*Far East J. Math. Sci.* 6(1) (1998), 1-14

# AN EXPLICIT INTEGRAL BASIS FOR A PURE CUBIC FIELD

**BLAIR K. SPEARMAN and KENNETH S. WILLIAMS**

( Received July 31, 1997 )

Submitted by K. K. Azad

**Abstract**

An explicit integral basis of the form

$$\left\{1,\ (a_1+\theta)/d_1,\ \left(a_2+a_3\theta+\theta^2\right)/d_2\right\},$$

where $a_1$, $a_2$, $a_3$, $d_1$, $d_2$ are integers, is given for a pure cubic field $K = Q(\theta)$, where $\theta^3 + a\theta + b = 0$.

## 1. Introduction

Every pure cubic field $F$ over the rational field $Q$ can be given in the form

$$F = Q(\theta), \qquad \theta^3 + a\theta + b = 0, \tag{1.1}$$

where $a$ and $b$ are integers such that the polynomial $X^3 + aX + b$ is irreducible in $Q[X]$ and its discriminant is of the form $-3c^2$ for some positive integer $c$, that is,

$$-4a^3 - 27b^2 = -3c^2. \tag{1.2}$$

In this note we obtain an explicit integral basis for $F$ in the form

1991 Mathematics Subject Classification: Primary 11R16, 11R04, 11R29.

Key words and phrases : pure cubic field, integral basis.

Research of the second author supported by a Natural Sciences and Engineering Research Council of Canada Grant A-7233.

$\{1, (a_1 + \theta)/d_1, (a_2 + a_3\theta + \theta^2)/d_2\}$ for suitable integers $a_1, a_2, a_3, d_1, d_2$. Such a basis has been given when $a = 0$ $\left(\text{in which case } K = Q\left(\sqrt[3]{-b}\right)\right)$ by Dedekind (see for example [2]), so we may assume that $a \neq 0$. Clearly $b \neq 0$. Throughout this paper $p$ denotes a prime and $v_p(m)$ denotes the unique nonnegative integer $e$ such that $p^e \mid m$, $p^{e+1} \nmid m$ (written $p^e \parallel m$), where $m$ is a nonzero integer. If $v_p(a) \geq 2$ and $v_p(b) \geq 3$ then $F = Q(\theta/p)$, where $(\theta/p)^3 + (a/p^2)(\theta/p) + (b/p^3) = 0$. Hence we may also assume that

$$v_p(a) < 2 \quad \text{or} \quad v_p(b) < 3 \quad \text{for every prime } p. \tag{1.3}$$

From (1.2) we see that

$$a = 3A, \qquad c = 3C, \tag{1.4}$$

for some integers $A$ and $C$, and (1.2) can be written in the form

$$(C + b)(C - b) = 4A^3. \tag{1.5}$$

As $a \neq 0$ we see that $A \neq 0$, $C + b \neq 0$, and $C - b \neq 0$. Thus

$$R = \frac{1}{2}(C + b), \qquad S = \frac{1}{2}(C - b), \tag{1.6}$$

are nonzero integers satisfying

$$R - S = b, \qquad R + S = C, \tag{1.7}$$

and

$$RS = A^3 = (a/3)^3. \tag{1.8}$$

In view of (1.8) we can define squarefree, coprime, positive integers $h$ and $k$ by

$$h = \prod_{\substack{p \\ v_p(R) \equiv 1 \pmod 3}} p = \prod_{\substack{p \\ v_p(S) \equiv 2 \pmod 3}} p, \tag{1.9}$$

$$k = \prod_{\substack{p \\ v_p(R) \equiv 2 \pmod 3}} p = \prod_{\substack{p \\ v_p(S) \equiv 1 \pmod 3}} p. \tag{1.10}$$

