta + \eta''$. If $4^2N\alpha_n \equiv |4b^2m^2 - (-\chi(-1)m)^2\ell| \equiv 0 \bmod 9$, then we have $1 - 2\chi(-1)m \equiv 0 \bmod 9$ from $(\ell, 3) = 1$. Then we take again $\xi = 3\eta + 2\eta''$. If $4^2N\alpha_n \equiv |4b^2m^2 - (7-\chi(-1)m)^2\ell| \equiv 0 \bmod 9$, then $1 + \chi(-1)m \equiv 0 \bmod 9$ must hold. This is a contradiction. By i)$_{1\sim5}$ we have $e \leqq 2$ and $e' \leqq 1$.

Next we estimate the case of even conductor. At first we consider the case of $\chi = \chi_0^{(\nu)}\chi_\ell\psi_m$, $n = 16\ell m$, $\ell m \equiv 1 \bmod 2$, where $\chi_0^{(\nu)}(x) = (-1)^{\nu(x-1)/2}\, i^{(x^2-1)/8}$ are the even and the odd biquadratic characters with conductor 16 for $\nu = 0$ and 1 respectively, and χ_ℓ, ψ_m are the biquadratic, the quadratic characters with conductors ℓ, m respectively. From $\chi((n/2)+1) = -1$, it follows that $\eta'' = \sigma^2(\eta) = \sum_{x\in H} \zeta_n^{((n/2)+1)x} = -\sum_{x\in H}\zeta_n^x = -\eta$. However it is known that $\{1, \eta, \eta', \sqrt{f}/2\}$ is an integral basis of K, where $d(K) = fn^2$ and $f = 8\ell$ is the conductor of $Q(\sqrt{8\ell})$ [3]. Then for $\xi = x\eta + y\eta' + z(\sqrt{f}/2)$ we obtain $\mathrm{Ind}\,\xi = |cN\alpha_f|$, where $\alpha_f = cm + d(\sqrt{f}/2)$, $c = -2xy(a-b) + (x^2 - y^2) \times (a + 2b)$, $d = 2z^2 - \chi(-1)(x^2 + y^2)m$. For $\xi_1 = \eta$, we have $\mathrm{Ind}\,\xi_1 = |a + 2b|m^2|(a+2b)^2 - 2\ell| \equiv 1 \bmod 2$. If $a + 2b \equiv \pm 3 \bmod 9$

and $m \not\equiv 0 \bmod 3$, then $\mathrm{Ind}\,\xi_1 \equiv \pm 3 \bmod 9$. If $a + 2b \equiv \pm 3 \bmod 9$ (resp. $\not\equiv 0 \bmod 3$) and $m \equiv 0 \bmod 3$, then for $\xi_2 = \eta + (\sqrt{f}/2)$ we get $\mathrm{Ind}\,\xi_2 = |a + 2b||(a + 2b)^2 m^2 - 8\ell| \equiv \pm 3 \bmod 9$ (resp. $\not\equiv 0 \bmod 3$). If $a + 2b \equiv 0 \bmod 9$ and $m \equiv 0 \bmod 3$, then $a - 2b \not\equiv 0 \bmod 3$ holds. Thus for $\xi_3 = \eta + \eta' + (\sqrt{f}/2)$ we have $\mathrm{Ind}\,\xi_3 \equiv 2|a - 2b|\ell \not\equiv 0 \bmod 3$. In the case of $(a + 2b)m \not\equiv 0 \bmod 3$, we have $\mathrm{Ind}\,\xi_1 \not\equiv 0 \bmod 3$ for $a \not\equiv - b \bmod 3$, and put $\xi_4 = \eta + \eta'$, then $\mathrm{Ind}\,\xi_4 \equiv \pm 3 \bmod 9$ for $a \equiv - b \bmod 3$. If $a + 2b \equiv 0 \bmod 9$ and $m \not\equiv 0 \bmod 3$, then we have $\mathrm{Ind}\,\xi_4 \not\equiv 0 \bmod 9$. Therefore we obtain $e = 0$ and $e' \leqq 1$. Secondly we treat the case of $\chi = \chi_\ell \psi_m$, $n = \ell m$, $m \equiv 0 \bmod 2$. In this case the set $\{1, \eta, \eta', \eta''\}$ is also not an integral basis of K. But $\{1, \eta, \eta', (1 + \sqrt{\ell})/2\}$ is an integral basis, where $d(K) = \ell n^2$, $f = \ell[3]$. Then for $\xi = x\eta + y\eta' + z(1 + \sqrt{\ell})/2$ we have $\mathrm{Ind}\,\xi = |cN\alpha_f|$, where $\alpha_f = cm + d\sqrt{f}$, $c = - xya + (x^2 - y^2)2b$, $d = (x^2 + y^2)(m/2) - \chi(-1)z^2$. For $\xi_1 = \eta + \eta' + (1 + \sqrt{\ell})/2$ we get $\mathrm{Ind}\,\xi_1 \equiv 1 \bmod 2$. Put $\xi_2 = \eta + \eta'$. If $abm \not\equiv 0 \bmod 3$, then $\mathrm{Ind}\,\xi_2 \not\equiv 0 \bmod 3$. We choose $\xi_3 = \eta$, $\xi_4 = \eta + (1 + \sqrt{\ell})/2$. If $a \equiv 0 \bmod 3$, then from $b \not\equiv 0 \bmod 3$ we have $\mathrm{Ind}\,\xi_3 \equiv \pm 3 \bmod 9$ for $m \not\equiv 0 \bmod 3$ and $\mathrm{Ind}\,\xi_4 \not\equiv 0 \bmod 3$ for $m \equiv 0 \bmod 3$. If $b \equiv 0 \bmod 3$, then from $a \not\equiv 0 \bmod 3$ we obtain $\mathrm{Ind}\,\xi_1 \not\equiv 0 \bmod 3$ for $m \not\equiv 0 \bmod 3$ and $\mathrm{Ind}\,\xi_1 \equiv \pm 3 \bmod 9$ for $m \equiv 0 \bmod 3$. Thus we have $e = 0$ and $e' \leqq 1$.

