Canad. Math. Bull. Vol. 13 (4), 1970

INTEGERS OF BIQUADRATIC FIELDS

BY
KENNETH S. WILLIAMS(1)

Let Q denote the field of rational numbers. If m, n are distinct squarefree integers the field formed by adjoining $\sqrt{m}$ and $\sqrt{n}$ to Q is denoted by $Q(\sqrt{m}, \sqrt{n})$. Since $Q(\sqrt{m}, \sqrt{n})=Q(\sqrt{m}+\sqrt{n})$ and $\sqrt{m}+\sqrt{n}$ has for its unique minimal polynomial $x^4-2(m+n)x^2+(m-n)^2$, $Q(\sqrt{m}, \sqrt{n})$ is a biquadratic field over Q. The elements of $Q(\sqrt{m}, \sqrt{n})$ are of the form $a_0+a_1\sqrt{m}+a_2\sqrt{n}+a_3\sqrt{mn}$, where $a_0, a_1, a_2, a_3 \in Q$. Any element of $Q(\sqrt{m}, \sqrt{n})$ which satisfies a monic equation of degree ≥ 1 with rational integral coefficients is called an integer of $Q(\sqrt{m}, \sqrt{n})$. The set of all these integers is an integral domain. In this paper we determine the explicit form of the integers of $Q(\sqrt{m}, \sqrt{n})$ (Theorem 1), an integral basis for $Q(\sqrt{m}, \sqrt{n})$ (Theorem 2), and the discriminant of $Q(\sqrt{m}, \sqrt{n})$ (Theorem 3). (With $Q(\sqrt{m}, \sqrt{n})$ considered as a relative quadratic field, that is, as a quadratic field over $Q(\sqrt{m})$, an integral basis for $Q(\sqrt{m}, \sqrt{n})$ has been given in [1].)

The form of the integers of a quadratic field are well known [3]. If k is a squarefree integer then the integers of $Q(\sqrt{k})$ are given by $\frac{1}{2}(x_0+x_1\sqrt{k})$, where x_0, x_1 are integers such that $x_0\equiv x_1 \pmod 2$, if $k\equiv 1 \pmod 4$; and by $x_0+x_1\sqrt{k}$, where x_0, x_1 are integers, if $k\equiv 2$ or $3 \pmod 4$. Thus we know the integers of the subfields $Q(\sqrt{m})$, $Q(\sqrt{n})$, $Q(\sqrt{mn})$ of $Q(\sqrt{m}, \sqrt{n})$.

We begin by making some simplifying assumptions about m and n. We let $l=(m, n)$ and write $m=lm_1$, $n=ln_1$ so that $(m_1, n_1)=1$. Since m, n are squarefree we have the following possibilities for the residues of m, n, m_1n_1 modulo 4.

m	n	m_1n_1
1	1	1
1	2	2
1	3	3
2	1	2
2	2	1 or 3
2	3	2
3	1	3
3	2	2
3	3	1

Received by the editors March 16, 1970.

(1) This research was supported by National Research Council of Canada Grant A-7233.

Thus as

$$Q(\sqrt{m}, \sqrt{n}) = Q(\sqrt{m}, \sqrt{m_1 n_1}) = Q(\sqrt{n}, \sqrt{m_1 n_1}) = Q(\sqrt{n}, \sqrt{m})$$

we may suppose without loss of generality that

(1) $$(m, n) \equiv (1, 1), (1,2), (2, 3) \text{ or } (3, 3) \pmod 4.$$

We now determine the form of the integers of $Q(\sqrt{m}, \sqrt{n})$, where (here and throughout) m, n satisfy (1).