We also define nonzero integers $\ell$ and $m$ by

$$\ell = \operatorname{sgn}(R) \prod_{\substack{p \\ v_p(R)\equiv 0 \pmod 3}} p^{v_p(R)/3} \prod_{\substack{p \\ v_p(R)\equiv 1 \pmod 3}} p^{(v_p(R)-1)/3} \prod_{\substack{p \\ v_p(R)\equiv 2 \pmod 3}} p^{(v_p(R)-2)/3} \quad (1.11)$$

and

$$m = \operatorname{sgn}(S) \prod_{\substack{p \\ v_p(S)\equiv 0 \pmod 3}} p^{v_p(S)/3} \prod_{\substack{p \\ v_p(R)\equiv 1 \pmod 3}} p^{(v_p(S)-1)/3} \prod_{\substack{p \\ v_p(S)\equiv 2 \pmod 3}} p^{(v_p(S)-2)}. \quad (1.12)$$

From (1.9)-(1.12) we deduce that

$$R = hk^2\ell^3, \qquad S = h^2km^3. \quad (1.13)$$

Appealing to (1.8) and (1.13), we obtain

$$A = hk\ell m, \qquad a = 3hk\ell m. \quad (1.14)$$

Further, from (1.4), (1.7) and (1.13), we have

$$b = hk\left(k\ell^3 - hm^3\right) \quad (1.15)$$

and

$$C = hk\left(k\ell^3 + hm^3\right), \qquad c = 3hk\left(k\ell^3 + hm^3\right). \quad (1.16)$$

From (1.3), (1.14) and (1.15), we deduce that

$$(\ell, m) = 1. \quad (1.17)$$

Thus we can choose $u$ and $v$ to be integers satisfying

$$\ell u + mv = 1. \quad (1.18)$$

It is also convenient to define an integer $F$ by

$$E = k\ell^3 + hm^3. \quad (1.19)$$

From (1.16) and (1.19) we have

$$C = hkE, \qquad c = 3hkE. \quad (1.20)$$

We also define $\phi_1 \in K$ and $\phi_2 \in K$ by

$$\phi_1 = \frac{2hk\ell m^2 - k\ell^2\theta + m\theta^2}{E} \tag{1.21}$$

and

$$\phi_2 = \frac{2hk\ell^2 m + hm^2\theta + \ell\theta^2}{E}. \tag{1.22}$$

Squaring (1.21) and (1.22), and appealing to (1.1), (1.14), (1.15) and (1.19), we obtain

$$\phi_1^2 = k\phi_2, \quad \phi_2^2 = h\phi_1, \tag{1.23}$$

so that

$$\phi_1\phi_2 = hk, \quad \phi_1^3 = hk^2, \quad \phi_2^3 = h^2k. \tag{1.24}$$

From (1.24) we see that $\phi_1$ and $\phi_2$ are algebraic integers so that $\phi_1 \in O_K$, $\phi_2 \in O_K$. Further, as $h$ and $k$ are squarefree, coprime, positive integers, we have $hk^2 =$ perfect cube $\Rightarrow h = k = 1 \Rightarrow a = 3\ell m$, $b = \ell^3 - m^3 \Rightarrow x^3 + ax + b$ has root $x = m - \ell$ contradicting that $x^3 + ax + b$ is irreducible. Hence $hk^2$ is not a perfect cube so that $\left[Q(\phi_1) : Q\right] = 3$ and

$$K = Q(\theta) = Q(\phi_1) = Q\left(\omega\sqrt[3]{hk^2}\right), \tag{1.25}$$

for some cube root of unity $\omega$. Thus the discriminant $d(K)$ of $K$ is given by

$$\begin{aligned} d(K) &= d\left(Q\left(\omega\sqrt[3]{hk^2}\right)\right) \\ &= d\left(Q\left(\sqrt[3]{hk^2}\right)\right) \\ &= \begin{cases} -27h^2k^2, & \text{if } h^2k^4 \not\equiv 1 \pmod 9, \\ -3h^2k^2, & \text{if } h^2k^4 \equiv 1 \pmod 9, \end{cases} \end{aligned} \tag{1.26}$$

see for example [2: p. 340].

The following proposition is proved in Section 2.