ii) The non-cyclic cases. Without loss of generality we can set $K = Q(\sqrt{\ell m_1}, \sqrt{\ell m_2})$, where $\ell m_1 m_2$ is a square-free integer and $\ell > 0$. For brevity we denote $(1 + \sqrt{\ell m_1})/2$, $(1 + \sqrt{\ell m_2})/2$ $(\sqrt{\ell m_2} + \sqrt{m_1 m_2})/2$ by α, β, γ respectively. ii)$_1$ If $\ell m_1 \equiv 1$, $\ell m_2 \equiv 2, 3 \bmod 4$, then $\{1, \alpha, 2\beta - 1, \gamma\}$ is an integral basis of K and the field discriminant $d(K) = 16\ell^2 m_1^2 m_2^2$ holds. For $\xi_1 = \alpha - (2\beta - 1) + 2\gamma$ we can compute $\mathrm{Ind}\,\xi_1 \equiv \ell m_1^2 \equiv 1 \bmod 2$. If $(\ell - m_2)m_1 \not\equiv 0 \bmod 3$, then $\mathrm{Ind}\,\xi_1 \not\equiv 0 \bmod 3$ follows. If $m_1 \equiv 0 \bmod 3$, then for $\xi_2 = \alpha + (2\beta - 1)$ we have $\mathrm{Ind}\,\xi_2 \equiv \ell^2 m_2 \not\equiv 0 \bmod 3$. If $\ell - m_2 \equiv 0 \bmod 3$, then $\ell m_2 \not\equiv 0 \bmod 3$. We can restrict $m_1 \not\equiv 0 \bmod 3$. In the case of $\ell - m_2 \equiv 0 \bmod 9$, we have $\ell - 4m_2 \not\equiv 0 \bmod 9$. Then $\mathrm{Ind}\,\xi_1 \not\equiv 0 \bmod 9$. In the case of $\ell - m_2 \equiv \pm 3 \bmod 9$, for $\xi_3 = \alpha + (2\beta - 1) + \gamma$ we get $\mathrm{Ind}\,\xi_3 \equiv |(\ell - m_2)m_1^2| \equiv \pm 3 \bmod 9$. Thus we obtain $e = 0$ and $e' \leqq 1$. ii)$_2$ if $\ell m_1 \equiv 3$, $\ell m_2 \equiv 2 \bmod 4$, then $\{1, 2\alpha - 1, 2\beta - 1, \gamma\}$ is an integral basis and $d(K) = 64\ell^2 m_1^2 m_2^2$. By $\ell \equiv 1 \bmod 2$, $\ell - m_1 \equiv 2 \bmod 4$ for $\xi_1 = \gamma$ we have $\mathrm{Ind}\,\xi_1 \equiv 1 \bmod 2$. Next if $(\ell - m_1)m_2 \not\equiv 0 \bmod 3$, then $\mathrm{Ind}\,\xi_1 \not\equiv 0 \bmod 3$ holds. If $m_2 \equiv 0 \bmod 3$, then for $\xi_2 = (2\alpha - 1) + (2\beta - 1)$ we have $\mathrm{Ind}\,\xi_2 = |(4\ell)^2(4m_2 - m_1)| \not\equiv 0 \bmod 3$. If $\ell - m_1 \equiv 0 \bmod 9$, then $\ell m_1 \not\equiv 0 \bmod 3$. We can restrict $m_2 \not\equiv 0 \bmod 3$. For $\xi_3 = 2(2\beta - 1) + \gamma$ $\mathrm{Ind}\,\xi_3 \equiv |(-m_2)(25\ell - m_1)(25m_2)| \equiv \pm 3 \bmod 9$ holds. If $\ell - m_1 \equiv \pm 3 \bmod 9$, then $\mathrm{Ind}\,\xi_1 \equiv \pm 3 \bmod 9$. Therefore we have $e = 0$ and $e' \leqq 1$. ii)$_3$ If $\ell m_1 \equiv \ell m_2 \equiv 1 \bmod 4$, then $\{1, \alpha, \beta, \alpha\beta \pm ((\ell - 1)/4)(2\gamma - 2\beta + 1)\}$ for $\ell \equiv m_1 \equiv m_2 \equiv 1 \bmod 4$ and $\{1, \alpha, \beta, \alpha\beta + (1/2) \mp ((\ell - 1)/4)(2\gamma - 2\beta + 1)\}$ for $\ell \equiv m_1 \equiv m_2 \equiv 3 \bmod 4$ are integral bases, where the sign is positive if and only if $m_1 < 0$ and $m_2 < 0$. For any integer ξ in K we have $\mathrm{Ind}\,\xi \equiv 0 \bmod 2$. Moreover in the case of $m_1 - m_2 \equiv 4 \bmod 8$ (resp. $\equiv 0 \bmod 8$), for $\xi_1 = \alpha + \beta$ (resp. $2\alpha + \beta$) we get $\mathrm{Ind}\,\xi_1 \equiv 4 \bmod 8$. If $\ell(m_1 - m_2) \not\equiv 0 \bmod 3$, then $\mathrm{Ind}\,\xi_1 \not\equiv 0 \bmod 3$. We denote by δ the fourth numbers of the integral bases. If $\ell \equiv 0$ and $m_1 - m_2 \not\equiv 0 \bmod 3$, then for $\xi_2 = \alpha + \beta + 2\delta$