THEOREM 1. *Letting x_0, x_1, x_2, x_3 denote rational integers, the integers of $Q(\sqrt{m}, \sqrt{n})$ are given as follows*:

(i) *if* $(m, n) \equiv (m_1, n_1) \equiv (1, 1) \pmod 4$, *the integers are*

$$\tfrac{1}{4}(x_0 + x_1\sqrt{m} + x_2\sqrt{n} + x_3\sqrt{m_1 n_1}),$$

where $x_0 \equiv x_1 \equiv x_2 \equiv x_3 \pmod 2$, $x_0 - x_1 + x_2 - x_3 \equiv 0 \pmod 4$;

(ii) *if* $(m, n) \equiv (1, 1)$, $(m_1, n_1) \equiv (3, 3) \pmod 4$, *the integers are*

$$\tfrac{1}{4}(x_0 + x_1\sqrt{m} + x_2\sqrt{n} + x_3\sqrt{m_1 n_1}),$$

where $x_0 \equiv x_1 \equiv x_2 \equiv x_3 \pmod 2$, $x_0 - x_1 - x_2 - x_3 \equiv 0 \pmod 4$;

(iii) *if* $(m, n) \equiv (1, 2) \pmod 4$, *the integers are*

$$\tfrac{1}{2}(x_0 + x_1\sqrt{m} + x_2\sqrt{n} + x_3\sqrt{m_1 n_1}),$$

where $x_0 \equiv x_1$, $x_2 \equiv x_3 \pmod 2$;

(iv) *if* $(m, n) \equiv (2, 3) \pmod 4$, *the integers are*

$$\tfrac{1}{2}(x_0 + x_1\sqrt{m} + x_2\sqrt{n} + x_3\sqrt{m_1 n_1}),$$

where $x_0 \equiv x_2 \equiv 0$, $x_1 \equiv x_3 \pmod 2$;

(v) *if* $(m, n) \equiv (3, 3) \pmod 4$, *the integers are*

$$\tfrac{1}{2}(x_0 + x_1\sqrt{m} + x_2\sqrt{n} + x_3\sqrt{m_1 n_1}),$$

where $x_0 \equiv x_3$, $x_1 \equiv x_2 \pmod 2$.

Proof. Let θ be an integer of $Q(\sqrt{m}, \sqrt{n})$, where m, n satisfy (1). Then θ can be written

(2) $$\theta = a_0 + a_1\sqrt{m} + a_2\sqrt{n} + a_3\sqrt{m_1 n_1},$$

where $a_0, a_1, a_2, a_3 \in Q$. As θ is an integer of $Q(\sqrt{m}, \sqrt{n})$ so are its conjugates over Q, namely,

(3) $$\begin{cases} \theta' = a_0 + a_1\sqrt{m} - a_2\sqrt{n} - a_3\sqrt{m_1 n_1}, \\ \theta'' = a_0 - a_1\sqrt{m} + a_2\sqrt{n} - a_3\sqrt{m_1 n_1}, \\ \theta''' = a_0 - a_1\sqrt{m} - a_2\sqrt{n} + a_3\sqrt{m_1 n_1}. \end{cases}$$

The three quantities

$$\tag{4} \begin{cases} \theta+\theta' = 2a_0+2a_1\sqrt{m} \in Q(\sqrt{m}), \\ \theta+\theta'' = 2a_0+2a_2\sqrt{n} \in Q(\sqrt{n}), \\ \theta+\theta''' = 2a_0+2a_3\sqrt{m_1n_1} \in Q(\sqrt{m_1n_1}), \end{cases}$$

are therefore all integers of $Q(\sqrt{m}, \sqrt{n})$. Hence they must be integers of $Q(\sqrt{m})$, $Q(\sqrt{n})$, $Q(\sqrt{m_1n_1})$ respectively.

We consider the cases $(m, n)\equiv(1, 2), (2, 3), (3, 3) \pmod 4$ first so that at least two of m, n, m_1n_1 are not congruent to 1 (mod 4), and so at least two of (4) have integral coefficients. Since $2a_0$ is common to all three of (4), the third one must also have integral coefficients. Hence $2a_0$, $2a_1$, $2a_2$, $2a_3$ are all integers and we can write (2) as

$$\tag{5} \theta = \tfrac{1}{2}(b_0+b_1\sqrt{m}+b_2\sqrt{n}+b_3\sqrt{m_1n_1}),$$

where b_0, b_1, b_2, b_3 are all integers. Let us define

$$\tag{6} c = b_0^2-m_1n_1b_3^2, \qquad d = b_0^2-mb_1^2-nb_2^2+m_1n_1b_3^2, \\ e = 2(b_0b_3-b_1b_2l),$$

so that θ satisfies

$$\tag{7} \theta^4-2b_0\theta^3+\left(c+\frac{d}{2}\right)\theta^2+\frac{(b_3m_1n_1e-b_0d)}{2}\theta+\frac{(d^2-m_1n_1e^2)}{16} = 0.$$

