Rep. Fac. Sci. Engrg.
Saga. Univ. Math.
33-1 (2004), 9 ∼ 22.

Reports of the Faculty of Science and Engineering,
Saga University, Mathematics, Vol. 33, No. 1, 2004

On Integral Bases of Certain Real Monogenic Biquadratic Fields

By
Yasuo MOTODA*

Abstract: Let K be a biquadratic field. M.-N. Gras and F. Tanoé gave a necessary and sufficient condition that K is monogenic by using a diophantine equation of degree 4 (Lemma 3). In Theorem, we determine all the generators of power integral bases of certain real monogenic biquadratic fields by using the above equation.

Key Words: real biquadratic field, monogenic field, power basis, unit

1. Introduction. Let $\boldsymbol{Z}$ be the ring of the rational integers. Let K, Z_K and D_K be a real biquadratic field $\boldsymbol{Q}\left(\sqrt{dm}, \sqrt{dn}\right)$ over the rationals $\boldsymbol{Q}$, the ring of integers of K and the discriminant of K, respectively. Let $D(\xi)$ be the discriminant of an integer ξ in Z_K. The index $I(\xi)$ of $\xi \in Z_K$ is defined by $D(\xi) = I(\xi)^2 D_K$. K is said to be monogenic if Z_K has a generator of a power basis, i.e., there exists an integer θ of K such that $Z_K = \boldsymbol{Z}[\theta]$, namely $I(\theta) = 1$.

M.-N. Gras and F. Tanoé [GT] gave a necessary and sufficient condition that a biquadratic field K has a generator of a power basis (Lemma 3 and Remark 5).

In this paper, we treat trivial real monogenic biquadratic fields, which are defined by M.-N. Gras and F. Tanoé [GT] (see Remark 1).

In section 2, we prepare some lemmas. In Lemma 2 we calculate an integral basis by using Hasse's conductor-discriminant formula (Lemma 1).

Received May 1, 2004, Revised June 25, 2004
*Department of Mathematics, Yatsushiro National College of Technology

AMS subject classification: 11R21, 11B39
Partially supported by a grant (#14540033) from the Japan Society for the Promotion of Science.

In the proof of Lemma 3 which is done in section 3, we induce three equations of degree 4 by calculating index $I(\xi)$ of $\xi \in Z_K$.

In the proof of the theorem, we determine all the genarators of power bases of the trivial real monogenic biquadratic fields by applying our key Lemma 5[NP] to above equations. Lemma 5 gives squares in binary sequence which relates units of real quadratic fields.

2. Theorem and preliminaries. In this section, we show the theorem and prepare some lemmas for the proof of the theorem. Let K be a real biquadratic field $\boldsymbol{Q}\left(\sqrt{dm}, \sqrt{dn}\right)$. We may assume that $d,\ m,\ n$ are all positive square-free integers and relatively prime to each other, $dm \equiv dn \pmod 4$, $m \equiv n \equiv 1 \pmod 2$ and $m > n$. Then K is monogenic if and only if the equation

$$(u^2 - v^2)^2(2^\delta m) - (u^2 + v^2)^2(2^\delta n) = \pm 4 \qquad (\natural)$$

has solutions, where δ is equal to 0 or 1 with $mn \equiv (-1)^\delta \pmod 4$ [Remark 5].

Theorem. *Let K be a real biquadratic field $\boldsymbol{Q}\left(\sqrt{dm}, \sqrt{dn}\right)$ with $dm \equiv dn \equiv 2$ or $3 \pmod 4$. Then K is monogenic if and only if $\{u,\ v\}$ in the equation above with $u \geq v \geq 0$, $(u,\ v) = 1$ satisfies one of the following three conditions:*

(1) *The case $d = 1,\ m - n = 4,\ m \equiv n \equiv -1 \pmod 4$. Then we have*
   (i) $u = 1,\ v = 0,$ *or*
   (ii) $m = f^2 + 2,\ n = f^2 - 2,\ u = f,\ v = 1,$ *where $f > 1$ is odd,*

(2) *The case $d = 2,\ m - n = 2$. Then we have*
   (i) $u = 1,\ v = 0,$ *or*
   (ii) $m = 2f^2 + 1, n = 2f^2 - 1,\ u = 2f,\ v = 1,$

(3) *The case $n = 1,\ m - 1 = 4d,\ d \not\equiv 1 \pmod 4$. Then we have $u = v = 1$.*

Then all the generators θ of power bases of Z_K are given by

$$\theta = uv\frac{1 - \delta + 2^\delta\sqrt{mn}}{2} + v^2\sqrt{dn} + (u^2 - v^2)\frac{\sqrt{dm} + \sqrt{dn}}{2}.$$

Remark 1 ([GT]). By the conditions of Theorem, we see that $d = 2^\delta$ or $n = 1$. M.-N. Gras and F. Tanoé called these conditions the trivial cases, where δ is 0 or 1 with $mn \equiv (-1)^\delta \pmod 4$. They gave solutions $\{u,\ v\}$ of Theorem, i.e., $\{u,\ v\} = \{1,\ 0\}$ in the cases (1) and (2), and $\{u,\ v\} = \{1,\ 1\}$ in the case (3). Then we shall call such a field with the above conditions a trivial real monogenic biquadratic field.

Remark 2 ([M_2]). As for the non-trivial real monogenic biquadratic field, the author proved that there exist infinitely many such fields for any pair $\{u,\ v\}$ with $(u,\ v) = 1$ and, at the same time, gave the method of their constructions.

Remark 3 ([KP, P]). A. Pethő determined all CNS bases by using power bases obtained from Theorem (Remark 5). Let K be an algebraic number field with the ring of integers Z_K. It is called CNS (canonical number system) ring if there exists $\alpha \in Z_K$ such that for any non-zero $\gamma \in Z_K$ there are integers $c_0, c_1, \cdots, c_\ell \in \{0, 1, \cdots, |N_{K/Q}(\alpha)| - 1\}$ such that $\gamma = \sum_{i=0}^{\ell} c_i \alpha^i$. It is well known that Z_K is CNS if and only if the field K is monogenic.

