J. Austral. Math. Soc. (*Series A*) 38 (1985), 351–371

INTEGRAL BASES OF DIHEDRAL NUMBERFIELDS. I

WALTER LEDERMANN and CAROL VAN DER PLOEG

(Received 2 December 1982; revised 25 July 1983)

Communicated by J. Loxton

Abstract

A dihedral number field is a non-normal quartic field K which possesses a quadratic subfield k. That is, $K = k(\sqrt{\alpha})$ for some integer α of k. Integral bases of these fields were known by Sommer (1907), but the form in which they were known was of little use for computational purposes. In this paper we construct integral bases of those dihedral fields with quadratic subfield of the form $Q(\sqrt{d})$, $d \not\equiv 1 \pmod 8$, for which only rational quantities need be determined. Although the general theory may easily be generalized to the case $d \equiv 1 \pmod 8$, the actual determination of integral bases in this case is left to a later paper.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*): 12 A 30.

1. Introduction

A dihedral number field K is a non-normal quartic extension of Q which possesses a quadratic subfield k. That is, $K = k(\sqrt{\alpha})$ for some integer α of k. Integral bases of these fields have been known for some time, indeed the following result is quoted by Sommer (1907):

"Let

$$(2) = \mathfrak{l}_1^{l_1}\mathfrak{l}_2^{l_2},$$

where one of the factors may be absent and l_1, l_2 are non-negative integers such that $0 < l_1 + l_2 \leqslant 2$ and

$$(\alpha) = \mathfrak{l}_1^{a_1}\mathfrak{l}_2^{a_2}\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_r^{e_r}$$

be prime decompositions of (2) and (α) in k. For $n \in Z$ denote by n' the greatest integer $\leqslant n/2$ and let g_1 and g_2 be the greatest rational integers for which the congruence

$$\alpha \equiv \nu^2 \left(\text{mod } \lambda_1^{2(g_1+a_1')}\lambda_2^{2(g_2+a_2')}\right)$$

is solvable for some integer ν of k. Let $\mathbf{b} = (\beta_1, \beta_2)$ be relatively prime to λ_1 and λ_2 in k and such that

$$\lambda_1^{g_1+a_1'}\lambda_2^{g_2+a_2'}\mathfrak{p}_1^{e_1'} \cdots \mathfrak{p}_r^{e_r'}\mathbf{b} = (\gamma)$$

is a principal ideal. Finally, let ν be chosen so that

$$(\nu) = \mathfrak{p}_1^{e_1'} \cdots \mathfrak{p}_r^{e_r'}\mathfrak{n}.$$

Then $\Omega_1 = \beta_1((\nu + \sqrt{\alpha})/\gamma)$ and $\Omega_2 = \beta_2((\nu + \sqrt{\alpha})/\gamma)$ are integers of K and, if $[1, \omega]$ is an integral basis of k, the four integers $[1, \omega, \Omega_1, \Omega_2]$ form an integral basis of K."

In this paper we construct integral bases of dihedral number fields with quadratic subfields $Q(\sqrt{d})$, where d is a square-free positive (rational) integer such that $d \not\equiv 1 \pmod 8$. Our method will be elementary in the following sense: if $[1, \omega]$ is an integral basis for $k = Q(\sqrt{d})$, then the dihedral number field can be written $K = k(\sqrt{\alpha})$, where $\alpha = A + B\omega$ with suitable rational integers A, B. It is our object to express the integral basis of K in rational terms, involving arithmetic properties of A, B, and d, and without recourse to p-adic arguments.

W. E. H. Berwick (1927) has devoted a monograph to the construction of integral bases. His introductory chapters bear some resemblance to our treatment, but the bulk of his applications refer to number fields of a different kind. In our theoretical approach we follow more closely Mann (1955). It goes without saying that all writers on this topic are decisively influenced by the monumental work of Hilbert (1897).

2. Definitions and notation

We employ the standard notations $n(\ )$, $\mathrm{tr}(\ )$ for the absolute norm and trace of an integer or ideal and $n_k(\ )$, $\mathrm{tr}_k(\ )$ for the relative norm and trace over k. I_K and I_k denote the rings of integers of K and k respectively. For a rational prime p and integer n, $p^e \| n$ means that $n \equiv 0 \pmod{p^e}$ but $n \not\equiv 0 \pmod{p^{e+1}}$. For n-tuples of rational integers $(r_1, \ldots, r_n)$, $(s_1, \ldots, s_n)$ the notation $[r_1, \ldots, r_n] \equiv [s_1, \ldots, s_n] \pmod m$ means that $r_i \equiv s_i \pmod m$ for $i = 1, \ldots, n$. This should not be confused with the highest common factor such as (A, B) below.

Let $[1, \omega]$ be an integral basis for $k = Q(\sqrt{d})$, so that

$$\omega = \begin{cases} \sqrt{d} & \text{if } d = 2, 3 \pmod 4, \\ (1 + \sqrt{d})/2 & \text{if } d = 1 \pmod 4, \end{cases}$$

and let $K = k(\sqrt{\alpha})$ where $\alpha = A + B\omega$, $A, B \in Z$.

https://doi.org/10.1017/S1446788700023648 Published online by Cambridge University Press

It is easily shown that we may assume, without loss of generality, that the highest common factor (A, B) is square-free and that $B > 0$. The validity of the first assumption is seen immediately; for if $\alpha = m^2\beta$ where $m \in Z$ and $\beta \in I_k$ has no squared rational divisors, then $K = k(\sqrt{\beta})$ and so we may assume from the outset that α has no squared divisors. For the second assumption, consider the conjugate $\bar{\omega}$ of ω in k. We shall use the notation

$$D = -\omega\bar{\omega} = \begin{cases} d & \text{if } d = 2,3 \pmod 4, \\ (d-1)/4 & \text{if } d = 1 \pmod 4, \end{cases} \tag{2.1}$$

$$E = \omega + \bar{\omega} = \begin{cases} 0 & \text{if } d = 2,3 \pmod 4, \\ 1 & \text{if } d = 1 \pmod 4 \end{cases} \tag{2.2}$$

so that if $\alpha = A + B\omega$ where $B < 0$ then $\alpha = (A + EB) - B\bar{\omega}$ and the coefficient of $\bar{\omega}$ is positive. Thus we may choose our notation for ω and $\bar{\omega}$ so that $B > 0$.

Suppose that (α) has prime decomposition

$$(\alpha) = \lambda_1^{2a_1+\varepsilon_1}\lambda_2^{2a_2+\varepsilon_2}\pi_1^{2e_1+\vartheta_1} \cdots \pi_f^{2e_f+\vartheta_f}\mathbf{Q}$$

in k, where $\lambda_i | (2)$, the π_i are distinct prime ideals of degree one, $\mathbf{Q}$ is a product of primes of degree two and ε_i, $\vartheta_i = 0$ or 1. Since (A, B) is square-free note that if $e_i > 0$ then either $\pi_i^{2e_i} | (\alpha)$ or $\bar{\pi}_i^{2e_i} | (\alpha)$, where the bar denotes conjugation in k. We choose our notation for π_i and $\bar{\pi}_i$ so that $\pi_i^{2e_i} | (\alpha)$. If $\pi_i = \bar{\pi}_i$ then $e_i = 1$. Let $n(\pi_i) = p_i$ where $(d/p_i) \neq -1$ and put $C = \prod_{i=1}^{f} p_i^{e_i}$.

3. Minimal integers

We employ a general method for constructing integral bases of algebraic numberfields based on a construction of Hilbert (1897); let $Q(\vartheta)$ be an arbitrary numberfield of degree n. Then any integer β of $Q(\vartheta)$ may be written in the form

$$\beta = \frac{c_0 + c_1\vartheta + c_2\vartheta^2 + \cdots + c_i\vartheta^i}{t}$$

where $c_0, c_1, \ldots, c_i$, $t \in Z$, $t > 0$ and $0 \leqslant i \leqslant n-1$. If $c_i \neq 0$ then β is called an integer of degree i in ϑ and a minimal integer of degree i in ϑ is one which, of all integers of degree i in ϑ, has least coefficient of ϑ^i in absolute value. It can be shown that every minimal integer of degree i in ϑ may be written in the form

$$\beta_i = \frac{c_0 + c_1\vartheta + c_2\vartheta^2 + \cdots + \vartheta^i}{t_i}$$

where $c_0, c_1, \ldots, c_{i-1}$, $t_i \in Z$ and $t_i > 0$ and that any set $[\beta_1, \beta_2, \ldots, \beta_{n-1}]$ forms an integral basis for $Q(\vartheta)$: see Mann (1955). We therefore seek minimal integers

of degrees one, two and three and in $\sqrt{\alpha}$ and for this the following observation is of fundamental importance:

If $\beta \in K$ then $\beta \in I_K$ if and only if $n_k(\beta)$, $\mathrm{tr}_k(\beta) \in I_k$.

