International Journal of Pure and Applied Mathematics
Volume 31 No. 4 2006, 481-490

MONOGENEITY IN BIQUADRATIC FIELDS

Mu-Ling Chang

Department of Mathematics
University of Wisconsin-Platteville
Platteville, WI 53818, USA
e-mail: changm@uwplatt.edu

Abstract: We establish necessary and sufficient conditions for the rings of algebraic integers of imaginary biquadratic fields to have power integral bases, and find all generators of power integral bases of such rings. We also find a sufficient condition for the monogeneity of real biquadratic fields.

G. Nyul proved the same theorem in [5], but in my paper I offered a different method which is easier to get the result.

AMS Subject Classification: 11R04
Key Words: power integral bases, monogeneity, biquadratic fields

1. Introduction

Let M and F be algebraic number fields with $M \supseteq F$, and let $\mathcal{O}_M$ and $\mathcal{O}_F$ be the rings of algebraic integers in M and F, respectively. The ring $\mathcal{O}_M$ is called $\mathcal{O}_F$-monogenic if $\mathcal{O}_M = \mathcal{O}_F[\beta]$ for some $\beta \in \mathcal{O}_M$, i.e. there exists a power integral basis of $\mathcal{O}_M$ over $\mathcal{O}_F$. We say that $\mathcal{O}_M$ is monogenic if it is $\mathbb{Z}$-monogenic. For example, the rings of algebraic integers of both quadratic and cyclotomic fields are monogenic. Many people have studied the monogeneity of biquadratic fields and recent work can be found in [4]. Here we are interested in imaginary biquadratic fields, and find the necessary and sufficient conditions for the monogeneity of these fields by using the procedure given in [1]. This method also gives us all generators of power integral bases of a monogenic ring, and it works very well when we deal with a number field of small degree and

Received: August 1, 2006

its subfields are well known. Later we obtain a sufficient condition for the monogeneity of real biquadratic fields by the calculation used on imaginary biquadratic fields.

We consider the imaginary biquadratic fields $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ where m and n are distinct squarefree integers. Let $l = (m, n) > 0$, $m = lm_1$, and $n = ln_1$. Without loss of generality we may assume that $(m, n) \equiv (1, 1), (2, 1), (2, 3), (3, 3)$ modulo 4 (see [6]). We can also assume that $m < 0$ because $\mathbb{Q}(\sqrt{m})$, $\mathbb{Q}(\sqrt{n})$, and $\mathbb{Q}(\sqrt{m_1 n_1})$ are the only three quadratic subfields of $\mathbb{Q}(\sqrt{m}, \sqrt{n})$, and $\mathbb{Q}(\sqrt{m}, \sqrt{n}) = \mathbb{Q}(\sqrt{m_1 n_1}, \sqrt{n}) = \mathbb{Q}(\sqrt{n}, \sqrt{m})$. It has been proved that the ring of algebraic integers of $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ is not monogenic when $(m, n) \equiv (1, 1)$ modulo 4 (see [2]), so we focus on the other three cases and the main result is summarized as follows.

Theorem 1.1. *Let m and n be distinct squarefree integers, $m < 0$ and $l = (m, n) > 0$. The ring of algebraic integers of the imaginary biquadratic field $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ is monogenic if and only if*

$$\begin{cases} l = 1 \text{ and } \ n = 4m + 1 & \text{if } (m, n) \equiv (2, 1) \bmod 4, \\ m = -2l \text{ and } n \pm m = l^2 & \text{if } (m, n) \equiv (2, 3) \bmod 4, \\ l = 1 \text{ with } \ n - m = \pm 4, \text{ or} & \\ m = -l \text{ with } \ n - m = 4l^2 & \text{if } (m, n) \equiv (3, 3) \bmod 4. \end{cases}$$

Moreover, all $\mathbb{Z}$-monogenic generators of the ring of algebraic integers of $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ are

$$\begin{cases} a + \frac{1}{2} + \mu\sqrt{m} + \frac{\nu\sqrt{n}}{2} & \text{if } (m, n) \equiv (2, 1) \bmod 4, \\ a + \frac{\mu\sqrt{m}}{2} + \frac{\nu\sqrt{mn}}{2l} & \text{if } (m, n) \equiv (2, 3) \bmod 4, \\ a + \frac{\mu\sqrt{m}}{2} + \frac{\nu\sqrt{n}}{2} & \text{if } (m, n) \equiv (3, 3) \bmod 4 \text{ and } l = 1, \\ a + \frac{1}{2} + \mu\sqrt{m} + \frac{\nu\sqrt{mn}}{2l} & \text{if } (m, n) \equiv (3, 3) \bmod 4 \text{ and } m = -l, \end{cases}$$

where $a \in \mathbb{Z}$ and μ, $\nu \in \{\pm 1\}$. Note that when $m = -1$ and $n \equiv 3 \bmod 4$, both $a + \frac{\mu\sqrt{m}}{2} + \frac{\nu\sqrt{n}}{2}$ and $a + \frac{1}{2} + \mu\sqrt{m} + \frac{\nu\sqrt{mn}}{2l}$ are $\mathbb{Z}$-monogenic generators of the ring of algebraic integers of $\mathbb{Q}(i, \sqrt{n})$