Lemma 1 (Hasse's Conductor-Discriminant Formula[W]). Let K be the number field associated to the group X of Dirichelet characters. Then the discriminant of K is given by

$$D(K) = (-1)^{r_2} \prod_{\chi \in X} f_\chi.$$

Here f_χ and $2r_2$ denote the conductor of χ and the number of the complex conjugations of $K/\boldsymbol{Q}$, respectively.

Lemma 2 ([GT, M_1, M_2]). *Let K be a biquadratic field $\boldsymbol{Q}\left(\sqrt{dm}, \sqrt{dn}\right)$. Then an integral basis of Z_K and the discriminant D_K of K are given by the followings;*

(1) *in the case* $dm \equiv dn \equiv 1 \pmod 4$;

$$Z_K = \boldsymbol{Z}\left[1, \frac{1+\sqrt{mn}}{2}, \frac{1+\sqrt{dn}}{2}, \frac{1+e\sqrt{mn}+\sqrt{dm}+\sqrt{dn}}{4}\right],$$

$$D_K = d^2m^2n^2, \text{ where } e = \pm 1 \text{ such that } d \equiv m \equiv n \equiv e \pmod 4,$$

(2) *in the case* $dm \equiv dn \equiv 3 \pmod 4$ *or* (3.1) $dm \equiv dn \equiv 2,\ mn \equiv 1 \pmod 4$;

$$Z_K = \boldsymbol{Z}\left[1, \frac{1+\sqrt{mn}}{2}, \sqrt{dn}, \frac{\sqrt{dm}+\sqrt{dn}}{2}\right],\ D_K = 2^4 d^2 m^2 n^2,$$

(3.2) *in the case* $dm \equiv dn \equiv 2,\ mn \equiv 3 \pmod 4$;

$$Z_K = \boldsymbol{Z}\left[1, \sqrt{mn}, \sqrt{dn}, \frac{\sqrt{dm}+\sqrt{dn}}{2}\right],\ D_K = 2^6 d^2 m^2 n^2.$$

Proof. Since in the case of a quadratic field k, the field discriminant and the conductor of k coinsides with to each other, by Lemma 1 we have $D_K = D_{k_1} D_{k_2} D_{k_3}$, where $k_1 = \boldsymbol{Q}(\sqrt{mn}),\ k_2 = \boldsymbol{Q}(\sqrt{dn}),\ k_3 = \boldsymbol{Q}(\sqrt{dm})$. First we consider the case (1). Since $D_{k_1} = mn,\ D_{k_2} = dn,\ D_{k_3} = dm$, we have $D_K = mn \cdot dn \cdot dm = d^2 m^2 n^2$. Let G be the Galois group of K, which is defined by $\left\langle \sigma, \tau; \sqrt{dn}^{\,\sigma} = -\sqrt{dn},\ \sqrt{dm}^{\,\tau} = -\sqrt{dm} \right\rangle$. For $\alpha_i \in Z_K,\ i = 1, 2, 3, 4$, we define $\Delta[\alpha_1, \alpha_2, \alpha_3, \alpha_4]$ by the determinant

$$\begin{vmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_1^{\sigma} & \alpha_2^{\sigma} & \alpha_3^{\sigma} & \alpha_4^{\sigma} \\ \alpha_1^{\tau} & \alpha_2^{\tau} & \alpha_3^{\tau} & \alpha_4^{\tau} \\ \alpha_1^{\sigma\tau} & \alpha_2^{\sigma\tau} & \alpha_3^{\sigma\tau} & \alpha_4^{\sigma\tau} \end{vmatrix}.$$

If $\Delta^2[\alpha_1, \alpha_2, \alpha_3, \alpha_4] = \pm D_K$, then we have $Z_K = \boldsymbol{Z}[\alpha_1, \alpha_2, \alpha_3, \alpha_4]$.

Now since $\frac{1+\sqrt{dm}}{2} \times \frac{1+\sqrt{dn}}{2} = \frac{d-e}{4}\sqrt{mn} + \frac{1+e\sqrt{mn}+\sqrt{dm}+\sqrt{dn}}{4}$, we have $\frac{1+e\sqrt{mn}+\sqrt{dm}+\sqrt{dn}}{4} \in Z_K$. Then we have

$$\Delta^2\left[1, \tfrac{1+\sqrt{mn}}{2}, \tfrac{1+\sqrt{dn}}{2}, \tfrac{1+e\sqrt{mn}+\sqrt{dm}+\sqrt{dn}}{4}\right] = 2^{-8}\Delta^2[1, \sqrt{mn}, \sqrt{dm}, \sqrt{dn}]$$

$$= 2^{-8}\begin{vmatrix} 1 & \sqrt{mn} & \sqrt{dm} & \sqrt{dn} \\ 1 & \sqrt{mn}^{\,\sigma} & \sqrt{dm}^{\,\sigma} & \sqrt{dn}^{\,\sigma} \\ 1 & \sqrt{mn}^{\,\tau} & \sqrt{dm}^{\,\tau} & \sqrt{dn}^{\,\tau} \\ 1 & \sqrt{mn}^{\,\sigma\tau} & \sqrt{dm}^{\,\sigma\tau} & \sqrt{dn}^{\,\sigma\tau} \end{vmatrix}^2 = 2^{-8}\begin{vmatrix} 1 & \sqrt{mn} & \sqrt{dm} & \sqrt{dn} \\ 1 & -\sqrt{mn} & \sqrt{dm} & -\sqrt{dn} \\ 1 & -\sqrt{mn} & -\sqrt{dm} & \sqrt{dn} \\ 1 & \sqrt{mn} & -\sqrt{dm} & -\sqrt{dn} \end{vmatrix}^2$$

$$= 2^{-8}(mn)(dn)(dn)\begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{vmatrix}^2 = d^2 m^2 n^2.$$

Therfore we have

$$Z_K = \boldsymbol{Z}\left[1, \frac{1+\sqrt{mn}}{2}, \frac{1+\sqrt{dn}}{2}, \frac{1+e\sqrt{mn}+\sqrt{dm}+\sqrt{dn}}{4}\right].$$

Similarly, we can obtain the discriminants and integral bases in the cases (2), (3,1) and (3,2). ∎

Remark 4 ([GT]). Lemma 2 (2), (3.1) and (3,2) are presented by the following form;

$$Z_K = \boldsymbol{Z}\left[1, \frac{1-\delta+2^\delta\sqrt{mn}}{2}, \sqrt{dn}, \frac{\sqrt{dm}+\sqrt{dn}}{2}\right],\ D_K = 4^{2+\delta}d^2m^2n^2,$$

where δ is 0 or 1 with $mn \equiv (-1)^\delta \pmod 4$.