4. Minimal integers of degree one

We seek the largest positive $t \in Z$ for which $\beta = (c_0 + \sqrt{\alpha})/t$ is an integer for some $c_0 \in Z$. Since $\mathrm{tr}_k(\beta) = 2c_0/t$ and

$$n_k(\beta) = \left(c_0^2 - \alpha\right)/t^2 = \left(c_0^2 - A\right)/t^2 - \left(B/t^2\right)\omega,$$

β is an integer if and only if the following congruences are solvable:

$$2c_0 \equiv 0 \pmod{t}, \tag{4.1}$$

$$A \equiv c_0^2 \pmod{t^2}, \tag{4.2}$$

$$B \equiv 0 \pmod{t^2}. \tag{4.3}$$

Let t_1 be the largest positive value of t for which (4.1)–(4.3) are solvable and denote by β_1 the corresponding minimal integer. If $t_1 \equiv 0 \pmod{p}$ for some odd prime p then by (4.1) $c_0 \equiv 0 \pmod{p}$ and so $A \equiv B \equiv 0 \pmod{p^2}$ by (4.2) and (4.3). This is impossible since (A, B) is square-free and so $t_1 = 2^x$. Clearly $x \leqslant 1$, for otherwise $(A, B) \equiv 0 \pmod 4$. Suppose $x = 1$: Since $(A, B) \not\equiv 0 \pmod 4$ c_0 must be odd and (4.1)–(4.3) are solvable provided that $[A, B] \equiv [1, 0] \pmod 4$. Thus we have

LEMMA 1. *A minimal integer of degree one in $\sqrt{\alpha}$ is given by*

$$\beta_1 = \begin{cases} (1 + \sqrt{\alpha})/2 & \text{if } [A, B] \equiv [1, 0] \pmod 4, \\ \sqrt{\alpha} & \text{otherwise.} \end{cases}$$

5. Minimal integers of degree two

The following result provides a lower bound for the denominator of a minimal integer:

LEMMA 2. *Let $\beta_i = (c_0 + c_1\vartheta + \cdots + c_{i-1}\vartheta^{i-1} + \vartheta^i)/t_i$ be a minimal integer. If $\gamma = (d_0 + d_1\vartheta + \cdots + d_{i-1}\vartheta^{i-1} + \vartheta^i)/t$ is an integer, where $d_0, d_1, \ldots, d_{i-1}$, $t \in Z$ and $t > 0$ then $t_i \equiv 0 \pmod{t}$.*

https://doi.org/10.1017/S1446788700023648 Published online by Cambridge University Press

PROOF. Let $m = \text{l.c.m.}(t, t_i)$ and put $m = st = rt_i$ where $(r, s) = 1$. Let u, $v \in Z$ be such that $ur + vs = 1$. Then

$$u\beta_i + v\gamma = \left(e_0 + e_1\vartheta + \cdots + e_{i-1}\vartheta^{i-1} + \vartheta^i\right)/m$$

is an integer. Since β_i is minimal $t_i \geqslant m$, so we must have $r = 1$ and $t_i = st$.

Since $\omega = (-A + \alpha)/B$ is an integer of degree two in $\sqrt{\alpha}$, Lemma 1 shows that every minimal integer of degree two in $\sqrt{\alpha}$ takes the form

$$\beta = \left(c_0 + c_1\sqrt{\alpha} + \alpha\right)/nB$$

for some positive integer n. Since

$$\mathrm{tr}_k(\beta) = 2(c_0 + A)/nB + (2/n)\omega$$

and $n_k(\beta) = ((c_0 + A)^2 - c_1^2A + DB^2)/n^2B^2 + [(2(c_0 + A) - c_1^2 + EB)/n^2B]\omega$ the number β is an integer if and only if the following four congruences are solvable for some $c_0, c_1, n \in Z$:

$$2 \equiv 0 \pmod{n}, \tag{5.1}$$

$$2(c_0 + A) \equiv 0 \pmod{nB}, \tag{5.2}$$

$$2(c_0 + A) - c_1^2 + EB \equiv 0 \pmod{n^2B}, \tag{5.3}$$

$$(c_0 + A)^2 - c_1^2A + DB^2 \equiv 0 \pmod{n^2B^2}. \tag{5.4}$$

We seek the largest positive value of n for which the congruences (5.1) and (5.4) are solvable. By (5.1) $n = 1$ or 2. Suppose $n = 2$. By (5.2) $c_0 + A \equiv 0 \pmod{B}$ and (5.3) and (5.4) yield $c_1^2 \equiv 0 \pmod{B}$ and $c_1^2A \equiv 0 \pmod{B^2}$. Putting $c_1^2 = lB$ gives $lA \equiv 0 \pmod{B}$. Let $m = (A, B)$ and put $A = mA_1$, $B = mB_1$ where $(A_1, B_1) = 1$. Then $lA_1 \equiv 0 \pmod{B_1}$ and so $l \equiv 0 \pmod{B_1}$, say $l = l_1B_1$. Thus $c_1^2 = l_1mB_1^2$ and this implies that $l_1 \equiv 0 \pmod{m}$ because m is square-free. Hence $c_1 \equiv 0 \pmod{B}$. Now putting $c_0 + A = xB$ and $c_1 = yB$ in (5.3) and (5.4) yields

$$2x - y^2B + E \equiv 0 \pmod{4}, \tag{5.5}$$

$$x^2 - y^2A + D \equiv 0 \pmod{4}. \tag{5.6}$$

We seek conditions on A and B for (5.5) and (5.6) to be solvable. Note that they are not solvable for even y; for if y is even they become

$$E \equiv 2x \pmod{4}, \qquad D \equiv -x^2 \pmod{4}$$

but when $d \equiv 1 \pmod{4}$ then $E = 1$ and the first is not satisfied and when $d \not\equiv 1 \pmod{4}$ then $E = 0$ so that x must be even and the second is not satisfied. Thus y is odd and (5.5) and (5.6) are solvable provided that

$$[A, B] = [D + x^2, E + 2x] \pmod{4}.$$

Conversely if A, B satisfy the above then

$$\beta = \left((-A + xB) + yB\sqrt{\alpha} + \alpha\right)/2B$$

https://doi.org/10.1017/S1446788700023648 Published online by Cambridge University Press

is an integer. Note that x and y need only be determined modulo 2; for if $x = x_0 + 2X$ and $y = y_0 + 2Y$ where $x_0 = 1$ or 0 and $y_0 = 1$, then

$$\beta = \big((-A + x_0B) + y_0B\sqrt{\alpha} + \alpha\big)/2B + (X + Y\sqrt{\alpha}).$$

But $X + Y\sqrt{\alpha} \in I_K$ and so we may assume that $x = 1$ or 0 and $y = 1$, without loss of generality. Thus if $[A, B] \equiv [D, E] \pmod 4$ then (5.1)–(5.4) are solvable for $n = 2$, $c_0 = -A$, $c_1 = B$ and so $(-A + B\sqrt{\alpha} + \alpha)/2B = (\omega + \sqrt{\alpha})/2$ is a minimal integer of degree two in $\sqrt{\alpha}$; and if $[A, B] \equiv [D + 1, E + 2] \pmod 4$ then (5.1)–(5.4) are solvable for $n = 2$, $c_0 = B - A$, $c_1 = B$ and so

$$\big((B - A) + B\sqrt{\alpha} + \alpha\big)/2B = (1 + \omega + \sqrt{\alpha})/2$$

is a minimal integer of degree two in $\sqrt{\alpha}$. Finally, if $[A, B] \not\equiv [D, E]$ or $[D + 1, E + 2] \pmod 4$ then (5.1)–(5.4) are not solvable for $n = 2$, but are clearly solvable for $n = 1$ because $\omega = (-A + \alpha)/B$ is an integer, which is minimal in this case. We summarize our results in the following:

LEMMA 3. *A minimal integer of degree two in $\sqrt{\alpha}$ is given by*

$$\beta_2 = \begin{cases} (\omega + \sqrt{\alpha})/2 & \text{if } [A, B] \equiv [D, E] \pmod 4, \\ (1 + \omega + \sqrt{\alpha})/2 & \text{if } [A, B] \equiv [D + 1, E + 2] \pmod 4, \\ \omega & \text{otherwise.} \end{cases}$$