If $\theta \in Q(\sqrt{m})$, $Q(\sqrt{n})$ or $Q(\sqrt{m_1n_1})$ the theorem is easily verified so we suppose that $\theta \notin Q(\sqrt{m})$, $Q(\sqrt{n})$, $Q(\sqrt{m_1n_1})$. Thus the coefficients of (7) must all be integers, that is, we must have

$$\tag{8} d^2-m_1n_1e^2 \equiv 0 \pmod{16},$$

since as e is even this implies that d must be even too.

If $(m, n)\equiv(1, 2) \pmod 4$, so that $l\equiv 1 \pmod 2$, $m_1n_1\equiv 2 \pmod 4$, (8) is equivalent to $d\equiv e\equiv 0 \pmod 4$, or

$$\tag{9a} b_0^2-b_1^2-2b_2^2+2b_3^2 \equiv 0 \pmod 4,$$

$$\tag{9b} b_0b_3-b_1b_2 \equiv 0 \pmod 2.$$

If $b_0\not\equiv b_1 \pmod 2$ then $b_0^2-b_1^2\equiv 1 \pmod 2$ and (9a) is insoluble. Thus we must have $b_0\equiv b_1 \pmod 2$, so $b_0^2-b_1^2\equiv 0 \pmod 4$ and (9a) implies $2(b_2^2-b_3^2)\equiv 0 \pmod 4$, that is $b_2\equiv b_3 \pmod 2$. Clearly (9b) is then satisfied and this proves case (iii) of the theorem.

If $(m, n)\equiv(2, 3) \pmod 4$, so that $l\equiv 1 \pmod 2$, $m_1n_1\equiv 2 \pmod 4$, (8) is equivalent to $d\equiv e\equiv 0 \pmod 4$, or

$$\tag{10a} b_0^2-2b_1^2+b_2^2+2b_3^2 \equiv 0 \pmod 4,$$

$$\tag{10b} b_0b_3-b_1b_2 \equiv 0 \pmod 2.$$

If either b_0 or b_2 is odd (10a) implies that the other is odd too. Then (10b) implies $b_1 \equiv b_3 \pmod 2$ and (10a) becomes $1-2b_1^2+1+2b_1^2 \equiv 0 \pmod 4$, which is impossible. Thus $b_0 \equiv b_2 \equiv 0 \pmod 2$ and so $b_1 \equiv b_3 \pmod 2$. This proves case (iv) of the theorem.

If $(m, n) \equiv (3, 3) \pmod 4$, so that $l \equiv 1 \pmod 2$, $m_1 n_1 \equiv 1 \pmod 4$, (8) is equivalent to $d \equiv e \pmod 4$, or

$$b_0^2+b_1^2+b_2^2+b_3^2 \equiv 2(b_0b_3-b_1b_2) \pmod 4,$$

or

$$(b_0-b_3)^2+(b_1+b_2)^2 \equiv 0 \pmod 4.$$

Thus we have $b_0 \equiv b_3$, $b_1 \equiv b_2 \pmod 2$, which proves case (v) of the theorem.

We now consider the case $(m, n) \equiv (1, 1) \pmod 4$, which has been excluded up to this point. We have $m_1 n_1 \equiv 1 \pmod 4$ so that $2a_0, 2a_1, 2a_2, 2a_3$ are either all integers or all halves of odd integers.

