

## LIFTING MONOGENIC CUBIC FIELDS TO MONOGENIC SEXTIC FIELDS

MELISA J. LAVALLEE, BLAIR K. SPEARMAN AND KENNETH S. WILLIAMS

### Abstract

Let  $e \in \{-1, +1\}$ . Let  $a, b \in \mathbf{Z}$  be such that  $x^6 + ax^4 + bx^2 + e$  is irreducible in  $\mathbf{Z}[x]$ . The cubic field  $C = \mathbf{Q}(\alpha)$ , where  $\alpha^3 + a\alpha^2 + b\alpha + e = 0$ , is said to lift to the sextic field  $K = \mathbf{Q}(\theta)$ , where  $\theta^6 + a\theta^4 + b\theta^2 + e = 0$ . The field  $K$  is called the lift of  $C$ . If  $\{1, \alpha, \alpha^2\}$  is an integral basis for  $C$  (so that  $C$  is monogenic), we investigate conditions on  $a$  and  $b$  so that  $\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5\}$  is an integral basis for the lift  $K$  of  $C$  (so that  $K$  is monogenic). As the sextic field  $K$  contains a cubic subfield (namely  $C$ ), there are eight possibilities for the Galois group of  $K$ . For five of these Galois groups, we show that infinitely many monogenic sextic fields can be obtained in this way, and for the remaining three Galois groups, we show that only finitely many monogenic fields can arise in this way, when  $e \in \{-1, +1\}$ .

### 1. Introduction

Suppose that a cubic field  $C$  is defined by a cubic polynomial  $g(x) = x^3 + ax^2 + bx \pm 1$  with  $a, b \in \mathbf{Z}$ . Let  $\alpha$  be a root of  $g(x)$  and suppose that  $\{1, \alpha, \alpha^2\}$  is an integral basis for  $C$  (so that  $C$  is monogenic). Let  $f(x) = g(x^2) = x^6 + ax^4 + bx^2 \pm 1$  and suppose that  $f$  defines a sextic field  $K$ . Let  $\theta$  be a root of  $f$ . We investigate conditions on  $a$  and  $b$  so that  $\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5\}$  is an integral basis for  $K$ . There are eight possibilities for the Galois group of a sextic field containing a cubic subfield [2, p. 325], namely  $C_6$ ,  $S_3$ ,  $D_6$ ,  $A_4$ ,  $(S_4, +)$ ,  $(S_4, -)$ ,  $A_4 \times C_2$  and  $S_4 \times C_2$ . We show that for five of these Galois groups, there are infinitely many monogenic sextic fields which can be obtained in this way. For the remaining three Galois groups, we show that there are at most finitely many such monogenic sextic fields. We prove the following theorem in Section 3 after some lemmas are proved in Section 2.

---

1991 *Mathematics Subject Classification.* 11R16, 11R21, 11R29.

*Key words and phrases.* Monogenic cubic fields, sextic fields, Galois group.

The research of the authors was supported by grants from the Natural Sciences and Engineering Research Council of Canada.

Received February 23, 2010; revised February 10, 2011.

**THEOREM 1.1.** *For those  $d$  specified in column 1 of TABLE 1 define  $f_d(x)$  as in column 2. Let  $\theta_d$  be a root of  $f_d(x)$ . Let  $K_d = \mathbf{Q}(\theta_d)$ . Then there are infinitely many  $d$  such that*

- (i)  $[K_d : \mathbf{Q}] = 6$ ,
- (ii)  $\text{Gal}(f_d)$  is as given in column 3 of TABLE 1,
- (iii)  $K_d$  is monogenic with integral basis  $\{1, \theta_d, \theta_d^2, \theta_d^3, \theta_d^4, \theta_d^5\}$ .

*Moreover the fields  $K_d$  are distinct.*

TABLE 1

$d \in \mathbf{Z}$	$f_d(x)$	$\text{Gal}(f_d)$
$4d^2 + 2d + 7$ squarefree	$x^6 + (2d + 2)x^4 + (2d - 1)x^2 - 1$	$A_4$
$4d^2 + 2d + 7$ squarefree	$x^6 - (2d + 2)x^4 + (2d - 1)x^2 + 1$	$A_4 \times C_2$
$d \equiv 1 \pmod{2}, d > 3, 4d^3 - 27$ squarefree	$x^6 - dx^2 - 1$	$(S_4, +)$
$d \equiv 1 \pmod{2}, d > 3, 4d^3 - 27$ squarefree	$x^6 - dx^2 + 1$	$S_4 \times C_2$
$d \equiv 1 \pmod{2}, d > 3, 4d^3 - 27$ squarefree	$x^6 + 2dx^4 + d^2x^2 + 1$	$D_6$

*Further, there exist only finitely many integers  $a$  and  $b$  such that*

- (iv)  $g(x) = x^3 + ax^2 + bx \pm 1$  defines a monogenic cubic field with integral basis  $\{1, \alpha, \alpha^2\}$ , where  $\alpha \in \mathbf{C}$  is a root of  $g(x)$ ,
- (v)  $f(x) = g(x^2) = x^6 + ax^4 + bx^2 \pm 1$  defines a monogenic sextic field with integral basis  $\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5\}$ , where  $\theta \in \mathbf{C}$  is a root of  $f(x)$ ,

*and*

- (vi)  $\text{Gal}(f) = C_6, S_3$  or  $(S_4, -)$ .

**2. Four lemmas**

In this section we prove four lemmas which will be used in the proof of Theorem 1.1 in Section 3.