6. Minimal integers of degree three

We use Lemma 2 to obtain a lower bound for the denominator of a minimal integer of degree three, using the following result:

THEOREM 1. (i) *There exist rational integers r, s, u, v such that*

$$A + rB = sC, \tag{6.1}$$

$$D - r(r - E) = uC, \tag{6.2}$$

$$(2r - E)s + uB = vC. \tag{6.3}$$

(ii) *The number $\eta = (-A + (r - E)B + \alpha)\sqrt{\alpha}/BC$ is an integer of K.*

PROOF. (i) Let $p^e \| C$ where $e > 0$. If $d \equiv 0 \pmod p$ then $e = 1$ and so we may put

$$d \equiv \begin{cases} r_p^2 \pmod{p^e} & \text{if } d \not\equiv 1 \pmod 4, \\ (2r_p - 1)^2 \pmod{4p^e} & \text{if } d \equiv 1 \pmod 4 \end{cases} \tag{6.4}$$

https://doi.org/10.1017/S1446788700023648 Published online by Cambridge University Press

for some $r_p \in Z$. (Clearly $r_p \equiv 0 \pmod p$ when $d \not\equiv 1 \pmod 4$ and $2r_p - 1 \equiv 0 \pmod p$ when $d \equiv 1 \pmod 4$.) Since in this case $p|(\alpha)$ we have $(A, B) \equiv 0 \pmod p$ and so we may straight away put

$$A + r_p B \equiv 0 \pmod{p^e}. \tag{6.5}$$

We show that (6.4) and (6.5) hold for some r_p also when $d \not\equiv 0 \pmod p$. So henceforth suppose that $d \not\equiv 0 \pmod p$. Then d is a quadratic residue modulo every power of p and so (6.4) is immediate. Substituting for d in (6.4) using (2.1) and (2.2) yields

$$D \equiv r_p(r_p - E) \pmod{p^e}. \tag{6.6}$$

Now let $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ in k, where the notation for $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ is chosen so that $\mathfrak{p}^{2e}|(\alpha)$. Factorizing (6.6) in k gives

$$(r_p - \omega)(r_p - \bar{\omega}) \equiv 0 \pmod{\mathfrak{p}^e\bar{\mathfrak{p}}^e}$$

and so either $r_p - \omega \equiv 0 \pmod{\mathfrak{p}^e}$ or $r_p - \bar{\omega} \equiv 0 \pmod{\mathfrak{p}^e}$, since neither factor has a rational divisor. But $r_p - \omega \equiv 0 \pmod{\mathfrak{p}^e}$ if and only if $(E - r_p) - \bar{\omega} \equiv 0 \pmod{\mathfrak{p}^e}$. Moreover r_p satisfies (6.6) if and only if $(E - r_p)$ does, and $r_p \not\equiv (E - r_p) \pmod p$ so we may choose our notation for r_p and $(E - r_p)$ so that

$$r_p \equiv \omega \pmod{\mathfrak{p}^e} \tag{6.7}$$

without loss of generality. We now consider two separate cases:

(a) $(A, B) \not\equiv 0 \pmod p$:

Since $A + B\omega = 0 \pmod{\mathfrak{p}^{2e}}$, (6.7) yields $A + r_p B \equiv 0 \pmod{\mathfrak{p}^e}$. But $A + r_p B \in Z$ and so (6.5) holds.

(b) $(A, B) \equiv 0 \pmod p$:

Put $A = A_1 p$ and $B = B_1 p$ where $(A_1, B_1) \not\equiv 0 \pmod p$ because (A, B) is square-free. Then $A_1 + B_1\omega \equiv 0 \pmod{\mathfrak{p}^{2e-1}}$ and, since $2e - 1 \geqslant e$, (6.7) yields $A_1 + r_p B_1 \equiv 0 \pmod{\mathfrak{p}^e}$. But $A_1 + r_p B_1 \in Z$ and so $A_1 + r_p B_1 \equiv 0 \pmod{p^e}$. Thus

$$A + r_p B \equiv 0 \pmod{p^{e+1}} \tag{6.8}$$

and (6.5) follows a fortiori.

Now for a prime $p_j|C$ let $N_{p_j} = \prod_{i=1;(i\neq j)}^{f} p_i^{e_i+1}$. Since $(N_{p_j}, p_j) = 1$ there exists a rational integer N'_{p_j} such that $N_{p_j} N'_{p_j} \equiv 1 \pmod{p_j^{e_j+1}}$. If we now put

$$r = \sum_{p|C} r_p N_p N'_p$$

then

$$r \equiv r_p \pmod{p^{e+1}} \tag{6.9}$$

and (6.5) yields $A + rB \equiv 0 \pmod{p^e}$. This holds for all primes p such that $p^e \| C$ and so we have proved (6.1). Similarly (6.2) follows from (6.6).

To prove (6.3) note that

$$n(\alpha) = A^2 + EAB - DB^2 \tag{6.10}$$
$$= (A - rB)(A + rB) + EB(A + rB) - uB^2C$$

by (6.2), so by (6.1)

$$n(\alpha) = s^2C^2 - ((2r - E)s + uB)BC. \tag{6.11}$$

If $d \equiv 0 \pmod{p}$ then $B \equiv 2r - E \equiv 0 \pmod{p}$ and since $e = 1$ we may put

$$(2r - E)s + uB \equiv 0 \pmod{p^e}. \tag{6.12}$$

If $d \not\equiv 0 \pmod{p}$ we consider cases (a) and (b) above separately:

(a) $(A, B) \not\equiv 0 \pmod{p}$:

By (6.1) $p \nmid B$ and so $p^e \| BC$. But by definition of C we have

$$n(\alpha) \equiv C^2 \equiv 0 \pmod{p^e}$$

and so by (6.11), (6.12) holds.

(b) $(A, B) \equiv 0 \pmod{p}$:

By (6.8) and the fact that (A, B) is square-free we have $p \| B$, and so $p^{e+1} \| BC$. Further, by (6.8) and (6.9), $A + rB \equiv 0 \pmod{p^{e+1}}$ and so (6.1) yields $s \equiv 0 \pmod{p}$. Thus in this case

$$n(\alpha) \equiv s^2C^2 \equiv 0 \pmod{p^{2e+1}}$$

and so by (6.11), (6.12) holds.

Thus (6.12) holds for all primes p such that $p^e \| C$ and this proves (6.3). Notice that (6.3) and (6.11) yield the useful identity

$$n(\alpha) = (s^2 - vB)C^2. \tag{6.13}$$

(ii) We show that $n_k(\eta)$ and $\mathrm{tr}_k(\eta)$ are integers of k: since $\alpha = A + B\omega$ we may write $\eta = (\omega + r - E)\sqrt{\alpha}/C$ from which it follows that $\mathrm{tr}_k(\eta) = 0$. A short calculation using (6.1)–(6.3) yields

$$n_k(\eta) = -(us + (r - E)v + v\omega) \tag{6.14}$$

and clearly $n_k(\eta) \in I_k$.

We use the integer η of this theorem to provide a lower bound for the denominator of a minimal integer of degree three in $\sqrt{\alpha}$, that is, an integer of the form $\beta = (c_0 + c_1\sqrt{\alpha} + c_2\alpha + \alpha\sqrt{\alpha})/t$ where c_0, c_1, c_2 and $t \in Z$ and $t > 0$ is maximal. In the usual manner, computation of the relative norm and trace yields four congruences, the simultaneous solvability of which is a necessary and sufficient condition for the number β to be integral:

$$2Bc_2 \equiv 0 \pmod{t}, \tag{6.15}$$

$$2(c_0 + Ac_2) \equiv 0 \pmod{t}, \tag{6.16}$$

https://doi.org/10.1017/S1446788700023648 Published online by Cambridge University Press

$$(6.17) \qquad (c_0 + Ac_2)^2 - A(c_1 + A)^2 - B^2DF \equiv 0 \pmod{t^2},$$

$$(6.18) \qquad B(2c_2(c_0 + Ac_2) - (3A + c_1)(A + c_1) - B(EF + BD)) \equiv 0 \pmod{t^2}$$

where $F = 3A + EB + 2c_1 - c_2^2$.