We will prove Lemma 3 after Proposition 1 in section 3.

Lemma 3 ([GT]). *Let K be a biquadratic field $\boldsymbol{Q}\left(\sqrt{dm}, \sqrt{dn}\right)$, then K is monogenic if and only if one of the following conditions is satisfied* ;

(1) *In the case* (3.1) $dm \equiv dn \equiv 2,\ mn \equiv 1 \pmod 4$ *or* $dm \equiv dn \equiv 3 \pmod 4$, *and* $m-n = 4d$, *the equation* $(u^2-v^2)^2m-(u^2+v^2)^2n = \pm 4$ *has a solution* $\{u,v\}$ *in* $\boldsymbol{Z}$, *or*

(2) *in the case* (3.2) $dm \equiv dn \equiv 2,\ mn \equiv 3 \pmod 4$, *and* $m-n = d$, *the equation* $(u^2-v^2)^2m-(u^2+v^2)^2n = \pm 2$ *has a solution* $\{u,v\}$ *in* $\boldsymbol{Z}$.

Remark 5 ([GT]). Two equations of Lemma 3 are presented by the following form;

$$(u^2-v^2)^2(2^\delta m)-(u^2+v^2)^2(2^\delta n) = \pm 4$$

where δ is equal to 0 or 1 with $mn \equiv (-1)^\delta \pmod 4$.

If K is monogenic, then we have $Z_K = \boldsymbol{Z}[\theta]$ with

$$\theta = uv\frac{1-\delta+2^\delta\sqrt{mn}}{2} + v^2\sqrt{dn} + (u^2-v^2)\frac{\sqrt{dm}+\sqrt{dn}}{2}.$$

Remark 6. From the equation (2) of Lemma 2, θ is determined up to parallel transformations by a rational integer, the signature of u, v, u^2-v^2, u^2+v^2, and permutation u and v. Especially, it is admissible to permute u^2 and $-u^2$, and v^2 and $-v^2$ simultaneously, because the following identity holds;

$$\pm u^2 = \frac{\pm(u^2+v^2) \pm (u^2-v^2)}{2}, \quad \pm v^2 = \frac{\pm(u^2+v^2) \mp (u^2-v^2)}{2}.$$

Let $G = <\sigma> \times <\tau>$ be the Galois group of $K/\boldsymbol{Q}$, where $\sqrt{dm}^{\,\sigma} = \sqrt{dm}$, $\sqrt{dn}^{\,\sigma} = -\sqrt{dn}$ and $\sqrt{dm}^{\,\tau} = -\sqrt{dm}$, $\sqrt{dn}^{\,\tau} = \sqrt{dn}$. By Lemma 2, θ is also determined up to automorphisms of K. Because the following identity holds;

$$\begin{aligned}\theta^{\sigma} &= uv\frac{1-\delta-2^{\delta}\sqrt{mn}}{2} - v^2\sqrt{dn} + (u^2-v^2)\frac{\sqrt{dm}-\sqrt{dn}}{2} \\ &= uv(1-\delta) - uv\frac{1-\delta+2^{\delta}\sqrt{mn}}{2} - u^2\sqrt{dn} - (v^2-u^2)\frac{\sqrt{dm}+\sqrt{dn}}{2}.\end{aligned}$$

We can obtain the similar results for the cases θ^{τ} and $\theta^{\sigma\tau}$.

Lemma 4 ([NS, M_2]). *Let $K = \boldsymbol{Q}\left(\sqrt{dm}, \sqrt{dn}\right)$ and let k be a quadratic subfield of K. Then K does not have any power basis if one of the following conditions is satisfied;*
(1) *2 decomposes completely in k, say $(2) = \mathfrak{p}_1\mathfrak{p}_2$, and $\mathfrak{p}_1$ remains prime or decomposes completely in K/k,*
(2) *3 decomposes completely in $K/\boldsymbol{Q}$.*

Remark 7. If $K = \boldsymbol{Q}(\sqrt{DM}, \sqrt{DN})$ satisfies the condition $DM \equiv DN \equiv 1 \pmod 4$, then by using Lemma 4, we can show that K is non-monogenic [M_2].
In the cases $DM \equiv DN \equiv 2$ or $3 \pmod 4$, 2 ramifies in $k = \boldsymbol{Q}(\sqrt{DM})$, say $(2) = \mathfrak{p}^2$. In these cases, there exists infinitely many real monogenic biquadratic fields satisfying each of following condition in K/k;
(i) $\mathfrak{p}$ remains prime, (ii) $\mathfrak{p}$ decomposes completely or (iii) $\mathfrak{p}$ ramifies [M_2].

3. The proofs of Lemma 3 and Theorem. First we prepare one lemma and two propositins for the proof of Lemma 3 and Theorem.