Let $L = \mathbb{Q}(\sqrt{m}, \sqrt{n})$, and $K = \mathbb{Q}(\sqrt{m})$. If $\mathcal{O}_L$ is monogenic, say $\mathcal{O}_L = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_L$, then $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. In other words, the set of the $\mathbb{Z}$-monogenic generators in $\mathcal{O}_L$ is just a subset of the $\mathcal{O}_K$-monogenic generators in $\mathcal{O}_L$. Therefore, we start with finding all $\mathcal{O}_K$-monogenic generators of $\mathcal{O}_L$.

2. Finding All $\mathcal{O}_K$-Monogenic Generators of $\mathcal{O}_L$

Let $\alpha \in \mathcal{O}_L$ be an $\mathcal{O}_K$-monogenic generator of $\mathcal{O}_L$, and $I = [\mathcal{O}_L : \mathcal{O}_K[\sqrt{n}\,]]$ be the index. Since $I\alpha \in \mathcal{O}_K[\sqrt{n}\,]$, the form of the $\mathcal{O}_K$-monogenic generators is determined, that is

$$\alpha = \frac{x + y\sqrt{n}}{I}$$

for some $x, y \in \mathcal{O}_K$. We find the exact values of I, y, and x, respectively.

Lemma 2.1.

$$I = \begin{cases} 4l & \text{if } (m,n) \equiv (2,1) \text{ or } (3,3) \bmod 4, \\ 2l & \text{if } (m,n) \equiv (2,3) \bmod 4. \end{cases}$$

Proof. Let $\mathrm{Disc}(A)$ be the discriminant of a free $\mathbb{Z}$-module A. Use the equality

$$\mathrm{Disc}(\mathcal{O}_K[\sqrt{n}\,]) = I^2 \cdot \mathrm{D}_{L/\mathbb{Q}}\,,$$

where $\mathrm{Disc}(\mathcal{O}_K[\sqrt{n}\,]) = \mathrm{Disc}_{L/\mathbb{Q}}(1, \sqrt{n}, \sqrt{m}, \sqrt{mn}\,) = 2^8 m^2 n^2$ and the discriminant of the field L (see [6]) is

$$\mathrm{D}_{L/\mathbb{Q}} = \begin{cases} 16 l^2 {m_1}^2 {n_1}^2 & \text{if } (m,n) \equiv (2,1) \text{ or } (3,3) \bmod 4, \\ 64 l^2 {m_1}^2 {n_1}^2 & \text{if } (m,n) \equiv (2,3) \bmod 4. \end{cases} \tag{1}$$

□

In order to calculate y, we use the transitivity of the discriminants, i.e. $\mathrm{D}_{L/\mathbb{Q}} = {\mathrm{D}_{K/\mathbb{Q}}}^2 \cdot \mathrm{N}_{K/\mathbb{Q}}(\mathrm{D}_{L/K})$, to get the discriminant of L over K, which is

$$\mathrm{D}_{L/K} = \begin{cases} (n_1) & \text{if } (m,n) \equiv (2,1) \text{ or } (3,3) \bmod 4, \\ (2n_1) & \text{if } (m,n) \equiv (2,3) \bmod 4. \end{cases}$$

Since $\mathrm{D}_{L/K} = \mathrm{D}_{L/K}(\alpha)$ by assumption and

$$\mathrm{D}_{L/K}(\alpha) = (\mathrm{Disc}_{L/K}(1,\alpha)) = \left(\frac{y}{I}\right)^2 (\mathrm{Disc}_{L/K}(1,\sqrt{n}\,)) = \left(\frac{4ny^2}{I^2}\right),$$

we obtain

$$(y^2) = \begin{cases} (4l) & \text{if } (m,n) \equiv (2,1) \text{ or } (3,3) \bmod 4, \\ (2l) & \text{if } (m,n) \equiv (2,3) \bmod 4. \end{cases}$$