In the consideration of the solution of these congruences we make use of the following result:

LEMMA 4. *If $a, b, c \in Z$ and (a, b) is square-free, and if*

$$(c - b)^2 b \equiv 0 \pmod{a^2} \quad \textit{and} \quad (c - b)(c - 3b) \equiv 0 \pmod{a},$$

then $c \equiv b \pmod{a}$.

PROOF. Let $(a, b) = m$ so that $a = ma_1$ and $b = mb_1$ where $(a_1, b_1) = 1$. Our first supposition becomes $(c - b)^2 b_1 \equiv 0 \pmod{a_1^2}$, which yields $c \equiv b \pmod{a_1}$. Putting $c - b = l_1 a_1$ yields $l_1^2 b_1 \equiv 0 \pmod{m}$, but $l_1^2 a_1 \equiv 0 \pmod{m}$ by our second assumption. Since m is square-free and $(a_1, b_1) = 1$ we must have $l_1 \equiv 0 \pmod{m}$. Putting $l_1 = ml$ gives $c = b + la$ as required.

THEOREM 2. *Every minimal integer of degree three in $\sqrt{\alpha}$ has denominator $2^a BC$ where a is a non-negative rational integer.*

PROOF. Applying Lemma 2 to η shows that the denominator of such an integer is of the form nBC where n is a non-negative rational integer. Suppose there exists an odd prime q for which $n \equiv 0 \pmod{q}$. Then there exist $c_0, c_1, c_2 \in Z$ which satisfy (6.15)–(6.18) with $t = qBC$ (and so also with $t = B$ and $t = BC$). We consider two separate cases according to the parity of B:

(a) B odd: Considering (6.16)–(6.18) with $t = B$ yields

$$A(c_1 + A)^2 \equiv 0 \pmod{B^2} \quad \text{and} \quad (3A + c_1)(A + c_1) \equiv 0 \pmod{B}$$

and so $c_1 \equiv -A \pmod{B}$ by Lemma 4. Put

$$(6.19) \qquad c_1 = lB - A,$$

Considering (6.15)–(6.18) with $t = qBC$, we first note that

$$c_2 \equiv 0 \pmod{qC}$$

by (6.15) and so $F \equiv A + (2l + E)B \pmod{q^2C^2}$, and that

$$c_0 + Ac_2 \equiv 0 \pmod{qBC}$$

by (6.16). Thus (6.17) and (6.18) become

$$(6.20) \qquad A(l^2 + D) + BD(2l + E) \equiv 0 \pmod{q^2C^2},$$

$$(6.21) \qquad A(2l + E) + B\big(D + (l + E)^2\big) \equiv 0 \pmod{q^2C^2}.$$

https://doi.org/10.1017/S1446788700023648 Published online by Cambridge University Press

(b) even: Considering (6.16)–(6.18) with $t = B = 2B_0$ and using Lemma 4 yields $c_1 \equiv -A \pmod{B_0}$ and so we may put

$$c_1 = l_0 B_0 - A.$$

Considering (6.15)–(6.18) with $t = qBC$, we first note that

$$c_2 \equiv 0 \pmod{qC}$$

as before, so $F \equiv A + (l_0 + E)B \pmod{q^2C^2}$, and that

$$c_0 + Ac_2 \equiv 0 \pmod{qB_0C_0}$$

by (6.16). Now (6.17) and (6.18) become

$$A\left(l_0^2 + 4D\right) + 8B_0D(l_0 + E) \equiv 0 \pmod{q^2C^2},$$
$$2A(l_0 + E) + B_0\left(4D + (l_0 + 2E)^2\right) \equiv 0 \pmod{q^2C^2}.$$

Now define the rational integer $2'$ such that $22' \equiv 1 \pmod{q^2C^2}$ and put $l = 2'l_0$. Then the above congruences are transformed into (6.20) and (6.21) respectively when the first is multiplied by $(2')^2$ and the second by $2'$. We therefore proceed from (6.20) and (6.21) in the general case.

Addition of suitable multiples of these yields

$$A\left(l(l + E) - D\right)^2 \equiv 0 \pmod{q^2C^2},$$
$$B\left(l(l + E) - D\right)^2 \equiv 0 \pmod{q^2C^2}$$

and so $D \equiv l(l + E) \pmod{qC}$ because (A, B) is square-free. Putting $D = l(l + E) + wqC$ in (6.20) and (6.21) gives

$$(6.22)\quad (2l + E)(A + (l + E)B) + (A + (2l + E)B)wqC \equiv 0 \pmod{q^2C^2},$$

$$(6.23)\qquad (2l + E)(A + (l + E)B) + BwqC \equiv 0 \pmod{q^2C^2}.$$

We show that there exists no odd prime q for which (6.22) and (6.23) are solvable. Since

$$(6.24)\qquad d = \begin{cases} D = l^2 + wqC & \text{if } d \not\equiv 1 \pmod 4, \\ 4D + 1 = (2l + 1)^2 + 4wqC & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

either $d \equiv 0 \pmod q$ or $(d/q) = 1$; we consider these two cases separately.

(i) $d \equiv 0 \pmod q$. Putting (6.23) in (6.22) gives $(A + (l + E)B)w \equiv 0 \pmod q$, that is

$$(6.25)\qquad A + (l + E)B \equiv 0 \pmod q$$

because $w \not\equiv 0 \pmod q$ as d is square-free. But $2l + E \equiv 0 \pmod q$ by assumption and so (6.23) yields $B \equiv 0 \pmod q$. Thus by (6.25) $(A, B) \equiv 0 \pmod q$, that is, $q \mid (\alpha)$. Hence $\pi^2 \mid (\alpha)$ where $(q) = \pi^2$ and so $C \equiv 0 \pmod q$, which is impossible since d is square-free.

https://doi.org/10.1017/S1446788700023648 Published online by Cambridge University Press

(ii) $(d/q) = 1$. Putting $D = l(l + E) + wqC$ in (6.10) gives

$$n(\alpha) = (A - lB)(A + (l + E)B) - B^2wqC. \tag{6.26}$$

Since now $2l + E \not\equiv 0 \pmod q$, (6.25) follows from (6.23). Putting $A + (l + E)B = xq$ in (6.26) yields

$$n(\alpha) = \big(x(A - lB) - wB^2C\big)q.$$

But since by (6.23), $(2l + E)x + BCw \equiv 0 \pmod q$, we have

$$x(A - lB) - wB^2C \equiv x(A + (l + E)B) \equiv 0 \pmod q$$

and so $n(\alpha) \equiv 0 \pmod{q^2}$. Thus either $C \equiv 0 \pmod q$ or $(A, B) \equiv 0 \pmod q$. But if $(A, B) \equiv 0 \pmod q$ then by (6.23) $A + (l + E)B \equiv 0 \pmod{q^2}$ and (6.26) yields $n(\alpha) = 0 \pmod{q^3}$: thus $C \equiv 0 \pmod q$ in any case.

Let $q^e \| C$ where $e > 0$. Then by (6.23) $A + (l + E)B = yq^{e+1}$ for some $y \in Z$. Putting $C = q^eC_1$ in (6.26), where $(C_1, q) = 1$, gives

$$n(\alpha) = \big(y(A - lB) - wB^2C_1\big)q^{e+1}.$$

But since by (6.23), $(2l + E)y + BC_1w \equiv 0 \pmod{q^{e+1}}$ we have

$$y(A - lB) - wB^2C_1 \equiv y(A + (l + E)B) \equiv 0 \pmod{q^{e+1}}$$

and so $n(\alpha) \equiv 0 \pmod{q^{2(e+1)}}$. Since $q^e \| C$ we must have $(A, B) \equiv 0 \pmod q$. Now by (6.23) $A + (l + E)B = zq^{e+2}$ for some $z \in Z$ and (6.26) yields

$$n(\alpha) = \big(z(A_1 - lB_1) - wB_1^2C_1\big)q^{e+3}$$

where $A = qA_1$ and $B = qB_1$. But since by (6.23) $(2l + E)z + B_1C_1w \equiv 0 \pmod{q^e}$ we have $z(A_1 - lB_1) - wB_1^2C_1 \equiv z(A_1 + (l + E)B_1) \equiv 0 \pmod{q^e}$ and so $n(\alpha) \equiv 0 \pmod{q^{2e+3}}$ which is impossible since it would imply that $C \equiv 0 \pmod{q^{e+1}}$.

Thus there exists no odd prime q such that $n \equiv 0 \pmod q$ and Theorem 2 is proved.