**LEMMA 2.1.** *Let  $g(x) = x^3 + ax^2 + bx + 1 \in \mathbf{Z}[x]$ . Let  $\alpha$  be a root of  $g(x)$ . Suppose that  $g(x)$  defines a monogenic cubic field  $C$  and that  $\{1, \alpha, \alpha^2\}$  is a power basis of  $C$ . Let  $f(x) = x^6 + ax^4 + bx^2 + 1$  and suppose that  $\theta$  is a root of  $f(x)$ . Let  $K = \mathbf{Q}(\theta)$  and suppose that  $[K : \mathbf{Q}] = 6$ . Then  $K$  is monogenic with power basis  $\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5\}$  if and only if*

$$(a, b) \not\equiv (0, 2), (1, 1), (2, 0), (2, 2), (3, 3) \pmod{4}.$$

*Proof.* We have

$$\text{disc}(x^3 + ax^2 + bx + 1) = -27 + 18ab + a^2b^2 - 4a^3 - 4b^3$$

and

$$\text{disc}(x^6 + ax^4 + bx^2 + 1) = -2^6(-27 + 18ab + a^2b^2 - 4a^3 - 4b^3)^2.$$

We denote the discriminant of an algebraic number field  $F$  by  $d(F)$ . As  $\mathbf{Q} \subset C \subset K$ ,  $[K : \mathbf{Q}] = 6$ ,  $[C : \mathbf{Q}] = 3$ , we have  $[K : C] = 2$  and

$$d(C)^2 \mid d(K)$$

so that

$$d(K) = -2^t(-27 + 18ab + a^2b^2 - 4a^3 - 4b^3)^2$$

with  $t \in \{0, 2, 4, 6\}$ . Thus  $K$  is monogenic with power basis  $\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5\}$  if and only if  $t = 6$ . Now  $t < 6$  if and only if

$$\lambda = \frac{a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\theta^4 + \theta^5}{2}$$

is an algebraic integer for some integers  $a_i \in \{0, 1\}$ . We show that  $\lambda$  is never an algebraic integer in the following twenty-three cases

- $(a_0, a_1, a_2, a_3, a_4) = (0, 0, 0, 0, 0), (0, 0, 0, 0, 1), (0, 0, 0, 1, 1), (0, 0, 1, 0, 0), (0, 0, 1, 0, 1),$   
 $(0, 0, 1, 1, 0), (0, 1, 0, 0, 1), (0, 1, 0, 1, 0), (0, 1, 0, 1, 1), (0, 1, 1, 0, 0),$   
 $(0, 1, 1, 1, 0), (0, 1, 1, 1, 1), (1, 0, 0, 0, 0), (1, 0, 0, 0, 1), (1, 0, 0, 1, 0),$   
 $(1, 0, 1, 0, 0), (1, 0, 1, 0, 1), (1, 0, 1, 1, 1), (1, 1, 0, 0, 0), (1, 1, 0, 1, 0),$   
 $(1, 1, 0, 1, 1), (1, 1, 1, 0, 1), (1, 1, 1, 1, 0).$

In the remaining nine cases TABLE 2 gives necessary and sufficient conditions on  $a$  and  $b$  for  $\lambda$  to be an algebraic integer.

TABLE 2

$(a_0, a_1, a_2, a_3, a_4)$	conditions on $(a, b)$ for $\lambda$ to be an algebraic integer
$(0, 0, 0, 1, 0)$	$(a, b) \equiv (3, 3) \text{ or } (7, 7) \pmod{8}$
$(0, 0, 1, 1, 1)$	$(a, b) \equiv (3, 3) \pmod{4}$
$(0, 1, 0, 0, 0)$	$(a, b) \equiv (1, 1) \text{ or } (3, 3) \pmod{4}$
$(0, 1, 1, 0, 1)$	$(a, b) \equiv (2, 2) \pmod{4} \text{ or } (a, b) \equiv (3, 3) \text{ or } (7, 7) \pmod{8}$
$(1, 0, 0, 1, 1)$	$(a, b) \equiv (3, 3) \text{ or } (7, 7) \pmod{8}$
$(1, 0, 1, 1, 0)$	$(a, b) \equiv (2, 2) \text{ or } (3, 3) \pmod{4}$
$(1, 1, 0, 0, 1)$	$(a, b) \equiv (1, 1) \text{ or } (3, 3) \pmod{4}$
$(1, 1, 1, 0, 0)$	$(a, b) \equiv (3, 3) \text{ or } (7, 7) \pmod{8}$
$(1, 1, 1, 1, 1)$	$(a, b) \equiv (0, 2) \text{ or } (2, 0) \pmod{4}$

To prove these assertions requires nothing more than modular arithmetic. We just give the details for two of the cases. We first show that

$$\mu = \frac{1 + \theta^3 + \theta^5}{2}$$

is not an algebraic integer. (This is the case  $(a_0, a_1, a_2, a_3, a_4) = (1, 0, 0, 1, 0)$ .) We begin by using MAPLE to determine the sextic polynomial  $x^6 + cx^5 + dx^4 + ex^3 + fx^2 + gx + h$  satisfied by  $\mu$ . We find that

$$f = \frac{f_1}{16},$$

where  $f_1$  is a polynomial in  $a$  and  $b$  with integral coefficients such that

$$f_1 \equiv a^2b^3 + a^3b + a^2b + ab^3 + ab + a^2 + a + b^5 + b^3 + b^2 + b \equiv ab \pmod{2}.$$

If  $a \equiv b \equiv 1 \pmod{2}$  then  $\mu$  is not an algebraic integer.