Corollary 2.2. *Let $\alpha = (x + y\sqrt{n})/I$ be defined as above. If α is an $\mathcal{O}_K$-monogenic generator of $\mathcal{O}_L$, then*

$$y = \begin{cases} \pm 2 \text{ with } l = 1 & \text{if } (m,n) \equiv (2,1) \bmod 4, \\ \pm\sqrt{m} \text{ with } m = -2l & \text{if } (m,n) \equiv (2,3) \bmod 4, \\ \pm 2 \text{ with } l = 1,\ \pm 2\sqrt{m} \text{ with } m = -l & \text{if } (m,n) \equiv (3,3) \bmod 4. \end{cases}$$

Proof. Let $y = s + t\sqrt{m} \neq 0$ for some $s, t \in \mathbb{Z}$. Assume that $(m,n) \equiv (3,3) \bmod 4$. By the last equality we get

$$s^2 + 2st\sqrt{m} + t^2 m = 4l\mu\,, \tag{2}$$

where $\mu \in \mathcal{O}_K{}^\times = \{\pm 1\}$, the group of the units in $\mathcal{O}_K$ if $m \neq -1$. Let $m \neq -1$, then $2st = 0$ and $s^2 + t^2 m = 4l\mu$. When $t = 0$, we have $s^2 = 4l\mu = 4l > 0$. Since l is squarefree, it follows that $s = \pm 2 = y$ and $l = 1$. When $s = 0$, we get

$$t^2 m = 4l\mu = -4l < 0, \tag{3}$$

i.e. $t^2 m_1 = -4$. Since m_1 is squarefree too, we obtain $t = \pm 2$ and $m_1 = -1$. Hence $y = \pm 2\sqrt{m}$ and $m = -l$.

When $m = -1$, we claim that μ must be ± 1 in (2). Note that in this case $\mathcal{O}_K{}^\times = \{\pm 1, \pm i\}$. Suppose $\mu = \pm i$, then (2) gives us $s^2 - t^2 = 0$ and $2st \pm 4 = 0$. A calculation shows that s and t are not integers, which is a contradiction. So $\mu = \pm 1$, and we have the same result for y by using the above calculation.

If $(m,n) \equiv (2,1) \bmod 4$, we can also use the above calculation to get the value of y, i.e. $y = \pm 2$ with $l = 1$, or $y = \pm 2\sqrt{m}$ with $m = -l$. But y can not be $\pm 2\sqrt{m}$ because $m = -l$ is not even.

When $(m,n) \equiv (2,3) \bmod 4$, we replace $4l$ by $2l$ in (2). Similar calculation shows that $t = \pm 1$ and $m_1 = -2$ when $s = 0$. So $y = \pm\sqrt{m}$ and $m = -2l$. When $t = 0$, we get a contradiction which is $l = 2$. This completes the proof. □

Now we find the possible values of x. To do so, we have to find some restrictions on x. Note that if $\mathcal{O}_L = \mathcal{O}_K[\,\beta\,]$ for some $\beta \in \mathcal{O}_L$, then $\mathcal{O}_L = \mathcal{O}_K[\,\beta + \gamma\,]$ for any $\gamma \in \mathcal{O}_K$. Hence we only need to find a representative of the equivalence class $[\,\beta\,]$ modulo $\mathcal{O}_K$. So we use x_0 instead of x to represent this concept in our $\mathcal{O}_K$-monogenic generator α, i.e. we let

$$\alpha = \frac{x_0 + y\sqrt{n}}{I}\,, \quad \text{where } x_0 = c + d\sqrt{m} \text{ with } c,\, d \in \{0, 1, 2, \ldots, I-1\}.$$

Corollary 2.3. *Let $\alpha = (x_0 + y\sqrt{n})/I$ be defined as above. If α is an $\mathcal{O}_K$-monogenic generator of $\mathcal{O}_L$, then*

$$x_0 = \begin{cases} 2 & \text{if } (m,n) \equiv (2,1) \bmod 4, \\ l\sqrt{m} & \text{if } (m,n) \equiv (2,3) \bmod 4, \\ 2\sqrt{m} \text{ when } y = \pm 2, & \\ 2l \text{ when } y = \pm 2\sqrt{m} & \text{if } (m,n) \equiv (3,3) \bmod 4. \end{cases}$$

Proof. Note that all coefficients of the minimal polynomial of $\alpha = (x_0 + y\sqrt{n})/I$ over K must be in $\mathcal{O}_K$, that is,

$$-2x_0/I \in \mathcal{O}_K, \tag{4}$$

$$({x_0}^2 - y^2 n)/I^2 \in \mathcal{O}_K. \tag{5}$$

By using these two conditions, Lemma 2.1 and Corollary 2.2, we are able to find the value of x_0.