7. Determination of minimal integers of degree three

We use the results of Section 6 to determine minimal integers of degree three in $\sqrt{\alpha}$ in the cases (i) $d \equiv 2, 3 \pmod 4$; (ii) $d \equiv 5 \pmod 8$. So from henceforth we shall assume that $d \not\equiv 1 \pmod 8$.

THEOREM 3. *Suppose there exists an integer*

$$\beta = \big(c_0 + c_1\sqrt{\alpha} + c_2\alpha + \alpha\sqrt{\alpha}\big)/2^aBC$$

where $a \in Z$ and $a > 0$. Then

(i) *There exist $h, l, m \in Z$ such that*

$$c_0 = 2^{a-1}C(hB - mA), \tag{7.1}$$

$$c_1 = lB - A, \tag{7.2}$$

$$c_2 = 2^{a-1}Cm. \tag{7.3}$$

https://doi.org/10.1017/S1446788700023648 Published online by Cambridge University Press

(ii) *There exist* $x, y, z \in Z$ *such that*

$$A + (l + E)B = 2^{a-1}xC, \tag{7.4}$$

$$D - l(l + E) = 2^{a-1}yC, \tag{7.5}$$

$$(2l + E)x + yB = 2^{a-1}zC. \tag{7.6}$$

(iii) *Without loss of generality we may choose* h *and* m *modulo* 2. *Finally the rational integers defined above satisfy*

$$h^2 + Dm^2 - lz - xy \equiv 0 \pmod 4, \tag{7.7}$$

$$2mh + Em^2 - z \equiv 0 \pmod 4. \tag{7.8}$$

PROOF. The assumption that β be integral is equivalent to the simultaneous solvability of (6.15)–(6.18) with $t = 2^aBC$ $(a > 0)$.

(i) (7.1) and (7.3) follow immediately from (6.15) and (6.16). Putting $t = 2B$ in (6.16)–(6.18) and using Lemma 4 yields (7.2).

(ii) Substituting (7.1)–(7.3) in (6.17) and (6.18) yields

$$2^{2(a-1)}C^2(h^2 + Dm^2) - A(l^2 + D) - BD(2l + E) \equiv 0 \pmod{2^{2a}C^2}, \tag{7.9}$$

$$2^{2(a-1)}C^2(2mh + Em^2) - A(2l + E) - B\big((l + E)^2 + D\big) \equiv 0 \pmod{2^{2a}C^2} \tag{7.10}$$

and so

$$A(l^2 + D) + BD(2l + E) \equiv 0 \pmod{2^{2(a-1)}C^2}$$

and

$$A(2l + E) + B\big((l + E)^2 + D\big) \equiv 0 \pmod{2^{2(a-1)}C^2}.$$

Addition of suitable multiples of these yields

$$A(l(l + E) - D)^2 \equiv 0 \pmod{2^{2(a-1)}C^2}$$

and

$$B(l(l + E) - D)^2 \equiv 0 \pmod{2^{2(a-1)}C^2}$$

so (7.5) follows from the fact that (A, B) is square-free. Substituting (7.5) in (7.9) and (7.10) yields

$$2^{2(a-1)}C^2(h^2 + Dm^2) - l(2l + E)(A + (l + E)B) - 2^{a-1}Cy(A + (2l + E)B) \equiv 0 \pmod{2^{2a}C^2} \tag{7.11}$$

$$2^{2(a-1)}C^2(2mh + Em^2) - (2l + E)(A + (l + E)B) - 2^{a-1}CyB \equiv 0 \pmod{2^{2a}C^2}. \tag{7.12}$$

https://doi.org/10.1017/S1446788700023648 Published online by Cambridge University Press

We claim that

$$A + (l + E)B \equiv 0 \pmod{2^{a-1}}. \tag{7.13}$$

If $d \equiv 1 \pmod 4$ then $2l + E$ is odd and (7.13) follows immediately from (7.12). If $d \equiv 2, 3 \pmod 4$ we note that (7.12) yields

$$-(2l + E)(A + (l + E)B) \equiv 2^{a-1}CyB \pmod{2^{2(a-1)}C^2}$$

which gives, on substitution in (7.11)

$$y(A + (l + E)B) \equiv 0 \pmod{2^{a-1}}.$$

If y is odd then (7.13) is immediate. Suppose then that y is even. Since $D(= d)$ is not a quadratic residue mod 4, (7.5) implies that $a = 1$ and so (7.13) is trivial. We may now put $A + (l + E)B = 2^{a-1}x_0$ in (7.12) and this yields $(2l + E)x_0 + yBC \equiv 0 \pmod{2^{a-1}C^2}$, say

$$(2 + E)x_0 + yBC = z2^{a-1}C^2. \tag{7.14}$$

Now by (6.10), (7.5) and (7.14) we have

$$\begin{aligned} n(\alpha) &= (A - lB)(A + (l + E)B) - 2^{a-1}yB^2C \\ &= 2^{2(a-1)}(x_0^2 - zBC^2). \end{aligned}$$

But $n(\alpha) \equiv 0 \pmod{C^2}$ so $2^{a-1}x_0 \equiv 0 \pmod C$ and we may put $x_0 = xC$ because C is odd. This yields (7.4) and substitution in (7.14) gives (7.6).

REMARK. Substitution for x_0 in the above formula for $n(\alpha)$ yields the useful identity

$$A^2 - DB^2 + EAB = 2^{2(a-1)}C^2(x^2 - zB). \tag{7.15}$$

(iii) Substitution of (7.4) and (7.6) in (7.11) and (7.12) gives (7.7) and (7.8) respectively. To show that h and m need only be determined modulo 2, write $m = m_0 + 2M$ and $h = h_0 + 2H$ where $M, H \in Z$ and $m_0, h_0 = 0$ or 1. Then putting (7.1) and (7.3) in the expression for β gives, after some calculation,

$$\beta = \left(2^{a-1}BC(h_0 + m_0\omega) + (c_1 + \alpha)\sqrt{\alpha}\right)/2^aBC + (H + M\omega).$$

Since β is an integer if and only if $\beta - (H + M\omega)$ is an integer, we may assume from the outset that $m = m_0$ and $h = h_0$.

COROLLARY. *If the number β of Theorem 3 is an integer then*

$$0 < a \leqslant 2 \text{ when } d \equiv 2, 3 \pmod 4$$

and

$$0 < a \leqslant 1 \text{ when } d \equiv 5 \pmod 8.$$

https://doi.org/10.1017/S1446788700023648 Published online by Cambridge University Press

PROOF. When $d = 2, 3 \pmod 4$ then $D(= d)$ is not a quadratic residue modulo 4 and so it follows from (7.5) that $a \leqslant 2$. When $d \equiv 5 \pmod 8$ substituting (2.1) in (7.5) yields

$$d = (2l + 1)^2 + 2^{a+1}yC$$

from which it follows immediately that $a \leqslant 1$ because d is not a quadratic residue (mod 8).

LEMMA 5. *The value of the integer r in Theorem* 1 *may be chosen modulo* 4 *without loss of generality.*

PROOF. If (r, s, u, v) is a solution of (6.1)–(6.3) then so is

$$\big(r + nC, s - nC, u + (2r - E)n + n^2C, v - 2ns + 2n^2B\big)$$

for any $n \in Z$. Since $(r, r + C, r + 2C, r + 3C)$ is a complete set of residues modulo 4, we may choose a solution to (6.1)–(6.3) so that r takes any value modulo 4, without loss of generality.

We are now able to determine minimal integers of degree three in $\sqrt{\alpha}$ according to the different values of A and B. We consider the two cases of the beginning of this section separately:

CASE (i) $d = 2, 3 \pmod 4$.

It turns out that the maximum value of a is $0, 1, 2$ according as (a) B is odd, (b) B is even and A is odd, (c) A and B are both even, respectively. We consider these three cases separately:

(a) *B odd.* Assume there exists an integer β with denominator $2BC$. Then (7.1)–(7.8) hold with $a = 1$, and by (7.15)

$$A^2 - d \equiv x^2 - zB \pmod 4$$

because C is odd. Using the above it is easy to verify that (7.4)–(7.8) cannot hold, in fact, for any values of A and d. For example, when A is odd and $d \equiv 2 \pmod 4$ then the above yields $x^2 - zB \equiv 3 \pmod 4$. Since by (7.8) we must have $z \equiv 0 \pmod 2$, this yields $x \equiv 1 \pmod 2$ and $z \equiv 2 \pmod 4$. Thus by (7.8), $m = h = 1$, so by (7.7) $y \equiv 1 \pmod 2$. But this contradicts (7.6) because B is odd. A similar argument holds when A is odd and $d \equiv 3 \pmod 4$, and when A is even. Thus there are no integers of degree three in $\sqrt{\alpha}$ with denominator $2BC$ and therefore the integer η of Theorem 1 is minimal in this case.