If  $a \equiv 0 \pmod{2}$  and  $b \equiv 1 \pmod{2}$  we set  $a = 2k$  ( $k \in \mathbf{Z}$ ) and find that

$$d = \frac{d_1}{4},$$

where  $d_1$  is a polynomial in  $b$  and  $k$  with integral coefficients such that

$$d_1 \equiv b \equiv 1 \pmod{2}$$

so that  $\mu$  is not an algebraic integer. If  $a \equiv b \equiv 0 \pmod{2}$  we set  $a = 2k$  ( $k \in \mathbf{Z}$ ) and  $b = 2j$  ( $j \in \mathbf{Z}$ ) and find that

$$d = \frac{d_2}{2},$$

where  $d_2$  is a polynomial in  $j$  and  $k$  with integral coefficients such that

$$d_2 \equiv 1 + j \pmod{2}.$$

If  $j \equiv 0 \pmod{2}$  then  $\mu$  is not an algebraic integer. If  $j \equiv 1 \pmod{2}$  we set  $j = 2m + 1$  ( $m \in \mathbf{Z}$ ) and find that

$$f = \frac{f_2}{8},$$

where  $f_2$  is a polynomial in  $m$  and  $k$  with integral coefficients with

$$f_2 \equiv k \pmod{2}.$$

If  $k \equiv 1 \pmod{2}$  then  $\mu$  is not an algebraic integer. If  $k \equiv 0 \pmod{2}$  we set  $k = 2n$  ( $n \in \mathbf{Z}$ ) and find that

$$h = \frac{h_1}{64},$$

where  $h_1$  is a polynomial in  $m$  and  $n$  with integral coefficients and

$$h_1 \equiv 1 \pmod{2}$$

so that  $\mu$  is not an algebraic integer.

If  $a \equiv 1 \pmod{2}$  and  $b \equiv 0 \pmod{2}$  we set  $b = 2l$  ( $l \in \mathbf{Z}$ ) and find that

$$d = \frac{d_3}{4},$$

where  $d_3$  is a polynomial in  $a$  and  $l$  with integral coefficients and

$$d_3 \equiv a^5 + a^3 + a^2 \equiv 1 \pmod{2}$$

so that  $\mu$  is not an algebraic integer.

Finally we show that

$$\mu = \frac{\theta^2 + \theta^3 + \theta^4 + \theta^5}{2}$$

is an algebraic integer if and only if  $(a, b) \equiv (3, 3) \pmod{4}$ . (This is the case  $(a_0, a_1, a_2, a_3, a_4) = (0, 0, 1, 1, 1)$ .) If  $(a, b) \equiv (3, 3) \pmod{4}$  we set  $a = 4n + 3$  and  $b = 4\ell + 3$ , where  $n, \ell \in \mathbf{Z}$ . Then, by MAPLE,  $\mu$  satisfies the polynomial

$$\begin{aligned} & x^6 + (-16n^2 - 20n + 8\ell)x^5 + (360n^2 + 68\ell^2 - 320\ell n^3 - 656\ell n^2 \\ & - 328\ell n + 80\ell^2 n - 3\ell + 3n + 896n^4 + 992n^3 + 256n^5)x^4 \\ & + (344n^2 + 144\ell^2 + 320\ell n^3 - 544\ell n^2 - 456\ell n - 224\ell^2 n - 256\ell^2 n^3 \\ & - 768\ell^2 n^2 + 192\ell^3 n - 2\ell + 2n + 320n^4 + 256\ell n^4 + 720n^3 + 144\ell^3)x^3 \\ & + (147n^2 + 101\ell^2 + 80\ell n^3 + 128\ell n^2 - 244\ell n - 500\ell^2 n + 64\ell^2 n^3 + 48\ell^2 n^2 \\ & - 400\ell^3 n + 32n^4 + 64\ell^5 + 240\ell^4 - 64\ell^3 n^2 - 64\ell^4 n + 120n^3 + 256\ell^3)x^2 \\ & + (26n^2 + 22\ell^2 + 16\ell n^3 + 24\ell n^2 - 48\ell n - 80\ell^2 n - 16\ell^2 n^2 - 16\ell^3 n \\ & + 16\ell^4 + 12n^3 + 44\ell^3)x + 2\ell^2 + 2n^2 - 4\ell n - \ell^2 n - \ell n^2 + \ell^3 + n^3, \end{aligned}$$

which belongs to  $\mathbf{Z}[x]$ , so that  $\mu$  is an algebraic integer. Now we prove the converse. Suppose that  $\mu$  is an algebraic integer. Let  $x^6 + cx^5 + dx^4 + ex^3 + fx^2 + gx + h$  be the polynomial (given by MAPLE) satisfied by  $\mu$ . Then

$$e = \frac{e_1}{4},$$

where  $e_1$  is a polynomial in  $a$  and  $b$  with integral coefficients such that

$$e_1 \equiv a^4 b + a^3 b^2 + a^3 b + a^2 b^2 + ab^3 + a^2 b + a^3 + a^2 + b^2 + 1 \equiv b + 1 \pmod{2}.$$