Consider $(m,n) \equiv (3,3) \bmod 4$ with $y = \pm 2\sqrt{m}$ and $m = -l$. The other cases are similar. Let $x_0 = c + d\sqrt{m}$ where c, $d \in 0, 1, \dots, 4l-1$ by Lemma 2.1. From (4) x_0 is divisible by $2l$ in $\mathcal{O}_K$, so $x_0 = 0$, $2l$, $2l\sqrt{m}$, or $2l + 2l\sqrt{m}$. Then we use (5) to check these possibilities, i.e.

$$\frac{{x_0}^2 - y^2 n}{I^2} = \frac{{x_0}^2 - 4mn}{16l^2} = \frac{{x_0}^2 - 4l^2 m_1 n_1}{16l^2}$$

$$= \begin{cases} \frac{-m_1 n_1}{4} \notin \mathcal{O}_K & \text{if } x_0 = 0, \\ \frac{1 - m_1 n_1}{4} \in \mathcal{O}_K & \text{if } x_0 = 2l, \\ \frac{m - m_1 n_1}{4} \notin \mathcal{O}_K & \text{if } x_0 = 2l\sqrt{m}, \\ \frac{1 + m - m_1 n_1}{4} + \frac{\sqrt{m}}{2} \notin \mathcal{O}_K & \text{if } x_0 = 2l + 2l\sqrt{m}, \end{cases}$$

because $m_1 n_1 \equiv l^2 m_1 n_1 = mn \equiv 1 \bmod 4$. Therefore $x_0 = 2l$. □

Theorem 2.4. *Let m and n be distinct squarefree integers, $m < 0$, $l = (m,n) > 0$, and $K = \mathbb{Q}(\sqrt{m})$. The ring of algebraic integers of the imaginary biquadratic field $L = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ is $\mathcal{O}_K$-monogenic if and only if*

$$\begin{cases} l = 1 & \text{if } (m,n) \equiv (2,1) \bmod 4, \\ m = -2l & \text{if } (m,n) \equiv (2,3) \bmod 4, \\ l = 1, \text{or } m = -l & \text{if } (m,n) \equiv (3,3) \bmod 4. \end{cases}$$

Moreover, all $\mathcal{O}_K$-generators of $\mathcal{O}_L$ are of the form $a+b\sqrt{m}+\alpha$ where a, $b \in \mathbb{Z}$, and $\alpha =$

$$\begin{cases} \frac{1\pm\sqrt{n}}{2} & \text{if } (m,n) \equiv (2,1) \bmod 4, \\ \frac{l\sqrt{m}\pm\sqrt{mn}}{2l} & \text{if } (m,n) \equiv (2,3) \bmod 4, \\ \frac{\sqrt{m}\pm\sqrt{n}}{2} \text{ when } l=1, \text{ and} & \\ \frac{l\pm\sqrt{mn}}{2l} \text{ when } m=-l & \text{if } (m,n) \equiv (3,3) \bmod 4. \end{cases}$$

Proof. Combining Lemma 2.1, Corollary 2.2 and 2.3, we get the values of $\alpha = (x_0 + y\sqrt{n})/I$. To make sure that these α are $\mathcal{O}_K$-monogenic generators of $\mathcal{O}_L$, we need to check if they are in $\mathcal{O}_L$. The fast way is to show that they are integral over $\mathcal{O}_K$. Assume that $(m,n) \equiv (2,3) \bmod 4$, and the other cases are similar. Since $\alpha = (l\sqrt{m} \pm \sqrt{mn})/(2l)$, we have $(2l\alpha - l\sqrt{m})^2 = (\pm\sqrt{mn})^2$. So $\alpha^2 - \sqrt{m}\alpha + (l^2m - mn)/(4l^2) = 0$, i.e. α satisfies the polynomial $X^2 - \sqrt{m}X + (m - m_1n_1)/4 \in \mathcal{O}_K[X]$ because $m_1n_1 \equiv l^2m_1n_1 = mn \equiv 2 \bmod 4$. Therefore, all $\mathcal{O}_K$-monogenic generators of $\mathcal{O}_L$ are of the form $\gamma + \alpha$ for any $\gamma \in \mathcal{O}_K$, and this completes the proof. □