(b) *A odd, B even.* Since (7.4) is clearly not solvable for $a \geqslant 2$, the following Lemma provides minimal integers of degree three in this case:

https://doi.org/10.1017/S1446788700023648 Published online by Cambridge University Press

LEMMA 6. *Suppose that A is odd and B is even, and let the integer η be defined by Theorem* 1(ii), *where the rational integer r is chosen so that $r \equiv d \pmod 2$. Then*

(i) $(\sqrt{d} + \eta)/2$ *is an integer when* $d \equiv 2 \pmod 4$,

(ii) $(1 + \sqrt{d} + \eta)/2$ *is an integer when* $d \equiv 3 \pmod 4$.

PROOF. (i) $\mathrm{tr}_k((\sqrt{d} + \eta)/2) = 0$ since $\mathrm{tr}_k(\eta) = 0$, and using (6.14) we get $n_k((\sqrt{d} + \eta)/2) = (d - (us + rv + v\sqrt{d}))/4$. Thus $(\sqrt{d} + \eta)/2$ is an integer if and only if $us \equiv d \pmod 4$ and $v \equiv 0 \pmod 4$. But by Lemma 5 we may choose r to be even, without loss of generality, and so (6.2) yields $u \equiv 2 \pmod 4$. Moreover (6.1) yields $s \equiv 1 \pmod 2$ as A is odd, and so $us \equiv 2 \pmod 4$. Finally (6.3) gives $v \equiv 0 \pmod 4$ and so $(\sqrt{d} + \eta)/2$ is indeed an integer provided that $d \equiv 2 \pmod 4$.

(ii) $\mathrm{tr}_k((1 + \sqrt{d} + \eta)/2) = 1 + \sqrt{d} \in I_k$, and by (6.14) $n_k((1 + \sqrt{d} + \eta)/2) = (1 + d - us - rv + (2 - v)\sqrt{d})/4$. Thus $(1 + \sqrt{d} + \eta)/2$ is an integer if and only if $us \equiv 1 + d + 2r \pmod 4$ and $v \equiv 2 \pmod 4$. But if we now choose r to be odd (6.2) again yields $u \equiv 2 \pmod 4$, hence $us \equiv 2 \pmod 4$ as s is odd by (6.1). Moreover (6.3) gives $v \equiv 2 \pmod 4$ and since when $d \equiv 3 \pmod 4$ $(1 + d + 2r) \equiv 2 \pmod 4$, $(1 + \sqrt{d} + \eta)/2$ is indeed an integer in this case.

(c) *A and B both even.* If we still choose the integer r of Theorem 1 so that $r \equiv d \pmod 2$ then the number $\eta/2$ is an integer in this case. For $\mathrm{tr}_k(\eta/2) = 0$ and $n_k(\eta/2) = -(us + vr + v\sqrt{d})/4 \in I_k$ if and only if $us \equiv v \equiv 0 \pmod 4$. But when $A \equiv B \equiv 0 \pmod 2$, (6.1) yields $s \equiv 0 \pmod 2$ and when $r \equiv d \pmod 2$, (6.2) yields $u \equiv 0 \pmod 2$, and (6.3) yields $v \equiv 0 \pmod 4$. Now $\eta/2$ is an integer of degree three in $\sqrt{\alpha}$ with denominator $2BC$, which we now show to be minimal unless

$$[A, B] \equiv [2(d^2 + 1), 2d] \pmod 4. \tag{7.16}$$

Suppose there exists an integer of degree three in $\sqrt{\alpha}$ with denominator $4BC$, so that (7.1)–(7.8) hold for $a = 2$: by (7.4) we have $A + lB \equiv 2x \pmod 4$ and by (7.5) we have $y \equiv 1 \pmod 2$ and $l \equiv d \pmod 2$ and so by (7.6), $2dx + yB \equiv 0 \pmod 4$ because $z \equiv 0 \pmod 2$ by (7.8). If $x \equiv 0 \pmod 2$ then the above imply that $[A, B] \equiv [0, 0] \pmod 4$ which is impossible. Hence $x \equiv 1 \pmod 2$ and $[A, B] \equiv [2(d^2 + 1), 2d] \pmod 4$.

Suppose now that (7.16) holds, and consider two separate cases according to the value of d modulo 4:

I $d \equiv 2 \pmod 4$. By (7.16), $[A, B, d] \equiv [2, 0, 2] \pmod 4$. From the above we have $l \equiv z \equiv 0 \pmod 2$ and $x \equiv y \equiv 1 \pmod 2$. Thus by (7.7) $h = 1$. We consider the solution of (7.4)–(7.8) in the two cases: $m = 0$, $h = 1$; $m = h = 1$. The calculations are tedious but it may be verified that a solution exists if and only if $A + B \equiv d \pmod 8$, so that if $[A, B, d] \equiv [2, 0, 2] \pmod 4$ but $A + B \not\equiv d \pmod 8$, the integer $\eta/2$ is again minimal.

https://doi.org/10.1017/S1446788700023648 Published online by Cambridge University Press

LEMMA 7. *Suppose that* $[A, B, d] \equiv [2, 0, 2] \pmod 4$ *and* $A + B \equiv d \pmod 8$. *Let the integer* η *be defined by Theorem* 1(iii) *where the integer* r *is chosen so that* $r \equiv 0 \pmod 4$. *Then*

(i) $(2 + \eta)/4$ *is and integer when* $B \equiv 0 \pmod 8$,

(ii) $(2(1 + \sqrt{d}) + \eta)/4$ *is an integer when* $B \equiv 4 \pmod 8$.

PROOF. Since $B \equiv 0 \pmod 4$ we have $A \equiv sC \pmod{16}$ by (6.2) and $D \equiv uC \pmod{16}$ by (6.1), on choosing $r \equiv 0 \pmod 4$, which is possible by Lemma 5. Hence $usC^2 \equiv Ad \pmod{16}$. Since s is even (6.3) yields $vC \equiv uB \pmod{16}$ and we have

$$[us, v] \equiv \begin{cases} [4, 0] \pmod{16} & \text{when } B \equiv \pmod 8, \\ [12, 8] \pmod{16} & \text{when } B \equiv 4 \pmod 8. \end{cases} \tag{7.17}$$

(i) $\mathrm{tr}_k((2 + \eta)/4) = 1 \in I_k$ and by (6.14)

$$n_k((2 + \eta)/4) = \big(4 - (us + rv + v\sqrt{d})\big)/16$$

and so by (7.17), $(2 + \eta)/4$ is an integer when $B \equiv 0 \pmod 8$.

(ii) $\mathrm{tr}_k((2(1 + \sqrt{d}) + \eta)/4) = 1 + \sqrt{d} \in I_k$ and by (6.14)

$$n_k\big((2(1 + \sqrt{d}) + \eta)/4\big) = \big(4(1 + d) - us - rv + (8 - v)/\sqrt{d}\big)/16$$

and by (7.17), $(2(1 + \sqrt{d}) + \eta)/4$ is an integer when $B \equiv 4 \pmod 8$.

II $d \equiv 3 \pmod 4$. By (7.16), $[A, B, d] \equiv [0, 2, 3] \pmod 4$. From the general argument above we have $z \equiv 0 \pmod 2$ and $l \equiv x \equiv y \equiv 1 \pmod 2$. Thus by (7.7), $m \not\equiv h \pmod 2$ and the solution of (7.4)–(7.8) need only be considered in the two cases: $m = 0$, $h = 1$; $m = 1$, $h = 0$. It turns out that a solution exists if and only if $A - 1 \equiv d \pmod 8$: a verification of this is tedious and therefore omitted. Thus if $[A, B, d] \equiv [0, 2, 3] \pmod 4$ and $A - 1 \not\equiv d \pmod 8$ the integer $\eta/2$ is minimal, and when $A - 1 \equiv d \pmod 8$ we have the following result:

LEMMA 8. *Suppose that* $[A, B, d] \equiv [0, 2, 3] \pmod 4$ *and* $A - 1 \equiv d \pmod 8$. *Let the integer* η *be defined by Theorem* 1(ii) *where the integer* r *is chosen so that* $r \equiv 1 \pmod 4$. *Then*

(i) $(2 + \eta)/4$ *is an integer when* $B \equiv 6 \pmod 8$,

(ii) $(2\sqrt{d} + \eta)/4$ *is an integer when* $B \equiv 2 \pmod 8$.