As  $\mu$  is an algebraic integer we must have  $b \equiv 1 \pmod{2}$ . We set  $b = 2k + 1$  ( $k \in \mathbf{Z}$ ). Then

$$g = \frac{g_1}{16},$$

where  $g_1$  is a polynomial in  $a$  and  $k$  with integral coefficients such that

$$g_1 \equiv a^3 + a^2 + a + 1 \equiv a + 1 \pmod{2}.$$

As  $\mu$  is an algebraic integer we deduce that  $a \equiv 1 \pmod{2}$ . We set  $a = 2m + 1$  ( $m \in \mathbf{Z}$ ). Then

$$d = \frac{d_1}{2},$$

where  $d_1$  is a polynomial in  $k$  and  $m$  with integral coefficients such that

$$d_1 \equiv m + k \pmod{2}.$$

As  $\mu$  is an algebraic integer we have  $k \equiv m \pmod{2}$ . If  $k \equiv m \equiv 0 \pmod{2}$  we set  $k = 2j$  ( $j \in \mathbf{Z}$ ) and  $m = 2i$  ( $i \in \mathbf{Z}$ ). Then

$$f = \frac{f_1}{2},$$

where  $f_1$  is a polynomial in  $i$  and  $j$  with integral coefficients such that

$$f_1 \equiv 1 \pmod{2},$$

contradicting that  $\mu$  is an algebraic integer. Hence  $k \equiv m \equiv 1 \pmod{2}$  so that  $a \equiv b \equiv 3 \pmod{4}$  as asserted.  $\square$

Our second lemma can be proved in a similar manner.

**LEMMA 2.2.** *Let  $g(x) = x^3 + ax^2 + bx - 1 \in \mathbf{Z}[x]$ . Let  $\alpha$  be a root of  $g(x)$ . Suppose that  $g(x)$  defines a monogenic cubic field  $C$  and that  $\{1, \alpha, \alpha^2\}$  is a power basis of  $C$ . Let  $f(x) = x^6 + ax^4 + bx^2 - 1$  and suppose that  $\theta$  is a root of  $f(x)$ . Let  $K = \mathbf{Q}(\theta)$  and suppose that  $[K : \mathbf{Q}] = 6$ . Then  $K$  is monogenic with power basis  $\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5\}$  if and only if*

$$(a, b) \not\equiv (0, 0), (2, 1), (2, 2), (1, 3), (3, 1), (3, 2) \pmod{4}.$$

*Proof.* It can be shown that

$$\lambda = \frac{a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\theta^4 + \theta^5}{2}$$

is never an algebraic integer when

$$\begin{aligned} (a_0, a_1, a_2, a_3, a_4) = & (0, 0, 0, 0, 0), (0, 0, 0, 1, 0), (0, 0, 0, 1, 1), (0, 1, 0, 0, 1), \\ & (0, 1, 0, 1, 0), (0, 1, 1, 0, 0), (0, 1, 1, 1, 1), (1, 0, 0, 1, 0), \\ & (1, 0, 1, 0, 0), (1, 0, 1, 1, 1), (1, 1, 0, 1, 1), (1, 1, 1, 0, 1), \\ & (1, 1, 1, 1, 0). \end{aligned}$$

In the remaining cases TABLE 3 gives necessary and sufficient conditions on  $a$  and  $b$  for  $\lambda$  to be an algebraic integer.  $\square$

TABLE 3

$(a_0, a_1, a_2, a_3, a_4)$	conditions on $(a, b)$ for $\lambda$ to be an algebraic integer
$(0, 0, 0, 0, 1)$	$(a, b) \equiv (13, 3) \pmod{16}$ and $a \equiv -b \pmod{64}$
$(0, 0, 1, 0, 0)$	$(a, b) \equiv (0, 0) \pmod{4}$
$(0, 0, 1, 0, 1)$	$(a, b) \equiv (3, 2) \pmod{4}$
$(0, 0, 1, 1, 0)$	$(a, b) \equiv (2, 1) \pmod{4}$
$(0, 0, 1, 1, 1)$	$(a, b) \equiv (1, 3) \pmod{4}$
$(0, 1, 0, 0, 0)$	$(a, b) \equiv (1, 3), (3, 1) \pmod{4}$
$(0, 1, 0, 1, 1)$	$(a, b) \equiv (2, 1) \pmod{4}$ or $(a, b) \equiv (13, 3) \pmod{16}$ and $a \equiv -b \pmod{64}$
$(0, 1, 1, 0, 1)$	$(a, b) \equiv (0, 0) \pmod{4}$ or $(a, b) \equiv (1, 7), (5, 3) \pmod{8}$
$(0, 1, 1, 1, 0)$	$(a, b) \equiv (3, 2) \pmod{4}$ or $(a, b) \equiv (13, 3) \pmod{16}$ and $a \equiv -b \pmod{64}$
$(1, 0, 0, 0, 0)$	$(a, b) \equiv (13, 3) \pmod{16}$ and $a \equiv -b \pmod{64}$
$(1, 0, 0, 0, 1)$	$(a, b) \equiv (2, 1) \pmod{4}$
$(1, 0, 0, 1, 1)$	$(a, b) \equiv (3, 2) \pmod{4}$ or $(a, b) \equiv (1, 7), (5, 3) \pmod{8}$
$(1, 0, 1, 0, 1)$	$(a, b) \equiv (13, 3) \pmod{16}$ and $a \equiv -b \pmod{64}$
$(1, 0, 1, 1, 0)$	$(a, b) \equiv (0, 0), (1, 3) \pmod{4}$
$(1, 1, 0, 0, 0)$	$(a, b) \equiv (3, 2) \pmod{4}$
$(1, 1, 0, 0, 1)$	$(a, b) \equiv (1, 3), (3, 1) \pmod{4}$
$(1, 1, 0, 1, 0)$	$(a, b) \equiv (13, 3) \pmod{16}$ and $a \equiv -b \pmod{64}$
$(1, 1, 1, 0, 0)$	$(a, b) \equiv (2, 1) \pmod{4}$ or $(a, b) \equiv (1, 7), (5, 3) \pmod{8}$
$(1, 1, 1, 1, 1)$	$(a, b) \equiv (0, 0), (2, 2) \pmod{4}$ or $(a, b) \equiv (13, 3) \pmod{16}$ and $a \equiv -b \pmod{64}$

Before proving the last two lemmas of this section we observe that  $4x^3 - 27$  ( $x \in \mathbf{Z}$ ) is a square if and only if  $x = 3$ . To see this we appeal to MAGMA [1], which tells us that the elliptic curve  $y^2 = x^3 - 432$  has conductor 27, rank 0, and  $(12, \pm 36)$  as its only integral points.