If $2a_0, 2a_1, 2a_2, 2a_3$ are all integers then as in the case $(m, n) \equiv (3, 3) \pmod 4$ we have $d \equiv e \pmod 4$, that is,

$$b_0^2-b_1^2-b_2^2+b_3^2 \equiv 2(b_0b_3-b_1b_2) \pmod 4,$$

or

$$(b_0-b_3)^2-(b_1-b_2)^2 \equiv 0 \pmod 4,$$

which implies

$$b_0-b_3 \equiv b_1-b_2 \pmod 2$$

or

$$b_0-b_1+b_2-b_3 \equiv 0 \pmod 2.$$

This gives θ in the form $\frac{1}{4}(c_0+c_1\sqrt{m}+c_2\sqrt{n}+c_3\sqrt{m_1n_1})$, with c_0, c_1, c_2, c_3 integers such that

$$c_0 \equiv c_1 \equiv c_2 \equiv c_3 \equiv 0 \pmod 2, \qquad c_0-c_1 \pm c_2-c_3 \equiv 0 \pmod 4.$$

If $2a_0, 2a_1, 2a_2, 2a_3$ are all halves of odd integers we can write (2) as

$$\theta = \tfrac{1}{4}(c_0+c_1\sqrt{m}+c_2\sqrt{n}+c_3\sqrt{m_1n_1}), \tag{11}$$

where c_0, c_1, c_2, c_3 are integers such that $c_0 \equiv c_1 \equiv c_2 \equiv c_3 \equiv 1 \pmod 2$. We have

$$\begin{gathered} c = \frac{c_0^2-m_1n_1c_3^2}{4}, \qquad d = \frac{c_0^2-mc_1^2-nc_2^2+m_1n_1c_3^2}{4}, \\ e = \frac{c_0c_3-c_1c_2l}{2}. \end{gathered} \tag{12}$$

These are all integers as $c_0 \equiv c_1 \equiv c_2 \equiv c_3 \equiv l \equiv 1 \pmod 2$ and $m \equiv n \equiv m_1 n_1 \equiv 1 \pmod 4$. Moreover

$$\begin{aligned} c_0^2 - mc_1^2 - nc_2^2 + m_1 n_1 c_3^2 &\equiv 1-m-n+m_1 n_1 \pmod 8 \\ &\equiv 1-m-n+l^2 m_1 n_1 \pmod 8 \\ &= 1-m-n+mn \\ &= (1-m)(1-n) \\ &\equiv 0 \pmod 8, \end{aligned}$$

so that d is even. Now θ satisfies

$$\theta^4 - c_0\theta^3 + \left(c+\frac{d}{2}\right)\theta^2 + \left(\frac{c_3 m_1 n_1 e - c_0 d}{4}\right)\theta + \left(\frac{d^2 - m_1 n_1 e^2}{16}\right) = 0. \tag{13}$$

Clearly $\theta \notin Q(\sqrt{m}), Q(\sqrt{n}), Q(\sqrt{m_1 n_1})$ so that the coefficients of (13) must all be integers, that is, we must have

$$d^2 - m_1 n_1 e^2 \equiv 0 \pmod{16}, \tag{14}$$

since (14) implies, as $d \equiv 0 \pmod 2$, $m_1 n_1 \equiv 1 \pmod 4$, that $d \equiv e \pmod 4$ and so

$$c_3 m_1 n_1 e - c_0 d \equiv c_3 e - c_0 d \equiv d(c_3 - c_0) \equiv 0 \pmod 4.$$

Clearly as $d \equiv 0 \pmod 2$, (14) is equivalent to $d \equiv e \pmod 4$.

Writing $c_i = 2d_i + 1$ $(i = 0, 1, 2, 3)$ we have

$$\begin{aligned} d &= (d_0^2 - md_1^2 - nd_2^2 + m_1 n_1 d_3^2) + (d_0 - md_1 - nd_2 + m_1 n_1 d_3) + \frac{(1-m-n+m_1 n_1)}{4} \\ &\equiv (d_0^2 - d_1^2 - d_2^2 + d_3^2) + (d_0 - d_1 - d_2 + d_3) + \frac{(1-m-n+m_1 n_1)}{4} \pmod 4, \end{aligned}$$

and

$$e = (2d_0 d_3 - 2ld_1 d_2) + (d_0 - ld_1 - ld_2 + d_3) + \frac{1-l}{2}.$$

Thus if $l \equiv 1 \pmod 4$, so that $(m_1, n_1) \equiv (1, 1) \pmod 4$, we have

$$d \equiv (d_0^2 - d_1^2 - d_2^2 + d_3^2) + (d_0 - d_1 - d_2 + d_3) + \frac{1-l}{2} \pmod 4,$$

$$e \equiv (2d_0 d_3 - 2d_1 d_2) + (d_0 - d_1 - d_2 + d_3) + \frac{1-l}{2} \pmod 4,$$

and so $d \equiv e \pmod 4$ gives

$$(d_0 - d_3)^2 - (d_1 - d_2)^2 \equiv 0 \pmod 4,$$

that is

$$d_0 - d_3 \equiv d_1 - d_2 \pmod 2,$$

or

$$c_0 - c_1 + c_2 - c_3 \equiv 0 \pmod 4,$$

which completes the proof of case (i) of the theorem.