PROOF. By Lemma 5 we may choose $r \equiv 1 \pmod 4$ without loss of generality. This gives $A + B \equiv sC \pmod 8$ by (6.1) and $D - 1 \equiv uC \pmod 8$ by (6.2). Hence $usC^2 \equiv (A + B)(D - 1) \pmod{16}$, that is,

$$us \equiv \begin{cases} 4 \pmod{16} & \text{when } B \equiv 6 \pmod 8, \\ 12 \pmod{16} & \text{when } B \equiv 2 \pmod 8. \end{cases}$$

Moreover, since $u \equiv s \pmod 8$ when $B \equiv 6 \pmod 8$ and $u \not\equiv s \pmod 8$ when $B \equiv 2 \pmod 8$ we have, by (6.3), $v \equiv 0 \pmod{16}$.

(i) The integrability of $(2 + \eta)/4$ is evident from the proof of Lemma 7(i): for $n_k((2 + \eta)/4) \in I_k$ since $[us, v] \equiv [4, 0] \pmod{16}$ when $B \equiv 6 \pmod 8$.

(ii) $\mathrm{tr}_k((2\sqrt{d} + \eta)/4) = \sqrt{d} \in I_k$ and by (6.14)

$$n_k\big((2\sqrt{d} + \eta)/4\big) = (4d - us - rv - v\sqrt{d})/16 \in I_k$$

when $[us, v] \equiv [12, 0] \pmod{16}$, that is, when $B \equiv 2 \pmod 8$.

Since there are no integers of degree three in $\sqrt{\alpha}$ with denominator 2^aBC, $a > 2$ (Theorem 3, corollary), the integers of Lemmas 7 and 8 are minimal. Thus we have completed our search for minimal integers of degree three in $\sqrt{\alpha}$ in the case $d \equiv 2, 3 \pmod 4$. We summarize our results in the following:

LEMMA 9. *Suppose that* $d \equiv 2, 3 \pmod 4$ *and let* $\eta = (r + \sqrt{d})\sqrt{\alpha}/C$ *where the rational integer* r *satisfies Theorem* 1 *and is chosen so that* $r \equiv d + 2 \pmod 4$. *Then a minimal integer of degree three in* $\sqrt{\alpha}$ *is given by*

$$\beta_3 = \begin{cases} \eta & \text{when } B \equiv 1 \pmod 2, \\ (\sqrt{d} + \eta)/2 & \text{when } [A, B] \equiv [1, 0] \pmod 2 \text{ and } d \equiv 2 \pmod 4, \\ (1 + \sqrt{d} + \eta)/2 & \text{when } [A, B] \equiv [1, 0] \pmod 2 \text{ and } d \equiv 3 \pmod 4, \\ (2(1 + \sqrt{d}) + \eta)/4 & \text{when } [A, B, d] \equiv [2, 4, 6] \text{ or } [6, 4, 2] \pmod 8, \\ (2\sqrt{d} + \eta)/4 & \text{when } [A, B, d] \equiv [0, 2, 7] \text{ or } [4, 2, 3] \pmod 8, \\ (2 + \eta)/4 & \text{when } [A, B, d] \equiv [2, 0, 2] \text{ or } [6, 0, 6], \\ & \quad \text{or } [0, 6, 7] \text{ or } [4, 6, 3] \pmod 8, \\ \eta/2 & \text{otherwise}. \end{cases}$$

CASE (ii) $d \equiv 5 \pmod 8$.

Suppose that there exists an integer of degree three in $\sqrt{\alpha}$ with denominator 2^aBC, $a > 0$. Then, by Theorem 3, (7.1)–(7.8) are solvable for $a = 1$ (but not for $a > 1$, by the corollary). We consider the solution for four separate cases according as $m, h = 0$ or 1:

(a) $m = h = 0$. There is no solution of (7.4)–(7.8). For by (7.8), $z \equiv 0 \pmod 4$ and so (7.7) yields $xy \equiv 0 \pmod 4$. But D is odd and so y is also odd, by (7.5). Hence $x \equiv 0 \pmod 4$ and (7.6) yields $B \equiv 0 \pmod 4$. Now by (7.4), $A \equiv 0 \pmod 4$, which is impossible.

(b) $m = 1$, $h = 0$. By (7.8), $z \equiv 1 \pmod 4$ and so (7.7) becomes $D \equiv l + xy \pmod 4$. This gives a solution of (7.4)–(7.6) for $[A, B]$ modulo 4 as set out below:

https://doi.org/10.1017/S1446788700023648 Published online by Cambridge University Press

	$D \equiv 1 \pmod 4$	$D \equiv 3 \pmod 4$
$l \equiv 0 \pmod 2$	[1, 0]	[1, 0]
$l \equiv 1 \pmod 2$	[2, 3]	[0, 3]

Now if $[A, B]$ is given in the above we have the following

LEMMA 10. *Suppose that* $d \equiv 5 \pmod 8$ *and that* $[A, B] \equiv [1, 0]$ *or* $[D + 1, 3] \pmod 4$. *Let the integer* η *be defined by Theorem* 1(*ii*) *where the rational integer* r *is chosen so that* $r \equiv A \pmod 4$. *Then* $(\omega + \eta)/2$ *is an algebraic integer.*

PROOF. That r may be chosen modulo 4 is clear by Lemma 5. Now

$$\mathrm{tr}_k((\omega + \eta)/2) = \omega \in I_k$$

and by (6.14)

$$n_k((\omega + \eta)/2) = (D - us - (r - 1)v + (1 - v)\omega)/4 \in I_k \text{ if } v \equiv 1 \pmod 4$$

and $us \equiv D - r + 1 \pmod 4$. It may easily be verified that v and us take the above values when $r \equiv A \pmod 4$, D is odd and $[A, B] \equiv [1, 0]$ or $[D + 1, 3] \pmod 4$. For example, if $[A, B, D] \equiv [2, 3, 1] \pmod 4$ then by (6.1) $s \equiv 0 \pmod 4$ and so $us \equiv 0 \pmod 4$. But $D - r + 1 \equiv 1 - 2 + 1 \equiv 0 \pmod 4$. Moreover multiplying (6.3) by C and using (6.2) yields

$$v \equiv uBC \equiv 3B \equiv 1 \pmod 4.$$

Similar arguments hold for the other values of A, B and D above, and the lemma is proved.

When $[A, B] \not\equiv [1, 0]$ or $[D + 1, 3] \pmod 4$, (7.4)–(7.6) are not solvable and so there exists no integer of degree three in $\sqrt{\alpha}$ with denominator $2BC$ where the coefficients c_0 and c_2 are given by (7.1) and (7.3) with $m = 1$ and $h = 0$.

(c) $m = 0$, $h = 1$. By (7.8), $z \equiv 0 \pmod 4$ and by (7.7), $xy \equiv 1 \pmod 4$. This gives the unique solution of (7.4)–(7.8) for $[A, B]$ modulo 4, according to the different values of D and l, as set out below:

	$D \equiv 1 \pmod 4$	$D \equiv 3 \pmod 4$
$l \equiv 0 \pmod 2$	[2, 3]	[0, 3]
$l \equiv 1 \pmod 2$	[1, 1]	[3, 1]

When $[A, B] \not\equiv [D + 1, 3]$ or $[D, 1] \pmod 4$ there exists no integer of degree three in $\sqrt{\alpha}$ with denominator $2BC$ where the coefficients c_0 and c_2 are given by (7.1) and (7.3) with $m = 0$ and $h = 1$. Otherwise, we have the following:

LEMMA 11. *Suppose that* $d \equiv 5 \pmod 8$ *and that* $[A, B] \equiv [D, 1]$ *or* $[D + 1, 3] \pmod 4$. *Let the integer* η *be defined by Theorem* 1(ii) *where the rational integer* r *is chosen so that* $r \not\equiv A \pmod 2$. *Then* $(1 + \eta)/2$ *is an algebraic integer.*

https://doi.org/10.1017/S1446788700023648 Published online by Cambridge University Press

PROOF. That the parity of r may be chosen without loss of generality, is clear by Lemma 5. Now $\mathrm{tr}_k((1+\eta)/2) = 1 \in I_k$ and by (6.14)

$$n_k((1+\eta)/2) = (1 - us - (r-1)v - v\omega)/4 \in I_k$$

if and only if $v \equiv 0 \pmod 4$ and $us \equiv 1 \pmod 4$. It is easily verified that v and us take the values when the conditions of the lemma are satisfied. For example, when $[A, B] \equiv [D, 1] \pmod 4$ we have, by (6.1), $sC \equiv D + r \pmod 4$ and, by (6.2), $uC \equiv D + r \pmod 4$, as r is even. Thus $usC^2 \equiv (D+r)^2 \equiv 1 \pmod 4$, as D is odd, so $us \equiv 1 \pmod 4$ because C is odd. Moreover, (6.3) yields, on multiplication by C,

$$v \equiv uC - sC \equiv 0 \pmod 4.$$

A similar argument holds when $[A, B] \equiv [D+1, 3] \pmod 4$ and the lemma is proved.