LEMMA 2.3. *For the values of  $d$  specified in column 1 of TABLE 4 define  $f_d(x)$  as in column 2. Then  $f_d(x)$  is irreducible and the Galois group of  $f_d(x)$  is given in column 3.*

TABLE 4

$d$	$f_d(x)$	$\text{Gal}(f_d)$
$d \in \mathbf{Z}$	$x^6 + (2d + 2)x^4 + (2d - 1)x^2 - 1$	$A_4$
$d \in \mathbf{Z}$	$x^6 - (2d + 2)x^4 + (2d - 1)x^2 + 1$	$A_4 \times C_2$
$d \in \mathbf{Z}, d \equiv 1 \pmod{2}, d > 3$	$x^6 - dx^2 - 1$	$(S_4, +)$
$d \in \mathbf{Z}, d \equiv 1 \pmod{2}, d > 3$	$x^6 - dx^2 + 1$	$S_4 \times C_2$
$d \in \mathbf{Z}, d \neq 0, 2, 3$	$x^6 + 2dx^4 + d^2x^2 + 1$	$D_6$

*Proof.* The assertion of the first row of TABLE 4 is proved in [4]. We now give the proofs of the assertions of the second, third, fourth and fifth rows.

We begin by proving the assertion of the second row of TABLE 4. Let

$$f_d(x) = x^6 - (2d + 2)x^4 + (2d - 1)x^2 + 1, \quad d \in \mathbf{Z},$$

$\theta_d$  be a root of  $f_d$ ,

$$K_d = \mathbf{Q}(\theta_d),$$

$L_d =$  normal closure of  $K_d$ ,

$$g_d(x) = x^3 - (2d + 2)x^2 + (2d - 1)x + 1.$$

First we prove that  $K_d$  contains a unique cyclic cubic subfield  $C_d$ . Clearly  $g_d(x)$  is irreducible by the rational root theorem. Hence  $C_d = \mathbf{Q}(\theta_d^2)$  is a cubic subfield of  $K_d$ . It is cyclic since the discriminant of  $g_d$  is equal to  $(4d^2 + 2d + 7)^2$ . Next we show that  $f_d(x)$  is irreducible over  $\mathbf{Q}$ . If  $f_d(x)$  were reducible over  $\mathbf{Q}$  then  $[K_d : \mathbf{Q}] < 6$ . Since  $K_d$  has a subfield of degree 3 over  $\mathbf{Q}$  we deduce that  $[K_d : \mathbf{Q}] = 3$ . Therefore  $\theta_d$  is a root of an irreducible cubic polynomial over  $\mathbf{Q}$ , say

$$h(x) = x^3 + ax^2 + bx + c, \quad a, b, c \in \mathbf{Z}.$$

Clearly  $-\theta_d$  is a root of  $-h(-x)$  and  $h(x) \neq -h(-x)$ . As  $\theta_d, -\theta_d$  are roots of  $f_d(x)$  we deduce that

$$f_d(x) = h(x)(-h(-x)) = x^6 + (-a^2 + 2b)x^4 + (b^2 - 2ac)x^2 - c^2.$$

This is a contradiction since the constant term of  $f_d$  is equal to 1. Next we show that  $f_d$  has four real roots and two complex (nonreal) roots. First we note that since the square of each root of  $f_d$  belongs to the real cubic subfield  $C_d$ , each root of  $f_d$  must be of the form  $r$  or  $ri$ , where  $r$  is a real number. We also note that for each root of  $f_d$  its negative is also a root of  $f_d$ . Since the discriminant of  $f_d(x)$  is equal to

$$-2^6(4d^2 + 2d + 7)^4 < 0$$

$f_d(x)$  does have nonreal roots. If  $f_d$  has four complex roots then its discriminant would be positive. Hence  $f_d$  has two or six complex roots. Therefore the number of real roots is zero or four. If there were no real roots then the roots of  $f_d$  would be

$$\pm r_1 i, \pm r_2 i, \pm r_3 i, \quad r_1, r_2, r_3 \in \mathbf{R}.$$

It would follow that  $f_d(x) = (x^2 + r_1^2)(x^2 + r_2^2)(x^2 + r_3^2)$  so that the coefficients of the  $x^4$  and  $x^2$  terms would both be positive. However this is obviously not the case. Therefore we may take the six roots of  $f_d$  as

$$\pm\phi_1 = \pm r_1, \quad \pm\phi_2 = \pm r_2, \quad \pm\phi_3 = \pm r_3 i,$$



where  $r_1, r_2$  and  $r_3$  are real numbers and  $\phi_1 = \theta_d$ . Next we show that

$$[L_d : \mathbf{Q}] = 24.$$

We know that  $[K_d : \mathbf{Q}] = 6$ . Suppose that  $\phi_2 \in K_d$ . Then

$$\phi_2 = \alpha + \beta\phi_1, \quad \alpha, \beta \in C_d.$$

Squaring both sides, and using  $\phi_1^2, \phi_2^2 \in C_d$ , and closure in  $C_d$ , we deduce that

$$2\alpha\beta\phi_1 \in C_d.$$

Since  $\phi_1$  generates an extension of degree 6, we have  $\phi_1 \notin C_d$  so that either  $\alpha = 0$  or  $\beta = 0$ . Clearly  $\beta \neq 0$  as  $\phi_2 \notin C_d$ . Therefore  $\alpha = 0$  so that