3. Finding All $\mathbb{Z}$-Monogenic Generators of $\mathcal{O}_L$

Recall that a $\mathbb{Z}$-monogenic generator of $\mathcal{O}_L$ is an $\mathcal{O}_K$-monogenic generator of $\mathcal{O}_L$, but the converse is false. From the previous theorem we have obtained all $\mathcal{O}_K$-monogenic generators of $\mathcal{O}_L$. If one of them is a $\mathbb{Z}$-monogenic generator of $\mathcal{O}_L$, then it has to satisfy $\mathcal{O}_L = \mathbb{Z}[a + b\sqrt{m} + \alpha] = \mathbb{Z}[b\sqrt{m} + \alpha]$. So we need to find an integer b such that the discriminant of the minimal polynomial of $b\sqrt{m} + \alpha$ equals the discriminant of the field L. When such b exists, we get a $\mathbb{Z}$-monogenic generator of $\mathcal{O}_L$, and $\mathcal{O}_L$ is monogenic. Finally, under integer translation all $\mathbb{Z}$-monogenic generators of $\mathcal{O}_L$ can be obtained by these specified $b\sqrt{m} + \alpha$. All calculation is in the proof of Theorem 1.1, which is as follows.

Proof of Theorem 1.1. Let $\nu = \pm 1$, let α be defined as in Theorem 2.4, and let $m(X)$ be the minimal polynomial of $b\sqrt{m} + \alpha$. Let α_1, α_2, α_3, and α_4 denote the conjugates of $b\sqrt{m} + \alpha$ for some integer b.

Case 1. $(m,n) \equiv (2,1) \bmod 4$ with $l = 1$:

$$\text{Let } \begin{cases} \alpha_1 = b\sqrt{m} + \frac{1+\nu\sqrt{n}}{2}, & \alpha_3 = -b\sqrt{m} + \frac{1+\nu\sqrt{n}}{2}, \\ \alpha_2 = b\sqrt{m} + \frac{1-\nu\sqrt{n}}{2}, & \alpha_4 = -b\sqrt{m} + \frac{1-\nu\sqrt{n}}{2}. \end{cases}$$

Then $\mathrm{Disc}(m(X))$ is

$$\begin{aligned}&[(\alpha_2-\alpha_1)(\alpha_4-\alpha_3)\cdot(\alpha_3-\alpha_1)(\alpha_4-\alpha_2)\cdot(\alpha_4-\alpha_1)(\alpha_3-\alpha_2)]^2\\=&[n\cdot 4b^2m\cdot(4b^2m-n)]^2.\end{aligned}$$

Set $\mathrm{Disc}(m(X))=\mathrm{D}_{L/\mathbb{Q}}$ by (1) , and simplify it by $l=1$, then we get $b^4(4b^2m-n)^2=1$. Since b and $4b^2m-n$ are integers, it follows that $b=\pm1$ and $4m-n=\pm1$. But $n=4m-1\equiv 3 \bmod 4$ is a contradiction, hence $n=4m+1$ only. Therefore, these algebraic integers $b\sqrt{m}+\alpha=\alpha_1=\mu\sqrt{m}+\frac{1+\nu\sqrt{n}}{2}$ with $\mu,\nu\in\{\pm1\}$ are $\mathbb{Z}$-monogenic generators.

Case 2. $(m,n)\equiv(2,3) \bmod 4$ with $m=-2l$:

$$\text{Let }\begin{cases}\alpha_1=\frac{(2b+1)\sqrt{m}}{2}+\frac{\nu\sqrt{mn}}{2l}, & \alpha_3=-\frac{(2b+1)\sqrt{m}}{2}-\frac{\nu\sqrt{mn}}{2l},\\ \alpha_2=\frac{(2b+1)\sqrt{m}}{2}-\frac{\nu\sqrt{mn}}{2l}, & \alpha_4=-\frac{(2b+1)\sqrt{m}}{2}+\frac{\nu\sqrt{mn}}{2l}.\end{cases}$$

By $m=m_1l=-2l$ and $n=n_1l$ we obtain

$$\begin{aligned}\mathrm{Disc}(m(X))&=\left[m_1n_1\cdot\left((2b+1)^2m-m_1n_1\right)\cdot(2b+1)^2m\right]^2\\&=64l^2n_1^2(2b+1)^4\left[(2b+1)^2l-n_1\right]^2.\end{aligned}$$

Let $\mathrm{Disc}(m(X))=\mathrm{D}_{L/\mathbb{Q}}$, then we have $(2b+1)^4[(2b+1)^2l-n_1]^2=4$ by (1). Since $2b+1$ is an odd integer, it has to be ±1. So $(2b+1)^2l-n_1=l-n_1=\pm2$. After we multiply both sides of $l-n_1=\pm2$ by l, we obtain $l^2-n=\mp m$. Hence these algebraic integers $b\sqrt{m}+\alpha=\alpha_1=\frac{\mu\sqrt{m}}{2}+\frac{\nu\sqrt{mn}}{2l}$ with $\mu,\nu\in\{\pm1\}$ are $\mathbb{Z}$-monogenic generators.