we have $\mathrm{Ind}\,\xi_2 \equiv |m_1 m_2(m_1 - m_2)| \not\equiv 0 \bmod 3$. If $\ell \not\equiv 0$ and $m_1 - m_2 \equiv 0 \bmod 9$, then $m_1 m_2 \not\equiv 0 \bmod 3$ holds. If for $\xi_3 = 2\alpha + \beta$ $\mathrm{Ind}\,\xi_3 = |4\ell^2(m_2 - 4m_1)| \equiv 0 \bmod 9$, then we have $3m_1 \equiv 0 \bmod 9$. This is a contradiction. If $\ell \not\equiv 0 \bmod 3$ and $m_1 - m_2 \equiv \pm 3 \bmod 9$, then $\mathrm{Ind}\,\xi_1 \equiv \pm 3 \bmod 9$. Next if $\ell \equiv 0 \bmod 3$ and $m_1 - m_2 \equiv \pm 3 \bmod 9$, then $\mathrm{Ind}\,\xi_2 \equiv \pm 3 \bmod 9$. Finally if $\ell \equiv 0 \bmod 3$ and $m_1 - m_2 \equiv 0 \bmod 9$, then for $\xi_4 = \beta + 2\delta$ we have $\mathrm{Ind}\,\xi_4 \equiv \pm 3 \bmod 9$. The estimates of ii)$_{1\sim 3}$ imply $1 \leqq e \leqq 2$ and $e' \leqq 1$. Therefore we have proved Lemma 1.

3. Results. Works related to the problem of Hasse are found in [1], [4], [5] and the references mentioned in [7]. From [6] and [7] we have

Theorem 1. There exist infinitely many non-cyclic but abelian (resp. exist cyclic) biquadratic fields over Q whose integer rings have a power basis.

In our case by Lemma 1 the index $m(K)$ is not larger than 12. In fact it follows

Theorem 2. There exist infinitely many such abelian biquadratic fields K over Q that the index is equal to 12 (resp. 6) and that neither $\{1, \alpha, \alpha^2, \beta\}$ nor $\{1, \alpha, \beta, \alpha^3\}$ (resp. $\{1, \alpha, \beta, \alpha^3\}$) for any α, β in K forms (resp. does not form) an integral basis of K.