**Proposition 1.** *One and only one of the following cases occurs:*

(A) $a \equiv 6 \pmod 9, \quad b \equiv \pm 2 \pmod 9, \quad b^2 \equiv -a+1 \pmod{27},$

(B) $a \equiv 6 \pmod 9, \quad b \equiv \pm 2 \pmod 9, \quad b^2 \not\equiv -a+1 \pmod{27},$

(C) $a \equiv 3 \pmod 9, \quad b \equiv 0 \pmod 9,$

(D) $a \equiv 3 \pmod 9, \quad b \equiv \pm 3 \pmod 9,$

(E) $a \equiv 0 \pmod 9, \quad b \equiv \pm 1 \pmod 9,$

(F) $a \equiv 0 \pmod 9, \quad b \equiv \pm 2 \pmod 9,$

(G) $a \equiv 0 \pmod 9, \quad b \equiv \pm 3 \pmod 9,$

(H) $a \equiv 0 \pmod 9, \quad b \equiv \pm 4 \pmod 9,$

(I) $a \equiv 0 \pmod{27}, \quad b \equiv \pm 9 \pmod{27}.$

It is clear that cases (A)-(I) are mutually exclusive. Table 1 below shows that they all occur. In Section 2 it is shown that they exhaust all possibilities. From Proposition 1 and (1.2), we obtain

$$\begin{cases} c \equiv 0 \pmod{27}, & \text{in case (A)}, \\ c \equiv \pm 9 \pmod{27}, & \text{in cases (B), (G)}, \\ c \equiv \pm 6 \pmod{27}, & \text{in cases (C), (D), (F)} \\ c \equiv \pm 3 \pmod{27}, & \text{in case (E)}, \\ c \equiv \pm 12 \pmod{27}, & \text{in case (H)}, \\ c \equiv \pm 27 \pmod{81}, & \text{in case (I)}. \end{cases} \tag{1.27}$$

The next proposition is proved in Section 3.

**Proposition 2.**

$$h^2k^4 \equiv \begin{cases} 0 \pmod 9, & \textit{cases } (\mathrm{G}), (\mathrm{I}), \\ 1 \pmod 9, & \textit{cases } (\mathrm{A}), (\mathrm{C}), (\mathrm{E}), \\ 4 \textit{ or } 7 \pmod 9, & \textit{cases } (\mathrm{B}), (\mathrm{D}), (\mathrm{F}), (\mathrm{H}). \end{cases}$$

In cases (A), (C), (E), Proposition 2 shows that we can define $\varepsilon = \pm 1$ by

$$hk^2 \equiv \varepsilon \pmod 9. \tag{1.28}$$

The next proposition is proved in Section 4.

**Proposition 3.** $\ell + \varepsilon km \not\equiv 0 \pmod 3$ *in cases* (C) *and* (E).

From (1.17) and Proposition 3, we see that

$$(3m, \ell + \varepsilon km) = 1 \text{ in cases (C) and (E).} \tag{1.29}$$

Thus we can choose integers $u'$ and $v'$ in cases (C) and (E) such that

$$3mu' + (\ell + \varepsilon km)v' = 1. \tag{1.30}$$

We note that $\ell v' \equiv 1 \pmod m$ so that

$$Ev' - k\ell^2 = \left(k\ell^3 + hm^3\right)v' - k\ell^2 \equiv k\ell^3 v' - k\ell^2 \equiv k\ell^2 - k\ell^2 \equiv 0 \pmod m,$$

showing that

$$\frac{Ev' - k\ell^2}{m} \text{ is an integer in cases (C) and (E).} \tag{1.31}$$

From (1.26) and Proposition 2 we have

**Proposition 4.**

$$d(K) = \begin{cases} -27h^2k^2, & \textit{cases } (B),\ (D),\ (F),\ (G),\ (H),\ (I), \\ -3h^2k^2, & \textit{cases } (A),\ (C),\ (E). \end{cases}$$

The next proposition is proved in Section 5.

**Proposition 5.**

(i) $\dfrac{b+\theta}{3} \in O_K$ *in case* (A).