If $l \equiv 3 \pmod 4$, so that $(m_1, n_1) \equiv (3, 3) \pmod 4$, we have

$$d \equiv (d_0^2 - d_1^2 - d_2^2 + d_3^2) + (d_0 - d_1 - d_2 + d_3) + \frac{1+l}{2} \pmod 4,$$

$$e \equiv (2d_0d_3 + 2d_1d_2) + (d_0 + d_1 + d_2 + d_3) + \frac{1-l}{2} \pmod 4,$$

and so $d \equiv e \pmod 4$ gives

$$(d_0 - d_3)^2 - (d_1 + d_2)^2 - 2(d_1 + d_2) - 1 \equiv 0 \pmod 4,$$

that is,

$$d_0 - d_3 \equiv d_1 + d_2 + 1 \pmod 2,$$

or

$$c_0 - c_1 - c_2 - c_3 \equiv 0 \pmod 4,$$

which completes the proof of case (ii) of the theorem.

We give three simple examples of Theorem 1.

EXAMPLE 1. $\theta = \frac{1}{4}(5 + 3\sqrt{5} + \sqrt{13} + 3\sqrt{65})$ is an integer of $Q(\sqrt{5}, \sqrt{13})$. θ satisfies $\theta^4 - 5\theta^3 - 71\theta^2 + 120\theta + 1044 = 0$.

EXAMPLE 2. $\theta = \frac{1}{4}(1 + \sqrt{21} + \sqrt{33} - \sqrt{77})$ is an integer of $Q(\sqrt{21}, \sqrt{33})$. θ satisfies $\theta^4 - \theta^3 - 16\theta^2 + 37\theta - 17 = 0$.

EXAMPLE 3. The integers of $Q(\sqrt{2}, \sqrt{-1})$ are of the form $a_0 + a_1\sqrt{2} + a_2\sqrt{-1} + a_3\sqrt{-2}$, where a_0, a_2 are both integers and a_1, a_3 are both integers or both halves of odd integers (see [2] for example).

As a consequence of Theorem 1 we have

THEOREM 2. *An integral basis for $Q(\sqrt{m}, \sqrt{n})$ is given by*

(i) $\left\{1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \frac{1+\sqrt{m}+\sqrt{n}+\sqrt{m_1n_1}}{4}\right\}$, *if* $(m, n) \equiv (1, 1)$, $(m_1, n_1) \equiv (1, 1) \pmod 4$,

(ii) $\left\{1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \frac{1-\sqrt{m}+\sqrt{n}+\sqrt{m_1n_1}}{4}\right\}$, *if* $(m, n) \equiv (1, 1)$, $(m_1, n_1) \equiv (3, 3) \pmod 4$,

(iii) $\left\{1, \frac{1+\sqrt{m}}{2}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{m_1n_1}}{2}\right\}$, *if* $(m, n) \equiv (1, 2) \pmod 4$,

(iv) $\left\{1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{m}+\sqrt{m_1n_1}}{2}\right\}$, *if* $(m, n) \equiv (2, 3)$ mod 4),

(v) $\left\{1, \sqrt{m}, \frac{\sqrt{m}+\sqrt{n}}{2}, \frac{1+\sqrt{m_1n_1}}{2}\right\}$, *if* $(m, n) \equiv (3, 3) \pmod 4$.