$$\phi_2 = \beta\phi_1.$$

Squaring gives

$$\phi_2^2 = \beta^2\phi_1^2.$$

Since the  $\phi_i^2$  are primitive conjugate elements of a cyclic (normal) cubic field there exists by Galois theory an isomorphism  $\sigma$  of  $C_d$  which we write in cycle notation as

$$(\phi_1^2, \phi_2^2, \phi_3^2).$$

Applying this to our equation gives

$$\phi_3^2 = \sigma(\beta^2)\phi_2^2.$$

However the right hand side is positive as it is the square of a real number and the left hand side is negative as it is the square of a quadratic imaginary giving a contradiction. Therefore

$$[K_d(\phi_2) : \mathbf{Q}] = 12,$$

so that as  $\phi_3$  is complex we have  $\phi_3 \notin K_d(\phi_2)$ . Therefore

$$[L_d : \mathbf{Q}] = 24.$$

Finally we determine the Galois group of  $f_d$ . Since

$$[L_d : \mathbf{Q}] = 24,$$

and the discriminant of  $f_d$  is negative we see [2, p. 325] that the Galois group is either  $(S_4, -)$  or  $A_4 \times C_2$ . Now  $L_d$  contains a normal cubic subfield so that  $\text{Gal}(f_d)$  contains a normal subgroup of index 3, that is a normal subgroup of order 8. However  $S_4$  does not have a normal subgroup of order 8. As there are 3 Sylow 2-subgroups of order 8 [3, p. 144], we deduce that  $\text{Gal}(f_d)$  is  $A_4 \times C_2$ .

We now prove the assertion of the third row of TABLE 4. Let

$$f_d(x) = x^6 - dx^2 - 1, \quad d \in \mathbf{Z}, \quad d \equiv 1 \pmod{2}, \quad d > 3,$$

$$\theta_d \text{ be a root of } f_d, \quad \text{disc}(f_d) = 2^6(4d^3 - 27)^2,$$

$$K_d = \mathbf{Q}(\theta_d),$$

$$L_d = \text{normal closure of } K_d,$$

$$g_d(x) = x^3 - dx - 1.$$

In a similar manner we can show that  $K_d$  contains a unique totally real non-abelian cubic field and  $f_d(x)$  is irreducible over  $\mathbf{Q}$ .

Next we show that  $f_d$  has two real roots and four nonreal roots. By Rolle's theorem  $f_d$  has some nonreal roots. In fact as  $f_d$  has a positive discriminant it must have exactly four nonreal roots. Therefore we may take the six roots of  $f_d$  to be

$$\pm\phi_1 = \pm r_1, \quad \pm\phi_2 = \pm r_2 i, \quad \pm\phi_3 = \pm r_3 i, \quad r_1, r_2, r_3 \in \mathbf{R},$$

where  $\phi_1 = \theta_d$ .

Next we show that

$$[L_d : \mathbf{Q}] = 24$$

and determine the Galois group of  $f_d$ . We know that  $[K_d : \mathbf{Q}] = 6$ . Suppose that  $\phi_2 \in K_d$ . This is impossible as  $\phi_2$  is nonreal and  $K_d$  is real. Therefore

$$[K_d(\phi_2) : \mathbf{Q}] = 12.$$

If

$$[L_d : \mathbf{Q}] = 12$$

then, since the discriminant of  $f_d$  is a square in  $\mathbf{Q}$ , by [2, p. 325] the Galois group would be  $A_4$  implying that  $L_d$  contains a normal cubic subfield. This is a contradiction. Therefore

$$[L_d : \mathbf{Q}] = 24$$

and the discriminant is a square in  $\mathbf{Q}$  so the Galois group must be  $(S_4, +)$ .

We now prove the assertion of the fourth row of TABLE 4. Let

$$f_d(x) = x^6 - dx^2 + 1, \quad d \in \mathbf{Z}, \quad d \equiv 1 \pmod{2}, \quad d > 3,$$

$$\theta_d \text{ be a root of } f_d,$$

$$K_d = \mathbf{Q}(\theta_d),$$

$$L_d = \text{normal closure of } K_d,$$

$$g_d(x) = x^3 - dx + 1.$$

In a similar manner we can show that  $K_d$  contains a unique totally real non-abelian cubic field and  $f_d(x)$  is irreducible over  $\mathbf{Q}$ .

Next we show that  $f_d$  has four real roots and two nonreal roots. Again since the cubic subfield is totally real, the roots of  $f_d$  must be real or pure imaginary. Since the discriminant of  $f_d(x)$  is equal to  $-2^6(4d^3 - 27)^2$ , which is negative,  $f_d$  does have some nonreal roots, in fact two or six. Thus the number of real roots is zero or four. If there were no real roots then the roots of  $f_d$  would be

$$\pm r_1 i, \pm r_2 i, \pm r_3 i, \quad r_1, r_2, r_3 \in \mathbf{R}.$$

It would then follow that  $f_d(x) = (x^2 + r_1^2)(x^2 + r_2^2)(x^2 + r_3^2)$  so that the signs of the  $x^4$  and  $x^2$  terms would both be positive. This is obviously not the case. Therefore we may take the six roots of  $f_d$  to be

$$\pm\phi_1 = \pm r_1, \quad \pm\phi_2 = \pm r_2, \quad \pm\phi_3 = \pm r_3 i, \quad r_1, r_2, r_3 \in \mathbf{R},$$

where  $\phi_1 = \theta_d$ .