(ii) $\dfrac{2hk\ell m + \left(hm^2u - k\ell^2 v\right)\theta + \theta^2}{E} \in O_K$ *in all cases.*

(iii) $\dfrac{(kEv' + 2hk\ell m) + \left(\left(Ev' - k\ell^2\right)/m\right)\theta + \theta^2}{3E} \in O_K$, *in cases* (C), (E).

From Propositions 4 and 5 we obtain immediately our main result since $d\left(1, \theta, \theta^2\right) = -4a^3 - 27b^2 = -3c^2 = -3^3h^2k^2E^2$.

**Theorem.** *An integral basis for the pure cubic field K is given by*

$$\left\{1, \frac{b+\theta}{3}, \frac{2hk\ell m + \left(hm^2u - k\ell^2 v\right)\theta + \theta^2}{E}\right\} \quad \textit{in case } (A),$$

$$\left\{1, \theta, \frac{2hk\ell m + \left(hm^2u - k\ell^2 v\right)\theta + \theta^2}{E}\right\} \quad \textit{in cases } (B), (D), (F), (G), (H), (I),$$

$$\left\{1, \theta, \frac{(kEv' + 2hk\ell m) + \left(\left(Ev' - k\ell^2\right)/m\right)\theta + \theta^2}{3E}\right\} \quad \textit{in cases } (C), (E).$$

Table 1 illustrates each of the nine cases (A)–(I)

Table 1 (values of parameters)

| case | $a$ | $b$ | $c$ | $A$ | $C$ | $R$ | $S$ | $h$ | $k$ | $\ell$ | $m$ | $u$ | $v$ | $\varepsilon$ | $u'$ | $v'$ | $E$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| (A) | 51 | 272 | 918 | 17 | 306 | 289 | 17 | 1 | 17 | 1 | 1 | 1 | 0 | | | | 18 |
| (B) | 6 | 2 | 18 | 2 | 6 | 4 | 2 | 1 | 2 | 1 | 1 | 1 | 0 | | | | 3 |
| (C) | 30 | 90 | 330 | 10 | 110 | 100 | 10 | 1 | 10 | 1 | 1 | | | 1 | 4 | −1 | 11 |
| (D) | 30 | 15 | 195 | 10 | 65 | 40 | 25 | 5 | 1 | 2 | 1 | 0 | 1 | | | | 13 |
| (E) | 90 | −170 | 1110 | 30 | 370 | 100 | 270 | 1 | 10 | 1 | 3 | | | 1 | 7 | −2 | 37 |
| (F) | 36 | 92 | 372 | 12 | 124 | 108 | 16 | 1 | 2 | 3 | 2 | 1 | −1 | | | | 62 |
| (G) | 27 | 240 | 738 | 9 | 246 | 243 | 3 | 1 | 3 | 3 | 1 | 0 | 1 | | | | 82 |
| (H) | 36 | 22 | 258 | 12 | 86 | 54 | 32 | 2 | 1 | 3 | 2 | 1 | −1 | | | | 43 |
| (I) | 27 | 72 | 270 | 9 | 90 | 81 | 9 | 3 | 1 | 3 | 1 | 0 | 1 | | | | 30 |

Table 1 (cont'd) (discriminant and integral basis)

| case | $d(K)$ | integral basis |
|---|---|---|
| (A) | $-3\cdot 17^2$ | $1, (272+\theta)/3, (34+\theta+\theta^2)/18$ |
| (B) | $-2^2\cdot 3^3$ | $1, \theta, (4+\theta+\theta^2)/3$ |
| (C) | $-2^2\cdot 3\cdot 5^2$ | $1, \theta, (-90-21\theta+\theta^2)/33$ |
| (D) | $-3^3\cdot 5^2$ | $1, \theta, (20-4\theta+\theta^2)/13$ |
| (E) | $-2^2\cdot 3\cdot 5^2$ | $1, \theta, (-680-28\theta+\theta^2)/111$ |
| (F) | $-2^2\cdot 3^3$ | $1, \theta, (24+22\theta+\theta^2)/62$ |
| (G) | $-3^5$ | $1, \theta, (18-27\theta+\theta^2)/82$ |
| (H) | $-2^2\cdot 3^3$ | $1, \theta, (24+17\theta+\theta^2)/43$ |
| (I) | $-3^5$ | $1, \theta, (18-9\theta+\theta^2)/30$ |