Proof. We just give the proof of (i) since the other four cases are very similar. By Theorem 1 the general integer of $Q(\sqrt{m}, \sqrt{n})$ can be written $\frac{1}{4}(x_0+x_1\sqrt{m}+x_2\sqrt{n}+x_3\sqrt{m_1n_1})$, where x_0, x_1, x_2, x_3 are integers such that

$$x_0 \equiv x_1 \equiv x_2 \equiv x_3 \pmod 2, \qquad x_0-x_1+x_2-x_3 \equiv 0 \pmod 4.$$

Write $z_3 = x_3$. As $x_0 \equiv x_1 \equiv x_2 \equiv z_3 \pmod 2$ there are integers y, z_1, z_2, such that

$$x_0 = z_3+2y, \qquad x_1 = z_3+2z_1, \qquad x_2 = z_3+2z_2.$$

But as $x_0-x_1+x_2-z_3 \equiv 0 \pmod 4$ we have $y \equiv z_1+z_2 \pmod 2$, so there is an integer z_0 such that $y = 2z_0+z_1+z_2$. Hence

$$\tfrac{1}{4}(x_0+x_1\sqrt{m}+x_2\sqrt{n}+x_3\sqrt{m_1n_1})$$

$$= z_0+z_1\left(\frac{1+\sqrt{m}}{2}\right)+z_2\left(\frac{1+\sqrt{n}}{2}\right)+z_3\left(\frac{1+\sqrt{m}+\sqrt{n}+\sqrt{m_1n_1}}{4}\right),$$

which proves the result as

$$1, \quad \frac{1+\sqrt{m}}{2}, \quad \frac{1+\sqrt{n}}{2}, \quad \frac{1+\sqrt{m}+\sqrt{n}+\sqrt{m_1n_1}}{4},$$

are integers of $Q(\sqrt{m}, \sqrt{n})$.

We illustrate Theorem 2 with a simple example.

Example 4. An integral basis for $Q(\sqrt{5}, \sqrt{13})$ is

$$\{\alpha_0, \alpha_1, \alpha_2, \alpha_3\} = \left\{1, \frac{1+\sqrt{5}}{2}, \frac{1+\sqrt{13}}{2}, \frac{1+\sqrt{5}+\sqrt{13}+\sqrt{65}}{4}\right\}$$

and the integer $\frac{1}{4}(5+3\sqrt{5}+\sqrt{13}+3\sqrt{65})$ is given in terms of this integral basis as $\alpha_0-\alpha_2+3\alpha_3$.

Finally as the discriminant of an algebraic number field is just the discriminant of an integral basis of the field, we have

Theorem 3. *The discriminant of $Q(\sqrt{m}, \sqrt{n})$ is given by*

(i) $l^2m_1^2n_1^2$, *if* $(m, n) \equiv (1, 1) \pmod 4$,
(ii) $16l^2m_1^2n_1^2$, *if* $(m, n) \equiv (1, 2)$ or $(3, 3) \pmod 4$,
(iii) $64l^2m_1^2n_1^2$, *if* $(m, n) \equiv (2, 3) \pmod 4$.

Thus, for example, we have

Example 5. The discriminant of $Q(\sqrt{2}, \sqrt{-1})$ is 256.

REFERENCES

1. H. Hancock, *Foundations of the theory of algebraic numbers*, Dover, N.Y., Vol. **2** (1964), 392–396.

2. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford Univ. Press, London, 4th ed. (1960), 230–231.

3. H. Pollard, *The theory of algebraic numbers*, Carus Math. Monograph, No. 1, M.A.A. Publ. (1961), 61–63.

CARLETON UNIVERSITY,
OTTAWA, ONTARIO

CORRECTIONS

On the Hahn–Banach Extension Property, by TING-ON TO. Canad. Math. Bull. (1) **13** (1970), 9–13.

A minor error in the proof of the theorem on page 12 is corrected upon replacing the penultimate sentence by "Let V_1 be a subspace of V complementary to V_0. Then $V_1 \cong V/V_0$ and $V = V_1 \oplus V_0$, the algebraic direct sum of the subspaces V_1 and V_0."

A Note on Endomorphism Semigroups, by CRAIG PLATT. Canad. Math. Bull. (1) **13** (1970), 47–48.

On page 48, the fourth sentence of paragraph 2 should read "If $\psi \in \text{End}\,(\mathfrak{B})$, then because of β_a, β_d, and β_c, we have $\psi(a) = a$, $\psi(d) = d$, and $\psi(c) = c$."