Case 3. $(m,n)\equiv(3,3) \bmod 4$ with $l=1$:

$$\text{Let }\begin{cases}\alpha_1=\frac{(2b+1)\sqrt{m}+\nu\sqrt{n}}{2}, & \alpha_3=\frac{-(2b+1)\sqrt{m}+\nu\sqrt{n}}{2},\\ \alpha_2=\frac{(2b+1)\sqrt{m}-\nu\sqrt{n}}{2}, & \alpha_4=\frac{-(2b+1)\sqrt{m}-\nu\sqrt{n}}{2}.\end{cases}$$

Then $\mathrm{Disc}(m(X))=[n\cdot(2b+1)^2m\cdot\left((2b+1)^2m-n\right)]^2$. The restriction $\mathrm{Disc}(m(X))=\mathrm{D}_{L/\mathbb{Q}}$ gives us $(2b+1)^4[(2b+1)^2m-n]^2=16$ since $l=1$. Again, the integer $2b+1$ is odd, so it must be ±1. Then $(2b+1)^2m-n=m-n=\pm4$. Therefore, these algebraic integers $b\sqrt{m}+\alpha=\alpha_1=\frac{\mu\sqrt{m}+\nu\sqrt{n}}{2}$ with $\mu,\nu\in\{\pm1\}$ are $\mathbb{Z}$-monogenic generators.

Case 4. $(m,n)\equiv(3,3) \bmod 4$ with $m=-l$:

$$\text{Let }\begin{cases}\alpha_1=b\sqrt{m}+\frac{1}{2}+\frac{\nu\sqrt{mn}}{2l}, & \alpha_3=-b\sqrt{m}+\frac{1}{2}-\frac{\nu\sqrt{mn}}{2l},\\ \alpha_2=b\sqrt{m}+\frac{1}{2}-\frac{\nu\sqrt{mn}}{2l}, & \alpha_4=-b\sqrt{m}+\frac{1}{2}+\frac{\nu\sqrt{mn}}{2l}.\end{cases}$$

By $m = m_1 l = -l$ and $n = n_1 l$ we have

$$\begin{aligned}\mathrm{Disc}(m(X)) &= [m_1 n_1 \cdot (4b^2 m - m_1 n_1) \cdot 4b^2 m]^2 \\ &= 16 l^2 n_1^2 b^4 (4b^2 l - n_1)^2.\end{aligned}$$

Set $\mathrm{Disc}(m(X)) = \mathrm{D}_{L/\mathbb{Q}}$, then we have $b^4(4b^2 l - n_1)^2 = 1$. Since b and $4b^2 l - n_1$ are integers, it follows that $b = \pm 1$ and $4b^2 l - n_1 = 4l - n_1 = \pm 1$. By multiplying both sides of $4l - n_1 = \pm 1$ by l, we obtain $4l^2 - n = \mp m$. But $4l^2 = n + m \equiv 2 \bmod 4$ is a contradiction, so we have $n - m = 4l^2$. Hence these algebraic integers $b\sqrt{m} + \alpha = \alpha_1 = \mu\sqrt{m} + \frac{1}{2} + \frac{\nu\sqrt{mn}}{2l}$ with $\mu, \nu \in \{\pm 1\}$ are $\mathbb{Z}$-monogenic generators. □

Example 3.1. Let $a \in \mathbb{Z}$ and $\mu, \nu \in \{\pm 1\}$. The rings of algebraic integers in the following imaginary biquadratic fields are monogenic, which are shown in [4] (see Table 0).

1. $\mathbb{Q}(\sqrt{-2}, \sqrt{-7}) = \mathbb{Q}(\sqrt{-2}, \sqrt{14}) = \mathbb{Q}(\sqrt{-7}, \sqrt{14})$:

Let $(m, n) = (-2, -7) \equiv (2, 1) \bmod 4$. Then $l = 1$ and $n = 4m + 1$. All $\mathbb{Z}$-monogenic generators of the ring of algebraic integers of $\mathbb{Q}(\sqrt{-2}, \sqrt{-7})$ are $a + \mu\sqrt{-2} + \frac{1+\nu\sqrt{-7}}{2}$.