## 2. Proof of Proposition 1

From (1.2) and (1.4) we have

$$4(a/3)^3 + b^2 = C^2 \equiv 0, 1, 4 \text{ or } 7 \pmod 9$$

so that one of the following possibilities must occur :

$$(\alpha) \quad a \equiv 6 \pmod 9,\ b \equiv \pm 2 \pmod 9,$$

$$(\beta) \quad a \equiv 3 \pmod 9,\ b \equiv 0 \pmod 3,$$

$$(\gamma) \quad a \equiv 0 \pmod 9.$$

($\alpha$) comprises cases (A) and (B). ($\beta$) comprises cases (C) and (D). ($\gamma$) comprises cases (E), (F), (G), (H), and

$$a \equiv 0 \pmod 9,\ b \equiv 0 \pmod 9. \tag{2.1}$$

If (2.1) holds, by (1.3), we must have $b \equiv \pm 9 \pmod{27}$. Thus $3 \mid A$, $3^2 \parallel b$. From (1.5) we deduce that $3^2 \mid C$ and $3^2 \mid A$ so that $a \equiv 0 \pmod{27}$. Hence (2.1) is the case (I).

## 3. Proof of Proposition 2

Table 2 follows easily from (1.14)–(1.17) and the fact that $h$ and $k$ are coprime.

Table 2

| $h, k, \ell, m$ | $a, b, c$ | cases |
|---|---|---|
| $3 \mid hk$ | $9 \mid a, 3 \mid b$ | (G) (I) |
| $3 \nmid hk$, $3 \mid \ell m$ | $9 \mid a$, $3 \nmid b$, $3 \parallel c$ | (E) (F) (H) |
| $3 \nmid hk$, $3 \nmid \ell m$ | $3 \parallel a$, $3 \nmid b$, $9 \mid c$<br>or<br>$3 \parallel a$, $3 \mid b$, $3 \parallel c$ | (A) (B)<br><br>(C) (D) |

If $3 \nmid \ell$ then $\ell^6 \equiv 1 \pmod 9$ and $h^2k^4 \equiv h^2k^4\ell^6 = R^2 = \left(\frac{1}{2}(C+b)\right)^2 \pmod 9$.

If $3 \mid \ell$ then $3 \nmid m$ so $m^6 \equiv 1 \pmod 9$ and $h^4k^2 \equiv h^4k^2m^6 = S^2 = \left(\frac{1}{2}(C-b)\right)^2$ $(\bmod 9)$. Then, appealing to Table 2, we obtain

(A) (C): $\quad h^2k^4 \equiv \left(\frac{1}{2}(0 \pm 2)\right)^2 \equiv 1 \pmod 9,$

(B) (D): $\quad h^2k^4 \equiv \left(\frac{1}{2}(\pm 3 \pm 2)\right)^2 \equiv 4 \text{ or } 7 \pmod 9,$

(E) : $\quad (3 \nmid \ell) \quad h^2k^4 \equiv \left(\frac{1}{2}(\pm 1 \pm 1)\right)^2 \equiv 1 \pmod 9,$

$(3 \mid \ell) \quad h^4k^2 \equiv \left(\frac{1}{2}(\pm 1 \mp 1)\right)^2 \equiv 1 \pmod 9$, so $h^2k^4 \equiv 1 \pmod 9$,

(F) : $\quad (3 \nmid \ell) \quad h^2k^4 \equiv \left(\frac{1}{2}(\pm 2 \pm 2)\right)^2 \equiv 4 \pmod 9,$