(d) $m = h = 1$. By (7.8), $z \equiv 1 \pmod 4$ and by (7.7) $1 + D + l - xy \equiv 0 \pmod 4$. This gives the unique solution of (7.4)–(7.8) for $[A, B] \pmod 4$ as set out below:

	$D \equiv 1 \pmod 4$	$D \equiv 3 \pmod 4$
$l \equiv 0 \pmod 2$	[1, 1]	[3, 1]
$l \equiv 1 \pmod 2$	[1, 0]	[1, 0]

When $[A, B] \not\equiv [D, 1]$ or $[1, 0] \pmod 4$ there exists no integer of degree three in $\sqrt{\alpha}$ with denominator $2BC$ and coefficients c_0 and c_2 given by (7.1) and (7.3) with $m = h = 1$. But when $[A, B] \equiv [D, 1]$ or $[1, 0] \pmod 4$ we have already found integers of degree three in with denominator $2BC$. This therefore completes our search for minimal integers of degree three in $\sqrt{\alpha}$, and our results are set out in the following:

LEMMA 12. *Suppose that* $d \equiv 5 \pmod 8$ *and let* $\eta = (r - 1 + \omega)\sqrt{\alpha}/C$, *where the rational integer* r *satisfies Theorem* 1 *and so may be chosen modulo* 4 *without loss of generality. Then a minimal integer of degree three in* $\sqrt{\alpha}$ *is given by*:

$$\beta_3 = \begin{cases} (1+\eta)/2 & \text{where } r \not\equiv A \pmod 2, \\ & \text{if } [A, B] \equiv [D, 1] \text{ or } [D+1, 3] \pmod 4; \\ (\omega+\eta)/2 & \text{where } r \equiv 1 \pmod 4, \text{ if } [A, B] \equiv [1, 0] \pmod 4; \\ \eta & \text{where } r \text{ is arbitrary, otherwise.} \end{cases}$$

8. Tables of integral bases

Having constructed minimal integers of degrees one, two and, when $d \not\equiv 1 \pmod 8$, degree three in $\sqrt{\alpha}$, we now have integral bases of the form

https://doi.org/10.1017/S1446788700023648 Published online by Cambridge University Press

$[1, \beta_1, \beta_2, \beta_3]$ as explained in Section 3, for all dihedral number fields with quadratic subfield $Q(\sqrt{d})$, $d \not\equiv 1 \pmod 8$.

Table 1: $d \equiv 2, 3 \pmod 4$.

Let $\eta = (r + \sqrt{d})\sqrt{\alpha}/C$ where the rational integer r satisfies Theorem 1 and is chosen so that $r \equiv d + 2 \pmod 4$.

A	B	d	Integral basis
	ODD		$[1, \sqrt{\alpha}, \sqrt{d}, \eta]$
1 (mod 4)	0 (mod 4)	2 (mod 4)	$[1, (1 + \sqrt{\alpha})/2, \sqrt{d}, (\sqrt{d} + \eta)/2]$
1 (mod 4)	0 (mod 4)	3 (mod 4)	$[1, (1 + \sqrt{\alpha})/2, \sqrt{d}, (1 + \sqrt{d} + \eta)/2]$
1 (mod 4) 3 (mod 4) 3 (mod 4)	2 (mod 4) 0 (mod 4) 2 (mod 4)	2 (mod 4) 2 (mod 4) 2 (mod 4)	$[1, \sqrt{\alpha}, \sqrt{d}, (\sqrt{d} + \eta)/2]$
1 (mod 4) 3 (mod 4) 3 (mod 4)	2 (mod 4) 0 (mod 4) 2 (mod 4)	3 (mod 4) 3 (mod 4) 3 (mod 4)	$[1, \sqrt{\alpha}, \sqrt{d}, (1 + \sqrt{d} + \eta)/2]$
0 (mod 2) 2 (mod 4)	2 (mod 4) 0 (mod 2)	2 (mod 4) 3 (mod 4)	$[1, \sqrt{\alpha}, \sqrt{d}, \eta/2]$
2 (mod 8) 6 (mod 8) 2 (mod 8) 6 (mod 8)	0 (mod 8) 0 (mod 8) 4 (mod 8) 4 (mod 8)	6 (mod 8) 2 (mod 8) 2 (mod 8) 6 (mod 8)	$[1, \sqrt{\alpha}, (\sqrt{d} + \sqrt{\alpha})/2, \eta/2]$
0 (mod 8) 0 (mod 8) 4 (mod 8) 4 (mod 8)	2 (mod 8) 6 (mod 8) 2 (mod 8) 2 (mod 8)	3 (mod 8) 3 (mod 8) 7 (mod 8) 7 (mod 8)	$[1, \sqrt{\alpha}, (1 + \sqrt{d} + \sqrt{\alpha})/2, \eta/2]$
2 (mod 8) 6 (mod 8)	0 (mod 8) 0 (mod 8)	2 (mod 8) 6 (mod 8)	$[1, \sqrt{\alpha}, (\sqrt{d} + \sqrt{\alpha})/2, (2 + \eta)/4]$
2 (mod 8) 6 (mod 8)	4 (mod 8) 4 (mod 8)	6 (mod 8) 2 (mod 8)	$[1, \sqrt{\alpha}, (\sqrt{d} + \sqrt{\alpha})/2, (2(1 + \sqrt{d}) + \eta)/4]$
0 (mod 8) 4 (mod 8)	2 (mod 8) 2 (mod 8)	7 (mod 8) 3 (mod 8)	$[1, \sqrt{\alpha}, (1 + \sqrt{d} + \sqrt{\alpha})/2, (2\sqrt{d} + \eta)/4]$
0 (mod 8) 4 (mod 8)	6 (mod 8) 6 (mod 8)	7 (mod 8) 3 (mod 8)	$[1, \sqrt{\alpha}, (\sqrt{d} + \sqrt{\alpha})/2, (2 + \eta)/4]$

https://doi.org/10.1017/S1446788700023648 Published online by Cambridge University Press

Table 2: $d \equiv 5 \pmod 8$.

Let $\eta = (r - 1 + (1 + \sqrt{d})/2)\sqrt{\alpha}/C$, where the rational integer r satisfies Theorem 1 and is chosen so that:

$$r \equiv 1 \pmod 4 \text{ if } [A, B] \equiv [1, 0] \pmod 4;$$

$$r \equiv 0 \pmod 2 \text{ if } A \equiv 1 \pmod 2 \text{ and } B \equiv 1 \pmod 4;$$

$$r \equiv 1 \pmod 2 \text{ if } A \equiv 0 \pmod 2 \text{ and } B \equiv 3 \pmod 4.$$

A	B	Integral basis
1 (mod 4)	0 (mod 4)	$[1,(1+\sqrt{\alpha})/2,(1+\sqrt{d})/2,((1+\sqrt{d})/2+\eta)/2]$
1 (mod 2)	1 (mod 4)	$[1,\sqrt{\alpha},((1+\sqrt{d})/2+\sqrt{\alpha})/2,(1+\eta)/2]$
0 (mod 2)	3 (mod 4)	$[1,\sqrt{\alpha},(1+(1+\sqrt{d})/2+\sqrt{\alpha})/2,(1+\eta)/2]$
otherwise		$[1,\sqrt{\alpha},(1+\sqrt{d})/2,\eta]$

References

W. E. H. Berwick (1927), *Integral bases*, Cambridge.

D. Hilbert (1897), 'Die Theorie der algebraischen Zahlkörper', *Jber. Deutsch. Math.-Verein.* **4**, 175–546.

H. Mann (1955), *Introduction to algebraic number theory*, Ohio State University Press.

J. Sommer (1907), *Introduction à la théorie des nombres algébriques*, Paris.

Mathematics Division
University of Sussex
Falmer, Brighton
United Kingdom

London School of Economics
London, England
United Kingdom