2. $\mathbb{Q}(\sqrt{-2}, \sqrt{3}) = \mathbb{Q}(\sqrt{-6}, \sqrt{3}) = \mathbb{Q}(\sqrt{-2}, \sqrt{-6})$:

Let $(m, n) = (-2, 3) \equiv (2, 3) \bmod 4$. Then $l = 1$, $m = -2l$, and $n + m = l^2$. If we let $(m, n) = (-6, 3) \equiv (2, 3) \bmod 4$, then $l = 3$, $m = -2l$, and $n - m = l^2$. All $\mathbb{Z}$-monogenic generators of the ring of algebraic integers of $\mathbb{Q}(\sqrt{-2}, \sqrt{3})$ are $a + \frac{\mu\sqrt{-2} + \nu\sqrt{-6}}{2}$.

3. $\mathbb{Q}(\sqrt{-13}, \sqrt{-17}) = \mathbb{Q}(\sqrt{-13}, \sqrt{221}) = \mathbb{Q}(\sqrt{-17}, \sqrt{221})$:

Let $(m, n) = (-13, -17) \equiv (3, 3) \bmod 4$. Then $l = 1$, and $n - m = -4$. If we let $(m, n) = (-17, -13) \equiv (3, 3) \bmod 4$, then $l = 1$, and $n - m = 4$. All $\mathbb{Z}$-monogenic generators of the ring of algebraic integers of $\mathbb{Q}(\sqrt{-13}, \sqrt{-17})$ are $a + \frac{\mu\sqrt{-13} + \nu\sqrt{-17}}{2}$.

4. $\mathbb{Q}(\sqrt{-13}, \sqrt{663}) = \mathbb{Q}(\sqrt{-13}, \sqrt{-51}) = \mathbb{Q}(\sqrt{-51}, \sqrt{663})$:

Let $(m, n) = (-13, 663) \equiv (3, 3) \bmod 4$. Then $l = 13$, $m = -l$, and $n - m = 4l^2$. All $\mathbb{Z}$-monogenic generators of the ring of algebraic integers of $\mathbb{Q}(\sqrt{-13}, \sqrt{663})$ are $a + \mu\sqrt{-13} + \frac{1+\nu\sqrt{-51}}{2}$.

5. $\mathbb{Q}(i, \sqrt{3}) = \mathbb{Q}(i, \sqrt{-3}) = \mathbb{Q}(\sqrt{-3}, \sqrt{3})$:

Let $(m, n) = (-1, 3) \equiv (3, 3) \bmod 4$. Then $l = 1$ and $n - m = 4$. Also, we can use another criterion, i.e. $l = 1$, $m = -l$, and $n - m = 4l^2$. All $\mathbb{Z}$-monogenic generators of the ring of algebraic integers of $\mathbb{Q}(i, \sqrt{3})$ are $a + \frac{\mu i + \nu\sqrt{3}}{2}$ and $a + \mu i + \frac{1+\nu\sqrt{-3}}{2}$. Note that $\mathbb{Q}(i, \sqrt{3}) = \mathbb{Q}(\zeta_{12})$ is the field of 12-th roots of unity, and the ring of algebraic integers of any cyclotomic field is monogenic.

4. A Sufficient Condition for the Monogeneity of Real Biquadratic Fields

We consider the real biquadratic fields $\mathbb{Q}(\sqrt{m}, \sqrt{n})$, where m and n are positive integers which satisfy all assumptions in the introduction except $m < 0$. To prove that an element is a $\mathbb{Z}$-monogenic generator, we only need to show that it is an algebraic integer and its discriminant equals the discriminant of the corresponding field. So we change the sign of m in the previous related calculation to obtain the following two theorems.

Theorem 4.1. *Let m and n be distinct positive squarefree integers, $l = (m, n)$, and $K = \mathbb{Q}(\sqrt{m})$. The ring of algebraic integers of the real biquadratic field $L = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ is $\mathcal{O}_K$-monogenic if*

$$\begin{cases} l = 1 & \text{if } (m,n) \equiv (2,1) \bmod 4, \\ m = 2l & \text{if } (m,n) \equiv (2,3) \bmod 4, \\ l = 1, \text{or } m = l & \text{if } (m,n) \equiv (3,3) \bmod 4. \end{cases}$$

Moreover, $\mathcal{O}_K$-monogenic generators of $\mathcal{O}_L$ can be $a + b\sqrt{m} + \alpha$ where a, $b \in \mathbb{Z}$, and

$$\alpha = \begin{cases} \frac{1 \pm \sqrt{n}}{2} & \text{if } (m,n) \equiv (2,1) \bmod 4, \\ \frac{l\sqrt{m} \pm \sqrt{mn}}{2l} & \text{if } (m,n) \equiv (2,3) \bmod 4, \\ \frac{\sqrt{m} \pm \sqrt{n}}{2} \text{ when } l = 1, \text{ and} & \\ \frac{l \pm \sqrt{mn}}{2l} \text{ when } m = l & \text{if } (m,n) \equiv (3,3) \bmod 4. \end{cases}$$