Next we show that

$$[L_d : \mathbf{Q}] = 48$$

and determine the Galois group of  $f_d$ . We know that  $[K_d : \mathbf{Q}] = 6$ . Let  $E_d$  denote the normal closure of  $C_d$ . The field  $E_d$  is an extension of  $\mathbf{Q}$  of degree 6. Suppose that  $\phi_1 \in E_d$ . Then the field  $K_d$  would be normal, which is impossible as  $E_d$  is real (recall that  $d > 3$ ) but  $\phi_3$  is nonreal. Therefore

$$[E_d(\phi_1) : \mathbf{Q}] = 12$$

as  $\phi_1^2 \in C_d \subset E_d$ . If  $\phi_2 \in E_d(\phi_1)$  then

$$\phi_2 = \alpha + \beta\phi_1, \quad \text{for } \alpha, \beta \in E_d \text{ (a normal real sextic field).}$$

Squaring both sides, and using closure properties, we deduce that

$$2\alpha\beta\phi_1 \in E_d.$$

Since  $\phi_1 \notin E_d$  we deduce that  $\alpha = 0$  or  $\beta = 0$ . But  $\beta = 0$  is impossible as  $\phi_2 \notin E_d$ . Therefore  $\alpha = 0$  so

$$\phi_2 = \beta\phi_1$$

so that

$$\phi_2^2 = \beta^2\phi_1^2.$$

Since the  $\phi_j^2$  are primitive conjugate elements of a cubic field there exists by Galois theory an isomorphism  $\sigma$  of  $E_d$ , which we write in cycle notation as  $(\phi_1^2, \phi_2^2, \phi_3^2)$ . Applying this to our equation gives  $\phi_3^2 = \sigma(\beta^2)\phi_2^2$ . However the right hand side of this equation is positive and the left hand side is negative giving a contradiction. Therefore

$$[E_d(\phi_1, \phi_2) : \mathbf{Q}] = 24.$$

Finally, as  $\phi_3$  is complex, we have  $\phi_3 \notin E_d(\phi_1, \phi_2)$ . Thus

$$[L_d : \mathbf{Q}] = 48.$$

Then, appealing to [4, p. 325], we deduce  $\text{Gal}(f_d) = S_4 \times C_2$ .

Finally we prove the assertion of the fifth row of TABLE 4. Let

$$f_d(x) = x^6 + 2dx^4 + d^2x^2 + 1, \quad d \in \mathbf{Z}, \quad d \neq 0, 2, 3,$$

$$\theta_d \text{ be a root of } f_d, \quad \text{disc}(f_d) = -2^6(4d^3 - 27)^2,$$

$$K_d = \mathbf{Q}(\theta_d),$$

$$L_d = \text{normal closure of } K_d,$$

$$g_d(x) = x^3 + 2dx^2 + d^2x + 1.$$

In a similar manner we can show that  $K_d$  contains a unique totally real non-abelian cubic field and  $f_d(x)$  is irreducible over  $\mathbf{Q}$ .

Next we note that over the field  $K_d$  we have the factorization

$$f_d(x) = (x - \theta_d)(x + \theta_d)(x^2 - \theta_d x + \theta_d^2 + d)(x^2 + \theta_d x + \theta_d^2 + d).$$

At least one of the quadratics must be irreducible over  $K_d$  because the splitting field of  $f_d(x)$  contains at least two quadratic subfields, namely  $\mathbf{Q}(\sqrt{4d^3 - 27})$  and  $\mathbf{Q}(\sqrt{-1})$ . These two fields are distinct since  $4d^2 - 27 = -z^2$  is impossible modulo 4. Therefore  $[L_d : \mathbf{Q}] \geq 12$ . However both quadratics in the above factorization have the same discriminant, namely,  $-3\theta_d^2 - 4d$ . Thus when we adjoin a root of one of them, we have constructed the entire splitting field. We have proved  $[L_d : \mathbf{Q}] = 12$ . Since the discriminant of  $f_d(x)$  is not a square in  $\mathbf{Q}$ , by Cohen [4, p. 325] the Galois group of  $f_d$  must be  $D_6$ .

This completes the proof of Lemma 2.3. □

LEMMA 2.4. *There exist at most finitely many polynomials  $f(x) = x^6 + ax^4 + bx^2 \pm 1$  irreducible over  $\mathbf{Q}$  with  $\text{Gal}(f) = C_6, S_3$  or  $(S_4, -)$  and such that a root of  $f(x)$  is a monogenic generator of a sextic field and a root of  $x^3 + ax^2 + bx \pm 1$  is a monogenic generator of a cubic field.*

*Proof.* We just treat the case when the Galois group is  $C_6$ . The remaining cases can be treated similarly. By way of contradiction we suppose that there are infinitely many such polynomials. According to [2, p. 325] the discriminant of the polynomial  $f(x)$  cannot be a square. As  $\text{disc}(x^6 + ax^4 + bx^2 - 1) = 2^6(-27 - 18ab + a^2b^2 + 4a^3 - 4b^3)^2$  this forces us to choose the plus sign, so  $f(x) = x^6 + ax^4 + bx^2 + 1$ . Moreover the discriminant of  $f(x)$  is equal to  $-z^2$  for some integer  $z$ , so that  $i$  belongs to the splitting field of  $f(x)$ . In this case this splitting field is equal to the compositum of a cyclic cubic field defined by  $g(x) = x^3 + ax^2 + bx + 1$  and the quadratic field generated by  $i$ . The roots of  $f(x)$  are either of the form  $\pm r$  or  $\pm ri$ , where  $r$  is a real number, because they are