Proposition 1. *Let $a > 1$ and $b > 1$ be relatively prime and square-free rational integers. Assume that the equation $ax^2 - by^2 = k$ has a solution $\{x_0, y_0\}$, with the positive minimal unit $\frac{1}{k}(x_0\sqrt{ak} + y_0\sqrt{bk})$, where $k = 1$, 2 or 4. Moreover we assume that the fundamental unit ε of the quadratic field $\boldsymbol{Q}(\sqrt{ab})$ is presented by the form $v + u\sqrt{ab}$ with rational integers u, v if $k = 1$ and asuume that $x_0 \equiv y_0 \equiv 1 \pmod 2$ if $k = 4$. Then ε is equal to $\frac{1}{k}\left(ax_0^2 + by_0^2 + 2x_0y_0\sqrt{ab}\right)$ with positive norm.*

Proof. By the identities $(ax)^2 - aby^2 = ak$, we obtan $\varepsilon_0 = \dfrac{ax_0 + y_0\sqrt{ab}}{ax_0 - y_0\sqrt{ab}} = \frac{1}{k}(ax_0^2 + by_0^2 + 2x_0y_0\sqrt{ab})$ and $\varepsilon_0^{-1} = \dfrac{ax_0 - y_0\sqrt{ab}}{ax_0 + y_0\sqrt{ab}} = \frac{1}{k}(ax_0^2 + by_0^2 - 2x_0y_0\sqrt{ab})$. So ε_0 is a unit with positive norm. Let ε be the fundamental unit > 1 of $\boldsymbol{Q}\left(\sqrt{ab}\right)$. ε is presented by the form $\frac{1}{e}(v + u\sqrt{ab})$, where u, v are rational integers and $e = 1$ if $k = 1$ or 2, $e = 2$ if $k = 4$. Now we show that $N(\varepsilon) = 1$, where the symbol $N(\cdot)$ denotes the norm of an integer of $\boldsymbol{Q}\left(\sqrt{ab}\right)$. If $\varepsilon_0 = \frac{1}{k}(x_0\sqrt{a} + y_0\sqrt{b})^2$ is equal to an even power ε^{2r} of ε, with a positive rational integer r, then $\frac{1}{\sqrt{k}}(x_0\sqrt{a} + y_0\sqrt{b}) = \varepsilon^r$. This does not occur, for the left hand side is an irrational integer of degree 4, while the right hand side is one of degree 2. So ε_0 is equal to an odd power of ε. Threfore we obtain $N(\varepsilon) = 1$ because $N(\varepsilon_0) = 1$. Hence we have $\varepsilon^{-1} = \frac{1}{e}(v - u\sqrt{ab}) > 0$. Then $\sqrt{\varepsilon_0}\varepsilon^{-1} = \frac{1}{\sqrt{k}}(x_0\sqrt{a} + y_0\sqrt{b}) \cdot \frac{1}{e}(v - u\sqrt{ab})$ is a unit $\frac{1}{ek}\left((x_0v - y_0bu)\sqrt{ak} + (y_0v - x_0au)\sqrt{bk}\right)$ of the biquadratic field $\boldsymbol{Q}\left(\sqrt{ak}, \sqrt{bk}\right)$. Then since $\sqrt{\varepsilon_0}\varepsilon^{-1}$ has degree 4, we have $\frac{1}{ek}(x_0v - y_0bu) \neq 0$, $\frac{1}{ek}(y_0v - x_0au) \neq 0$, which are coefficients of the $\sqrt{ak}$-part and $\sqrt{bk}$-part, respectively. By the minimality of $\sqrt{\varepsilon_0}$ and $\sqrt{\varepsilon_0}\varepsilon^{-1} < \sqrt{\varepsilon_0}$, we obtain (i) $x_0v - y_0bu > 0$ and $y_0v - x_0au < 0$ or (ii) $x_0v - y_0bu < 0$ and $y_0v - x_0au > 0$. Now

$$\begin{aligned} \varepsilon^0 \leq \quad \varepsilon_0\varepsilon^{-1} &= \frac{1}{k}(ax_0^2 + by_0^2 + 2x_0y_0\sqrt{ab}) \cdot \frac{1}{e}(v - u\sqrt{ab}) \\ &= \frac{1}{ek}\left((ax_0^2 + by_0^2)v - 2abx_0y_0u - \{(ax_0^2 + by_0^2)u - 2x_0y_0v\}\sqrt{ab}\right). \end{aligned}$$

We evaluate the coefficient of the $\sqrt{ab}$-part. In the case (i), we have
$0 \leq \frac{1}{ek}\left((ax_0^2 + by_0^2)u - 2x_0y_0v\right) < \frac{1}{ek}\left((ax_0^2 + by_0^2)u - 2y_0 \cdot y_0bu\right) = \frac{1}{ek}(ax_0^2 - by_0^2)u = \frac{1}{e}u$.
Thus we obtain $\varepsilon_0\varepsilon^{-1} = 1$ namely $\varepsilon_0 = \varepsilon$. In the case (ii), we have $0 \leq (ax_0^2 + by_0^2)u -$

$2x_0y_0v < (ax_0^2 + by_0^2)u - 2x_0 \cdot x_0au = -(ax_0^2 - by_0^2)u = -ku$, which is a contradiction. Therefore ε_0 is the fundamental unit.

∎

Remark 8. On the equation above in the case $k = 1$, if the fundamental unit ε of $\boldsymbol{Q}\left(\sqrt{ab}\right)$ does not belong to $\boldsymbol{Z}[\sqrt{ab}]$, then $\frac{1}{k}\left(ax_0^2 + by_0^2 + 2x_0y_0\sqrt{ab}\right)$ is equal to ε^3 [Remark 9]. For each $k = 1,\ 2$ and 4, Proposition 1 relates to equations of Lemma 3 or Remark 5. We must use this proposition for the proof of Theorem.