$(3 \mid \ell) \quad h^4k^2 \equiv \left(\frac{1}{2}(\pm 2 \mp 2)\right)^2 \equiv 4 \pmod 9$, so $h^2k^4 \equiv 7 \pmod 9$,

(H) : $\quad (3 \nmid \ell) \quad h^2k^4 \equiv \left(\frac{1}{2}(\pm 4 \pm 4)\right)^2 \equiv 7 \pmod 9,$

$(3 \mid \ell) \quad h^4k^2 \equiv \left(\frac{1}{2}(\pm 4 \mp 4)\right)^2 \equiv 7 \pmod 9$, so $h^2k^4 \equiv 4 \pmod 9$,

(G) (I): $\quad h^2k^4 \equiv 0 \pmod 9,$

which completes the proof of Proposition 2.

## 4. Proof of Proposition 3

In case (C) we have

$$A \equiv 1 \pmod 3, \quad b \equiv 0 \pmod 9, \quad C \equiv 2\delta \pmod 9,$$

where $\delta = \pm 1$. Then, from (1.14), (1.15), (1.16), we obtain

$$hk\ell m \equiv 1 \pmod{3}, \quad hk^2\ell^3 \equiv \delta \pmod{9}, \quad h^2km^3 \equiv \delta \pmod{9}.$$

As $hk^2 \equiv \varepsilon \pmod{9}$, where $\varepsilon = \pm 1$, we have $h \equiv \varepsilon \pmod{3}$ so that $\ell \equiv \varepsilon\delta \pmod{3}$, $km \equiv \delta \pmod{3}$, and $\ell + \varepsilon km \equiv \varepsilon\delta + \varepsilon\delta = 2\varepsilon\delta \not\equiv 0 \pmod{3}$.

In case (E) we have $3 \nmid hk, 3 \mid \ell m$ (Table 2). If $3 \mid \ell$ then $3 \nmid m$ so $\ell + \varepsilon km \equiv \varepsilon km \not\equiv 0 \pmod{3}$. If $3 \mid m$ then $3 \nmid \ell$ so $\ell + \varepsilon km \equiv \ell \not\equiv 0 \pmod{3}$.

## 5. Proof of Proposition 5

(i) In case (A) we have $a \equiv 6 \pmod{9}$, $b \equiv \pm 2 \pmod{9}$, $b^2 \equiv a+1 \pmod{27}$, so

$$a + 3b^2 \equiv 6 + 3(4) \equiv 0 \pmod{9}$$

and

$$1 - a - b^2 \equiv 0 \pmod{27}$$

showing that $\left(a + 3b^2\right)/9$ and $\left(b - ab - b^3\right)/27$ are integers. Now $\phi = (b + \theta)/3 \ (\in K)$ satisfies the monic cubic equation

$$\phi^3 - b\phi^2 + \frac{\left(a + 3b^2\right)}{9}\phi + \frac{\left(b - ab - b^3\right)}{27} = 0,$$

so that $\phi$ is an algebraic integer, and hence $\phi \in O_K$.

(ii) Appealing to (1.18), (1.21) and (1.22) we have

$$\frac{2hk\ell m + \left(hm^2u - k\ell^2v\right)\theta + \theta^2}{E} = v\phi_1 + u\phi_2 \in O_K.$$

(iii) In cases (C) and (E) we have $hk^2 \equiv \varepsilon \pmod 9$ $(\varepsilon = \pm 1)$ and we consider $\alpha = \left(k + \varepsilon k\phi_1 + \phi_2\right)/3 \in K$. Making use of (1.23) and (1.24), we find that $\alpha$ satisfies the monic cubic equation

$$\alpha^3 - k\alpha^2 + \frac{k^2(1-\varepsilon h)}{3}\alpha - \frac{k\left(h^2 + k^2 + \varepsilon hk^4 - 3\varepsilon hk^2\right)}{27} = 0.$$