The method of a proof of this theorem is the same as in [6].

i) The cyclic case. Let n be the conductor of the field K.

We choose $n = a^2 + 72^2$, $a \equiv 5 \bmod 12$ (resp. $n = a^2 + 12^2$, $a \equiv 1 \bmod 12$). Since the set $\{1, \eta, \eta', \eta''\}$ with the Gauss period η makes an integral basis of K, we may put $\xi = x\eta + y\eta' + z\eta''$ for any integer ξ in K. Then we obtain $\mathrm{Ind}\,\xi = |cN\alpha_n|$ where α_n is the same number of $Q(\sqrt{n})$ as in the previous section. By virtue of $\lambda = a + 72i$ and

$$N\alpha_n \equiv \left\{\begin{array}{l}(x-z)^2y^2 - (xy+yz+zx)^2 \bmod 3 \\ 2(x+y+z)(x+z)y - (x-y)(z-y)xz \bmod 4\end{array}\right\} \quad \text{(resp.}$$

$$\lambda = a + 12i \quad \text{and} \quad N\alpha_n \equiv \left\{\begin{array}{l}(x-z)^2y^2 - (xy+yz+zx)^2 \bmod 3 \\ 0 \bmod 2\end{array}\right\} \text{)}$$

we have $\mathrm{Ind}\,\xi \equiv 0 \bmod 12$ (resp. $\mathrm{Ind}\,\xi \equiv 0 \bmod 6$ and $\mathrm{Ind}\,\eta \equiv 2 \bmod 4$). Then by Lemma 1 we get $m(K) = 12$ (resp. $m(K) = 6$). Moreover by $\chi(2) = 1$ (resp. $\left\{\begin{array}{l}\chi(2) = -1 \\ \chi(3) = 1\end{array}\right\}$) we can see

$$\sigma^j(\eta)^2 \equiv \sigma^j(\eta) \bmod 2 \quad \text{(resp.} \left\{\begin{array}{l}\sigma^j(\eta)^2 \equiv \sigma^{j+2}(\eta) \bmod 2 \\ \sigma^j(\eta)^3 \equiv \sigma^j(\eta) \bmod 3\end{array}\right\}\text{).}$$

Since $\mathrm{Ind}\,\xi$ is equal to the absolute value of the determinant of the transformation matrix for $\{1, \xi, \xi^2, \xi^3\}$ with respect to an integral basis $\{1, \eta, \eta', \eta''\}$, we can see that any three rows in the matrix are linearly dependent modulo 2 (resp. the second and the fourth rows are so modulo 3). Then none of $\{1, \alpha, \alpha^2, \beta\}$ nor $\{1, \alpha, \beta, \alpha^3\}$ (resp. $\{1, \alpha, \beta, \alpha^3\}$) for all integers α, β can make (resp. can not make) a Z-basis of $\mathcal{O}_K$. Finally our parametrization satisfies the next lemma.

Lemma 2[6]. For $a > 0$, $b, c \in Z$, $a \equiv b$, $c \equiv 1 \bmod 2$, set

$$n(t) = at^2 + bt + c.$$

Let the congruences $n(t) \equiv 0 \bmod q^2$ have at most two solutions for every prime q within $1 \leqq t \leqq q^2$. Then the number $n(t)$ is square-free for infinitely many $t \in Z$.

ii) The non-cyclic case. For a field $K = Q(\sqrt{\ell m_1}, \sqrt{\ell m_2})$ assume $\ell m_1 \equiv \ell m_2 \equiv 1 \bmod 24$. Then using Lemma 1 we have $m(K) = 12$. Next we choose $\ell m_1 \equiv \ell m_2 \equiv 1 \bmod 3$, $\ell \equiv 5 \bmod 8$ and $m_1 \equiv m_2 \equiv 1 \bmod 16$. Then we can see $\mathrm{Ind}\,\xi \equiv 0 \bmod 6$ for any integer ξ in K. Also for $\xi_0 = ((1 + \sqrt{\ell m_1})/2) + ((1 + \sqrt{\ell m_1}) \times (1 + \sqrt{\ell m_2})/4) + ((\ell - 1)/4)\sqrt{m_1 m_2}$ it follows $\mathrm{Ind}\,\xi_0 \equiv 2 \bmod 4$. Thus we obtain $m(K) = 6$. Under this parametrization we can perform the same argument as in the case i). Therefore we obtain Theorem 2.

Remark 1. Among the fields K with even conductor there does not exist any K which satisfies the properties in Theorem 2.