Remark 9. Let $\varepsilon = \frac{1}{2}(v + u\sqrt{D})$ be the fundamental unit of the quadratic field $\boldsymbol{Q}(\sqrt{D})$, where $u \equiv v \equiv 1 \pmod 2$ and D is a square-free positive integer. Then we have $D \equiv 5 \pmod 8$. Put $\varepsilon^n = \frac{1}{2}(v_n + u_n\sqrt{D})$. Then $v_n \equiv u_n \equiv 0 \pmod 2$ i.e., ε^n belongs to $\boldsymbol{Z}[\sqrt{D}]$ if and only if $n \equiv 0 \pmod 3$. These results are well known. If $ax_0^2 - by_0^2 = 1$ with $x_0,\ y_0$ are minimal positive integers, $a > 1, b > 1$ and the fundamental uint ε does not belong to $\boldsymbol{Z}[\sqrt{D}]$ Then we have $ax_0^2 + by_0^2 + 2x_0y_0\sqrt{ab} = \varepsilon^3$. For example, the fields $\boldsymbol{Q}(\sqrt{21})$ has the fundamental unit $\varepsilon = \frac{1}{2}(5 + \sqrt{21})$ which does not belong to $\boldsymbol{Z}[\sqrt{21}]$ and $\varepsilon^3 = 55 + 12\sqrt{21} = (3\sqrt{3} + 2\sqrt{7})^2,\ 3^2 \cdot 3 - 2^2 \cdot 7 = 1$, i.e., $a = 3, b = 7, x_0 = 3, y_0 = 2$. Also, the field $\boldsymbol{Q}(\sqrt{69})$ has the fundamental unit $\varepsilon = \frac{1}{2}(25 + 3\sqrt{69})$ with positive norm. Therefore the equation $3x^2 - 23y^2 = 4$ has a solution $x_0 = 3,\ y_0 = 1$.

On the other hand, the field $\boldsymbol{Q}(\sqrt{85})$ has the fundamental unit $\varepsilon = \frac{1}{2}(81 + \sqrt{85})$ with negative norm. Therefore the equation $5x^2 - 17y^2 = \pm 4$ does not have any solution.

Proof of Lemma 3. Assume K is monogenic and let ξ be a generator of a power basis of Z_K. We calculate the index of ξ. Put $\xi = a_0 + a_1\frac{1 - \delta + 2^\delta\sqrt{mn}}{2} + a_2\sqrt{dn} + a_3\frac{\sqrt{dm} + \sqrt{dn}}{2}$, where $a_i,\ i = 0, 1, 2, 3$ are rational integers. Then we have
$D(\xi) = \{(\xi - \xi^\tau)(\xi - \xi^\tau)^\sigma \cdot (\xi - \xi^\sigma)(\xi - \xi^\sigma)^\tau \cdot (\xi - \xi^{\sigma\tau})(\xi - \xi^{\sigma\tau})^\tau\}^2$. Now put $x = a_1, y = 2a_2 + a_3, z = a_3$. Then we have $y \equiv z \pmod 2$ and $(\xi - \xi^\tau)(\xi - \xi^\tau)^\sigma = (2^\delta x\sqrt{mn} + z\sqrt{dm})(-2^\delta x\sqrt{mn} + z\sqrt{dm}) = z^2dm - 4^\delta x^2mn = 2^\delta m\frac{z^2d - 4^\delta x^2n}{2^\delta}$, $(\xi - \xi^\sigma)(\xi - \xi^\sigma)^\tau = (2^\delta x\sqrt{mn} + y\sqrt{dn})(-2^\delta x\sqrt{mn} + y\sqrt{dn}) = y^2dn - 4^\delta x^2mn = 2^\delta n\frac{y^2d - 4^\delta x^2m}{2^\delta}$ and $(\xi - \xi^{\sigma\tau})(\xi -$

$\xi^{\sigma\tau})^{\tau} = (y\sqrt{dn}+z\sqrt{dm})(y\sqrt{dn}-z\sqrt{dm}) = y^2dn-z^2dm = 2^{2-\delta}d\frac{y^2n-z^2m}{2^{2-\delta}}$, where $\frac{z^2d-4^{\delta}x^2n}{2^{\delta}}$, $\frac{y^2d-4^{\delta}x^2m}{2^{\delta}}$ and $\frac{y^2n-z^2m}{2^{2-\delta}}$ are rational integers. Therefore $D(\xi)$
$= 2^{4+2\delta}d^2m^2n^2\cdot(\frac{z^2d-4^{\delta}x^2n}{2^{\delta}})^2\cdot(\frac{y^2d-4^{\delta}x^2m}{2^{\delta}})^2\cdot(\frac{y^2n-z^2m}{2^{2-\delta}})^2$. Since $D_K = 2^{4+2\delta}d^2m^2n^2$, we have $I(\xi) = |\frac{z^2d-4^{\delta}x^2n}{2^{\delta}}\cdot\frac{y^2d-4^{\delta}x^2m}{2^{\delta}}\cdot\frac{y^2n-z^2m}{2^{2-\delta}}| = 1$ namely $z^2d-4^{\delta}x^2n = \pm 2^{\delta},\ y^2d-4^{\delta}x^2m = \pm 2^{\delta},\ y^2n-z^2m = \pm 2^{2-\delta}$. Now we have the identity:

$$(\xi-\xi^{\tau})(\xi-\xi^{\tau})^{\sigma}-(\xi-\xi^{\sigma})(\xi-\xi^{\sigma})^{\tau}+(\xi-\xi^{\tau\sigma})(\xi-\xi^{\tau\sigma})^{\tau} = 0$$

namely $2^{\delta}m \mp 2^{\delta}n \pm 2^{2-\delta}d = 0$. Since $m > n$, we obtain (i) $2^{\delta}m-2^{\delta}n = 2^{2-\delta}d$ or (ii) $2^{\delta}m+2^{\delta}n = 2^{2-\delta}d$. For solutions of Pythagorian equation $X^2+Y^2 = Z^2$ i.e., $(X,Y,Z) = 1$, it has a property $Z \equiv 1 \pmod 2$. Therefore from the case (i) we can obtain $(y^2-z^2)d = 4^{\delta}x^2(m-n)$, and $m-n = 4^{1-\delta}d$, i.e., $y^2-z^2 = 4x^2$, hence $y^2 = z^2+4x^2$. In the Gauss field $\boldsymbol{Q}(i)$, since $(z+2xi, z-2xi) = 1$, we can put $(u+vi)^2 = z+2xi$ for a suitable Gauss integer $u+vi$. Then we have $u^2-v^2 = z, uv = x$, hence $y = u^2+v^2$. Moreover we can deduce that the case (ii) does not occur. In fact, if $m+n = 4^{1-\delta}d$, then $mn+n^2 \equiv 4^{1-\delta}dn \pmod 4$,namely $mn \equiv -1+4^{1-\delta}dn \pmod 4$. If $\delta = 0$, then $mn \equiv -1 \equiv (-1)^{\delta} \pmod 4$, hence $\delta = 1$, whichi is a contradiction. If $\delta = 1$, then $mn \equiv -1+dn \pmod 4$, and $mn \equiv (-1)^{\delta} \equiv -1 \pmod 4$ hence $dn \equiv 0 \pmod 4$, whichi is a contradiction, because dn is square-free. Therefore we obtained Remark 5 and hence Lemma 3. ∎