As $h \equiv \varepsilon \pmod 3$, $(1-\varepsilon h)/3$ is an integer. We show next that $\left(h^2 + k^2 + \varepsilon hk^4 - 3\varepsilon hk^2\right)/27$ is also an integer. Clearly $3 \nmid k$ so $k^2 \equiv 1, 4, 7 \pmod 9$. Set $k^2 = r + 9s$, where $r = 1, 4, 7$ and $s$ is an integer. Then $h \equiv hr^3 \equiv hk^2r^2 \equiv \varepsilon r^2 \pmod 9$, so $h = \varepsilon r^2 + 9t$ for some integer $t$. Hence

$$h^2 \equiv r^4 + 18\varepsilon r^2 t \pmod{27},$$

$$k^4 \equiv r^2 + 18rs \pmod{27},$$

$$hk^4 \equiv \varepsilon r^4 + 9r^2 t + 18\varepsilon r^3 s \pmod{27}.$$

Then, as $r \equiv 1 \pmod 3$, $r^2 \equiv 2r - 1 \pmod 9$, and $r^3 \equiv 3r - 2 \pmod{27}$, we have

$$\begin{aligned} & h^2 + k^2 + \varepsilon hk^4 - 3\varepsilon hk^2 \\ \equiv & \left(r^4 + 18\varepsilon r^2 t\right) + (r + 9s) + \left(r^4 + 9\varepsilon r^2 t + 18r^3 s\right) - 3 \\ \equiv & \ 2r^4 + r - 3 \equiv 6r^2 - 3r - 3 \equiv 9r - 9 \\ \equiv & \ 0 \pmod{27}. \end{aligned}$$

We have now shown that $\alpha \in O_K$. Finally, appealing to (1.19), (1.21), (1.22) and (1.30), we obtain

$$\frac{(kEv' + 2hk\ell m) + \left(\left(Ev' - k\ell^2\right)/m\right)\theta + \theta^2}{3E} = v'\alpha + u'\phi_1 \in O_K.$$

## 6. Concluding Remarks

The discriminant of an arbitrary cubic field has been given by Llorente and Nart [3] and an integral basis by Alaca [1]. From [3 : Theorem 2] in the case of a pure cubic field $K$ given by (1.1), we have

$$d(K) = -3^{\beta} \prod_{\substack{p \neq 3 \\ 1 \leq v_p(b) \leq v_p(a)}} p^2, \tag{6.1}$$

where

$$\beta = \begin{cases} 1, & \text{cases (A), (C), (E),} \\ 3, & \text{cases (B), (D), (F), (H),} \\ 5, & \text{cases (G), (I).} \end{cases} \tag{6.2}$$

Combining (6.1) with Proposition 4, we see that

$$hk = 3^{\gamma} \prod_{\substack{p \neq 3 \\ 1 \leq v_p(b) \leq v_p(a)}} p, \tag{6.3}$$

where

$$\gamma = \begin{cases} 0, & \text{cases (A), (B), (C), (D), (E), (F), (H),} \\ 1, & \text{cases (G), (I).} \end{cases} \tag{6.4}$$

We leave it to the reader to deduce (6.3) arithmetically from the properties of $a$, $b$, $h$, $k$ given in Section 1.

### Acknowledgment

The second author acknowledges the hospitality of Okanagan University College, Kelowna, BC, Canada and Macquarie University, Sydney, Australia, where this paper was completed.

## References

[1] S. Alaca, $p$-integral bases of algebraic number fields, Ph. D. Thesis, Carleton University, Ottawa, Ontario, Canada, 1994.

[2] H. Cohen, A Course in Computational Algebraic Number Theory, Springer-Verlag, Berlin Heidelberg, 1993.

[3] P. Llorente and E. Nart, Effective determination of the decomposition of the rational primes in a cubic field, Proc. Amer. Math. Soc. 87 (1983), 579-585.

Department of Mathematics and Statistics
Okanagan University College
Kelowna, B. C. V1V 1V7
Canada
e-mail : bkspearm@okanagan.bc.ca

Department of Mathematics and Statistics
Carleton University
Ottawa, Ontario K1S 5B6
Canada
e-mail : williams@math.carleton.ca