Theorem 4.2. *Let m and n be distinct positive squarefree integers, and $l = (m, n)$. The ring of algebraic integers of the real biquadratic field $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ is monogenic if*

$$\begin{cases} l = 1 \text{ and } \ n = 4m + 1 & \text{if } (m,n) \equiv (2,1) \bmod 4, \\ m = 2l \text{ and } n \pm m = l^2 & \text{if } (m,n) \equiv (2,3) \bmod 4, \\ l = 1 \text{ with } n - m = \pm 4, \text{ or} & \\ m = l \text{ with } n - m = 4l^2 & \text{if } (m,n) \equiv (3,3) \bmod 4. \end{cases}$$

Moreover, the ring of algebraic integers of $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ can be generated by

$$\begin{cases} a + \frac{1}{2} + \mu\sqrt{m} + \frac{\nu\sqrt{n}}{2} & \text{if } (m,n) \equiv (2,1) \bmod 4, \\ a + \frac{\mu\sqrt{m}}{2} + \frac{\nu\sqrt{mn}}{2l} & \text{if } (m,n) \equiv (2,3) \bmod 4, \\ a + \frac{\mu\sqrt{m}}{2} + \frac{\nu\sqrt{n}}{2} & \text{if } (m,n) \equiv (3,3) \bmod 4 \text{ and } l = 1, \\ a + \frac{1}{2} + \mu\sqrt{m} + \frac{\nu\sqrt{mn}}{2l} & \text{if } (m,n) \equiv (3,3) \bmod 4 \text{ and } m = l, \end{cases}$$

where $a \in \mathbb{Z}$ *and* μ, $\nu \in \{\pm 1\}$.

Example 4.3. The rings of algebraic integers in the following real biquadratic fields are monogenic, which are shown in [4] (see Table 0).

1. $\mathbb{Q}(\sqrt{10}, \sqrt{41}\,) = \mathbb{Q}(\sqrt{410}, \sqrt{41}\,) = \mathbb{Q}(\sqrt{10}, \sqrt{410}\,)$:

Let $(m, n) = (10, 41) \equiv (2, 1) \bmod 4$. Then $l = 1$ and $n = 4m + 1$.

2. $\mathbb{Q}(\sqrt{6}, \sqrt{15}\,) = \mathbb{Q}(\sqrt{10}, \sqrt{15}\,) = \mathbb{Q}(\sqrt{6}, \sqrt{10}\,)$:

Let $(m, n) = (6, 15) \equiv (2, 3) \bmod 4$. Then $l = 3$, $m = 2l$, and $n - m = l^2$. If we let $(m, n) = (10, 15) \equiv (2, 3) \bmod 4$, then $l = 5$, $m = 2l$, and $n + m = l^2$.

3. $\mathbb{Q}(\sqrt{3}, \sqrt{7}\,) = \mathbb{Q}(\sqrt{21}, \sqrt{7}\,) = \mathbb{Q}(\sqrt{3}, \sqrt{21}\,)$:

Let $(m, n) = (3, 7) \equiv (3, 3) \bmod 4$. Then $l = 1$, and $n = m + 4$.

4. $\mathbb{Q}(\sqrt{3}, \sqrt{39}\,) = \mathbb{Q}(\sqrt{13}, \sqrt{39}\,) = \mathbb{Q}(\sqrt{3}, \sqrt{13}\,)$:

Let $(m, n) = (3, 39) \equiv (3, 3) \bmod 4$. Then $l = 3$, $m = l$, and $n - m = 4l^2$.

5. Acknowledgments

I would like to thank Larry Washington for his suggestions.

References

[1] M. Chang, Non-monogeneity in a family of sextic fields, *J. Number Theory*, **97** (2002), 252-268.

[2] I. Gaál, On the indices of biquadratic number fields having Galois group V_4, *Arch. Math.*, **57** (1991), 357-361.

[3] I. Gaál, N. Schulte, Computing all power integral bases of cubic fields, *Math Comp.*, **53** (1989), 689-696.

[4] M.N. Gras, Corps biquadratiques monogénées, *Manuscripta Math.*, **86** (1995), 63-79.

[5] G. Nyul, Power integral bases in totally complex biquadratic number fields, *Acta Acda. Paed. Aegriensis, Sect. Math.*, **28** (2001), 79-86.

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