Theorem 3. There exist infinitely many non-cyclic but abelian biquadratic fields K which have the index 1 and still whose minimum indices are greater than N for any given integer N. Consequently the integer rings $\mathcal{O}_K$ have not a power basis.

Proof. We consider the field $K_\ell = Q(\sqrt{\ell m_1}, \sqrt{\ell m_2})$ with $\ell m_1 \equiv 1$, $\ell m_2 \equiv -1 \bmod 12$. Then from Lemma 1 the index $m(K_\ell)$ is odd. Under the same notations as in the proof ii)$_1$ of Lemma 1 for a number $\xi = x\alpha + y\beta + z\gamma$ we obtain

$\mathrm{Ind}\,\xi = |(x^2\ell - z^2 m_2)(z^2 m_1 - (2y + z)^2 \ell)(x^2 m_1 - (2y + z)^2 m_2)|/4.$

Thus it holds that $\mathrm{Ind}(\alpha + \beta) \not\equiv 0 \bmod 3$. Then $m(K_\ell) = 1$ holds. In an imaginary case we select $0 > m_1 \equiv 1$, $0 < -m_2 \equiv 1$, $0 < \ell \equiv 1 \bmod 12$. Then $\mathrm{Ind}\,\xi > \ell$ holds for any primitive element ξ in $\mathcal{O}_{K_\ell}$.

In a real case set $0 < \ell \equiv -1 \bmod 12$. We estimate the factor $I = x^2 m_1 - (2y+z)^2 m_2$ of $\mathrm{Ind}\,\xi$. For any integer $N > 0$ we can find the following primes $p_i \equiv -1$, $q_i \equiv 1 \bmod 12$ and $p_i \neq \ell$ for $1 \leqq i \leqq N$. Put $m_1 = p_1$ and $m_2 = q_1$ such that

$$\left(\frac{x^2 p_1}{q_1}\right) = \left(\frac{p_1}{q_1}\right) \neq \left(\frac{1}{q_1}\right),$$ where $\left(\frac{*}{p}\right)$ denotes the Legendre symbol.

Then $I \neq \pm 1$. Next for a prime $q_2 > q_1$, there exists an integer a_2 with $\left(\frac{a_2}{q_2}\right) \neq \left(\frac{2}{q_2}\right)$. We select p_2 such that $p_2 \equiv \begin{Bmatrix} p_1 \bmod q_1 \\ a_2 \bmod q_2 \end{Bmatrix}$.

Reset $m_1 = p_2$, $m_2 = q_1 q_2$, then $I = \pm 1, \pm 2$. Successively we can choose primes p_N, q_N such that $p_N \equiv \begin{Bmatrix} p_{N-1} & \bmod q_1 \cdots q_{N-1} \\ a_N & \bmod q_N \end{Bmatrix}$

with $q_N > q_{N-1}$ and $\left(\frac{a_N}{q_N}\right) \neq \left(\frac{N}{q_N}\right)$. For $m_1 = p_N$, $m_2 = q_1 \cdots q_N$ define the biquadratic field $K_N = Q(\sqrt{\ell m_1}, \sqrt{\ell m_2})$, then it holds that $\mathfrak{m}(K_N) > N$. Therefore we have proved Theorem 3.

References

[1] K. Győry, On discriminants and indices of integers of an algebraic number field, J. Reine Angew. Math. 324(1981), 114 - 126.

[2] M. Hall, Indices in cubic fields, Bull. Amer. Math. Soc. 43 (1937), 104 - 108.

[3] H. Hasse, Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen und biquadratischen Zahlkörpern, Abh. Deutsch. Akad. Wiss. Berlin, Math. -Nat. Kl. 2(1950), 3 - 95 (= Math. Abhandlungen Bd. 3, 289 - 379, Berlin - New York, 1975).

[4] I. Kátai; B. Kovács, Kanonische Zahlsysteme in der Theorie der quadratischen algebraischen Zahlen, Acta Sci. Math. (Szeged), 42(1980),99 - 107.

[5] B. Kovács, Canonical number systems in algebraic number fields, Acta Math. Acad. Sci. Hungar. 37(1981), 159 - 164.

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

[7] T. Nakahara, On a problem of Hasse, RIMS Kōkyūroku, 456(1982), 152 - 157.

[8] E. von Żyliński, Zur Theorie der ausserwesentlichen Diskriminantenteiler algebraischer Körper, Math. Ann. 73(1913), 273 - 274.

Department of Mathematics
Faculty of Science and Engineering
Saga University
Saga 840, Japan