Proposition 2. Let D be not a square integer and let $\varepsilon = \frac{1}{2}(v+\sqrt{D})$ be the fundamental unit of $\boldsymbol{Q}(\sqrt{D})$ with a positive norm. Put $\varepsilon^n = \frac{1}{2}(v_n+u_n\sqrt{D})$. Then the sequences $\{v_n\}$ and$\{u_n\}$ have the same binary recurrent sequence $X_{n+2} = vX_{n+1}-X_n$ with initial conditions $v_0 = 2,\ v_1 = v,\ u_0 = 0,\ u_1 = 1$. Further we have $u_{n+1} = \frac{1}{2}(vu_n+v_n)$.

Proof. ε is a solution of the equation $x^2-vx+1 = 0$. Then we have $\varepsilon^{n+2}-v\varepsilon^{n+1}+\varepsilon^n = 0$. So the sequences $\{v_n\}$ and$\{u_n\}$ have the same binary recurrent sequence $X_{n+2} = vX_{n+1}-X_n$. Since $\varepsilon^{n+1} = \varepsilon^n\cdot\varepsilon$, we have $\frac{1}{2}(v_{n+1}+u_{n+1}\sqrt{D}) = \frac{1}{2}(v_n+u_n\sqrt{D})\cdot\frac{1}{2}(v+\sqrt{D})$ and hence $u_{n+1} = \frac{1}{2}(vu_n+v_n)$. ∎

Lemma 5 ([NP]). *Let* $a > 2$ *be a rational integer,* $D = a^2 - 4 \geq 5$ *with* D *is not square and* S *is the set of the square rational integers. Put* $\alpha = \frac{1}{2}(a+\sqrt{D})$, $\alpha^n = \frac{1}{2}(v_n+u_n\sqrt{D})$. *Then* $u_n \in cS$ *for* $n > 3$ *and* $c \in \{1, 2, 3, 6\}$ *if and only if* $(n, a, c) = (4, 338, 1)$ *or* $(6, 3, 1)$. *Here* α *is a unit of* $\boldsymbol{Q}(\sqrt{D})$ *and has the positive norm with respect to* $\boldsymbol{Q}\left(\sqrt{D}\right)/\boldsymbol{Q}$.

Proof of Theorem. Let K be trivial and monogenic. we note that $d = 2^\delta$, where δ is 0 or 1 with $mn \equiv (-1)^\delta \pmod 4$ or $n = 1$. Put $x = uv, y = u^2 + v^2, z = u^2 - v^2$ in Lemma 3. First, assume $d = 2^\delta$ and put $u = 1$, $v = 0$, then we have $y = z = 1$ and the equations of Lemma 3 are satisfied. Moreover if $d = 1$, then $m \equiv n \equiv 3 \pmod 4$ by Lemma 3 (1). Next, assume $n = 1$ and put $u = v = 1$, then we have $y = 2$, $z = 0$ and by Remark 5, $-4 \cdot 2^\delta n = -4$. This holds when $\delta = 0$. Then we have $m - 1 = 4d$, $d \not\equiv 1 \pmod 4$ by Lemma 3. We have obtained (1)(i), (2)(i) and (3) of Theorem.

So we assume $u > v \geq 1$. We show that any other trivial and monogenic biquadratic field does not exist and at the same time, we search all the other power bases. First, we consider the case (1) $d = 1$, $\delta = 0$. Since $m = n + 4$, we have $mn \equiv 1 \pmod 4$. The case $m = 5, n = 1$ does not occur because K should be a biquadratic field. Since $m \cdot 1^2 - n \cdot 1^2 = 4$, by Proposition 1 the fundamental unit ε of $\boldsymbol{Q}(\sqrt{mn})$ is equal to $\frac{1}{4}(m \cdot 1^2 + n \cdot 1^2 + 2\sqrt{mn})$ namely $\frac{1}{2}(m - 2 + \sqrt{mn})$ with positive norm. Any prime factor of n ramifies in $\boldsymbol{Q}(\sqrt{mn})$. If there exist integers α and β of $\boldsymbol{Q}(\sqrt{mn})$ such that $N(\alpha) = n$ and $N(\beta) = -n$, then $(\alpha)^2 = (\beta)^2$ namely $(\alpha) = (\beta)$ as ideals. So $\dfrac{\alpha}{\beta}$ is a unit of $\boldsymbol{Q}(\sqrt{mn})$ with the negative norm. This is a contradiction. Since $N(\frac{1}{2}(n + \sqrt{mn})) = -n$, we obtain $\frac{1}{4}\{(yn)^2 - z^2 mn\} = n \cdot (\pm 1) = -n$. Then there exists a unit $\varepsilon^k = \frac{1}{2}(v_k + u_k\sqrt{mn})$ such that $\frac{1}{2}(yn + z\sqrt{mn}) = \frac{1}{2}(n + \sqrt{mn}) \cdot \frac{1}{2}(v_k + u_k\sqrt{mn})$ and hence

$$\begin{cases} y = \frac{1}{2}(v_k + u_k m) \\ z = \frac{1}{2}(v_k + u_k n). \end{cases}$$

Therefore by Proposition 2, we have

$$(2uv)^2 = y^2 - z^2 = u_k\{2v_k + 2u_k(m-2)\} = 4u_k u_{k+1}.$$

We may assume $k \geq 0$ because $u_{-k} = -u_k$. Since $(u_k, u_{k+1}) = 1$, u_k and u_{k+1} are square numbers. But by Lemma 5, if $k > 3$, then at most one of u_k or u_{k+1} is a square number. This is a contradiction. Two sequences $\{v_k\}$ and $\{u_k\}$ are given by

$$\{v_k\} = \{2,\ m-2,\ (m-2)^2-2,\ (m-2)^3-3(m-2),\ \cdots\},$$
$$\{u_k\} = \{0,\ 1,\ (m-2),\ (m-2)^2-1,\ \cdots\}.$$

Then $u_3 = (m-2)^2 - 1$ is not square. We can obtain $k = 1$ or $k = 0$ because $4u_k u_{k+1}$ is square. If $k = 1$, then $m - 2 = f^2$ i.e. $m = f^2 + 2$ and $n = f^2 - 2$, where $f > 1$ is odd and $u^2 + v^2 = y = m - 1$, $u^2 - v^2 = z = m - 3$, $u = f$, $v = 1$. This is the case (1) (ii). If $k = 0$, then $y = 1, z = 1, u = 1, v = 0$. This case is excluded because we assume $v \geq 1$.

Next, we consider the case (2) $d = 2$, $\delta = 1$. Since $m - n = 2$, by Proposition 1 the fundamental unit ε of $\boldsymbol{Q}(\sqrt{mn})$ is equal to $\frac{1}{2}(m + n + 2\sqrt{mn})$ namely $m - 1 + \sqrt{mn}$ with positive norm. By the assumption, we obtain $N(n + \sqrt{mn}) = -2n$. So on the signature of the right hand side, by the same reason as in the case (1), we obtain $(yn)^2 - z^2 mn = -2n$. Then there exists a unit $\varepsilon^k = \dfrac{v_k + u_k\sqrt{4mn}}{2}$ such that $yn + z\sqrt{mn} = (n + \sqrt{mn})\dfrac{v_k + u_k\sqrt{4mn}}{2}$ and hence

$$\begin{cases} y = \dfrac{v_k}{2} + u_k m \\ z = \dfrac{v_k}{2} + u_k n, \end{cases}$$

Therfore by Proposition 2, we have

$$(2uv)^2 = y^2 - z^2 = 4u_k\left(\frac{v_k}{2} + u_k(m-1)\right) = 4u_k u_{k+1}.$$

By the same way as in the case (1), we may assume $k \geq 0$. Since $(u_k, u_{k+1}) = 1$, u_k and u_{k+1} are square numbers. But by the same reason as in the case (1), $k > 3$ is impossible.

Two sequences $\{v_k\}$ and $\{u_k\}$ are given by

$$\{v_k\} = \{2,\ 2(m-1),\ 4(m-1)^2-2,\ 8(m-1)^3-5(m-1),\ \cdots\},$$
$$\{u_k\} = \{0,\ 1,\ 2(m-1),\ 4(m-1)^2-1,\ \cdots\}.$$

Since $u_3 = 4(m-1)^2 - 1$ is not square, we obtain $k = 1$ or $k = 0$ because $4u_k u_{k+1}$ is square. If $k = 1$, then $2(m-1) = (2f)^2$, i.e. $m = 2f^2 + 1$, $n = 2f^2 - 1$ and $u^2 + v^2 = y = 2m - 1$, $u^2 - v^2 = z = 2m - 3$, $u = 2f$, $v = 1$. This is the case (2) (ii). If $k = 0$, then $u = 1, v = 0$. This case is excluded because we assume $v \geq 1$.

Finally, we consider the case (3) $n = 1$. We may show the following two cases;

$(*)_1$ if $n = 1$, $\delta = 0$, then $u = v = 1$.

$(*)_2$ if $n = 1$, $\delta = 1$, then $m = 3$, $d = 2$. This case is contained in (2) (ii).

Now we consider the case $(*)_1$ $n = 1$, $\delta = 0$. Then $m - 4d = 1$. By Proposition 1 the fundamental unit of $\boldsymbol{Q}\left(\sqrt{dm}\right)$ is equal to $m + 4d + 4\sqrt{dm}$ namely $2m - 1 + \sqrt{16dm}$ with positive norm. From $y^2 - z^2 m = \pm 4$ and $m - 1 = 4d$, we obtain $x^2 m - y^2 d = \pm 1$ and hence $(yd)^2 - dmx^2 = \mp d$. Since $N(2d + \sqrt{dm}) = -d$, we obtain $(yd)^2 - dmx^2 = -d$. Then there exists a unit $\varepsilon^k = \dfrac{v_k + u_k\sqrt{64dm}}{2}$ such that $yd + x\sqrt{dm} = (2d + \sqrt{dm})\dfrac{v_k \pm u_k\sqrt{64dm}}{2}$ and hence

$$\begin{cases} y = v_k + 4mu_k, \\ x = \dfrac{v_k}{2} + 8du_k. \end{cases}$$

So by proposition 2 we have

$$z^2 = y^2 - 4x^2 \;=\; 16u_k\{\frac{v_k}{2} + (m + 4d)u_k\} = 16u_k u_{k+1}.$$

Since $(u_k, u_{k+1}) = 1$, u_k and u_{k+1} are square numbers. However by Lemma 5, $k > 3$ is imposible. Two sequences $\{v_k\}$ and $\{u_k\}$ are given by

$$\{v_k\} = \{2,\ 2(2m-1),\ 4(2m-1)^2 - 2,\ 8(2m-1)^3 - 6(2m-1),\ \cdots\},$$
$$\{u_k\} = \{0,\ 1,\ 2(2m-1),\ 4(2m-1)^2 - 1,\ \cdots\}.$$

$u_2 = 2(2m-1)$ and $u_3 = 4(2m-1)^2 - 1$ are not square numbers. So we have $k = 0$ and hence $z = 0$, $u = v = 1$. Therefore in the case $n = 1$, $\delta = 0$, we obtain $u = v = 1$.

Now we consider the case $(*)_2$ $n = 1$, $\delta = 1$. In this case, we have $m \equiv 3 \pmod 4$. By Remark 3 (2), $y^2 - z^2 m = \mp 2$ and hence $m(2x)^2 - dy^2 = \mp 2$. Especially, we see that $2|d$. Then $2mx^2 - \dfrac{d}{2}y^2 = \mp 1$. We may assume $\dfrac{d}{2} \neq 1$, because in the case $\dfrac{d}{2} = 1$, we have already considered in the case (2) and have obtained $u = 2$, $v = 1$, $m = 3$, $d = 2$.

Then since the above equation satisfies the conditoin of Proposition 1, we can obtain the fundamental unit $\varepsilon = 2mx_0^2 + \frac{d}{2}y_0^2 + 2x_0y_0\sqrt{dm}$ of the quadratic field $\boldsymbol{Q}\left(\sqrt{dm}\right)$ with the minimal solution $\{x_0, y_0\}$ of the equation $2mx^2 - \frac{d}{2}y^2 = \mp 1$. On the other hand, since the fundamental unit of $\boldsymbol{Q}\left(\sqrt{dm}\right)$ is given by $\varepsilon = 2m - 1 + 2\sqrt{dm}$, we have $2mx_0^2 + \frac{d}{2}y_0^2 = 2m - 1$. But this does not occur because $2mx_0^2 + \frac{d}{2}y_0^2 > 2m - 1$. Thus in the case $n = 1,\ \delta = 1,$ we obtain $m = 3,\ d = 2$.

Therefore we have proved theorem completely. ∎

Corollary. *We solved completely the following equations with $u,\ v$ variables and m parameter, and all the solutions are given the followings*;

(1) $(u^2 + v^2)^2 - u^2v^2m = 1,\ m \equiv -1 \pmod 4$ *and* $m,\ m - 4$ *are squarefree, then* $\{u,\ v\} = \{1,\ 0\},$ *and* $\{f,\ 1\}$ *with* $f > 1$ *is odd if* $m = f^2 + 2$.

(2) $(u^2 + v^2)^2 - 2u^2v^2m = 1,$ *and* $m,\ m - 2$ *are squarefree, then* $\{u,\ v\} = \{1,\ 0\},$ *and* $\{2f,\ 1\}$ *if* $m = 2f^2 + 1$.

(3) $(u^2 - v^2)^2m - (u^2 + v^2)^2 = -4,\ m \not\equiv 5 \pmod{16}$ *and* $m,\ \frac{m-1}{4}$ *are square-free, then* $\{u,\ v\} = \{1,\ 1\}$.

Remark 10. We partially prove Corollary by solving above equations directly.

First we consider the case (1) and try to find solutions with $u > v \geq 1$. We have $u^4 - (m-2)v^2u^2 + v^4 - 1 = 0$ and hence $u^2 = \frac{1}{2}\left((m-2)v^2 \pm \sqrt{m(m-4)v^4 + 1}\right)$. Then we can put $t^2 = m(m-4)v^4 + 1$. So we have $t^2 - m(m-4)v^4 = 1$. By duality of the equation (1) with respect to u and v, we can obtain the equation $s^2 - m(m-4)u^4 = 1$. Then we can apply Lemma 5 to these relations. By similar argument of the proof of Theorem (1), we can obtain $u^2 = u_2 = m - 2 = f^2$ and $v^2 = u_1 = 1$ and hence $u = f,\ v = 1$.

Next we consider the case (2) and try to find solutions with $u > v \geq 1$. We have $u^4 - 2(m-1)v^2u^2 + v^4 - 1 = 0$ and hence $u^2 = (m-1)v^2 \pm \sqrt{m(m-2)v^4 + 1}$. Then we can put $t^2 = m(m-2)v^4 + 1$. So we have $t^2 - m(m-2)v^4 = 1$. Similarly we can obtain $s^2 - m(m-2)u^4 = 1$. By the same argument as above we can obtain $u^2 = u_2 = 2(m-1) =$

$(2f)^2$ and $v^2 = u_1 = 1$ and hence $u = 2f,\ v = 1$.

Remark 11. Three fundamental units in the proof of theorem and two of them in Remark 10 are of all Richaud-Degart type[D, H]. These units are obtained from the equations of Proposition 1.

References

[D] G. Degart, *Über die Bestimmung der Gruneinheit gewißer reell-quadratisher Zhalkörper,* Abh. Math. Semi. Univ. Hamburg, **22**(1958), 92-97.

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

[H] H. Hasse, *Über mehrklassige, aber eingeschlechtige reell-quadratische Zahlkörper,* El. Math., **XX**(1965), 49-59.

[KP] B. Kovács and A. Pethő, *Number Systems in Integral Domains, Especially in Ordes of Algebraic Number Fields,* Acta Sci. Math., **55**(1991), 287-299.

[M_1] Y. Motoda, *On Biquadratic Fields*, Mem. Fac. Sci. Kyushu Univ., Series A, **29**-2 (1975), 263-268.

[M_2] Y. Motoda, *Notes on Quartic Fields*, Rep. Fac. Sci. Engrg. Saga Univ. Math. **32**-1 (2003), 1-19.

[NP] K. Nakamula and A. Pethő, *Squares in Binary Recurrence*, Proceedings of the International Conference held in Eger,Hungary July 29 - August, 1996, Walter de Gruyter. Berlin - New York 1998,409-421.

[P] A. Pethő, *Connections Between Power Integral Bases and Radix Representations in Algebraic Number Fields*, preprint.

[SN] S. I. A. Shah and T. Nakahara, *Monogenesis of the Rings of Integers in Certain Imaginary Abelian Fields,* Nagoya Math. J. **168**(2002), 85-92.

[W] L. C. Washington, Introduction to cyclotomic fields, Graduate texts in mathematics **83**, Springer-Verlag, New York-Heidelberg-Berlin, 1980.

Yasou Motoda

Yatsushiro National College of Technology
2627 hirayama shinmachi
Kumamoto 866-8501
Japan

E-mail: motoda@as.yatsushiro-nct.ac.jp