the square roots of elements in a cyclic cubic field. In fact they must all have the form  $\pm ri$  since each generates a sextic field (the same field) which contains  $i$ . So  $f(x)$  has six pure imaginary roots. Consider the monic sextic polynomial  $t(x)$  whose roots are equal to  $i$  times the roots of  $f(x)$ . We must have  $t(x) = x^6 - ax^4 + bx^2 - 1$ . The roots of  $t(x)$  are real numbers so they cannot generate the splitting field of  $f(x)$ . On the other hand their squares generate a cyclic cubic field. Therefore the roots of  $t(x)$  must generate the same cyclic cubic field. Hence  $t(x)$  must factor over  $\mathbf{Z}$  into two monic cubic polynomials, say

$$t(x) = (x^3 + ux^2 + vx + 1)(x^3 - ux^2 + vx - 1), \quad u, v \in \mathbf{Z},$$

taking advantage of the fact that if  $\alpha$  is a root of  $t(x)$  then so is  $-\alpha$ . Now if  $\beta$  is a root of one of these cubics say  $c(x) = x^3 + ux^2 + vx + 1$  then  $-\beta^2$  is a root of  $x^3 + ax^2 + bx + 1$ . By assumption the ring of integers of the cyclic cubic field is  $\mathbf{Z}[\beta^2]$ . Of course  $\mathbf{Z}[\beta^2] = \mathbf{Z}[\beta]$  in this case. Consequently the discriminants of the minimal polynomials of  $\beta$  and  $\beta^2$  are equal. For  $\beta$  the minimal polynomial is  $c(x)$  and from this a MAPLE calculation shows that the discriminant of the minimal polynomial of  $\beta^2$  is equal to  $\text{disc}(c(x))(uv - 1)^2$ . We deduce from  $\text{disc}(c(x)) = \text{disc}(c(x))(uv - 1)^2$  that  $uv - 1 = \pm 1$  so that either  $u = 0$  or  $v = 0$  or  $(u, v) = (-2, -1), (1, 2), (2, 1)$  or  $(-1, -2)$ . The first two choices lead to  $x^3 + ux^2 + 1$  with discriminant  $-4u^3 - 27$  and to  $x^3 + vx + 1$  with discriminant  $-4v^3 - 27$ . These are only squares if  $u = v = -3$ , therefore cannot generate  $C_3$  fields. Only finitely many choices remain so the theorem is proved.  $\square$

### 3. Proof of Theorem 1.1

We first state a result of Llorente and Nart [5] giving the discriminant of a cubic field. For a prime  $p$  and a nonzero integer  $m$  we denote by  $v_p(m)$  the largest integer  $k$  such that  $p^k | m$ .

LEMMA 3.1. *Let  $f(x) = x^3 - ax + b \in \mathbf{Z}[x]$  be irreducible over  $\mathbf{Z}$ . Let  $\Delta := 4a^3 - 27b^2 (\neq 0)$ . For a prime  $p$  set  $s_p = v_p(\Delta)$  and  $\Delta_p = \Delta/p^{s_p}$ . Suppose further that  $f(x)$  satisfies the simplifying assumption, that is, if  $p$  is a prime then  $v_p(a) < 2$  or  $v_p(b) < 3$ . Let  $\theta \in \mathbf{C}$  be a root of  $f(x)$  and set  $K = \mathbf{Q}(\theta)$ . Then*

$$d(K) = \text{sgn}(\Delta) 2^{s_2} 3^{s_3} \prod_{\substack{p>3 \\ s_p \text{ odd}}} p \prod_{\substack{p>3 \\ 1 \leq v_p(b) \leq v_p(a)}} p^2,$$

where

$$\alpha = \begin{cases} 3, & \text{if } s_2 \equiv 1 \pmod{2}, \\ 2, & \text{if } 1 \leq v_2(b) \leq v_2(a), \text{ or} \\ & s_2 \equiv 0 \pmod{2} \text{ and } \Delta_2 \equiv 3 \pmod{4}, \\ 0, & \text{otherwise,} \end{cases}$$

and

$$\beta = \begin{cases} 5, & \text{if } 1 \leq v_3(b) < v_3(a), \\ 4, & \text{if } v_3(a) = v_3(b) = 2, \text{ or} \\ & a \equiv 3 \pmod{9}, b \not\equiv 0 \pmod{3} \text{ and } b^2 \not\equiv 4 \pmod{9}, \\ 3, & \text{if } v_3(a) = v_3(b) = 1, \text{ or} \\ & a \equiv 0 \pmod{3}, b \not\equiv 0 \pmod{3}, a \not\equiv 3 \pmod{9} \text{ and} \\ & b^2 \not\equiv a + 1 \pmod{9}, \text{ or} \\ & a \equiv 3 \pmod{9}, b^2 \equiv 4 \pmod{9} \text{ and } b^2 \not\equiv a + 1 \pmod{27}, \\ 1, & \text{if } 1 = v_3(a) < v_3(b), \text{ or} \\ & a \equiv 0 \pmod{3}, a \not\equiv 3 \pmod{9} \text{ and } b^2 \equiv a + 1 \pmod{9}, \text{ or} \\ & a \equiv 3 \pmod{9}, b^2 \equiv a + 1 \pmod{27} \text{ and } s_3 \equiv 1 \pmod{2}, \\ 0, & \text{if } 3 \nmid a, \text{ or} \\ & a \equiv 3 \pmod{9}, b^2 \equiv a + 1 \pmod{27} \text{ and } s_3 \equiv 0 \pmod{2}. \end{cases}$$

LEMMA 3.2. For the values of  $d$  specified in column 1 of TABLE 5 define  $g_d(x)$  as in column 2. Then  $g_d(x)$  is irreducible and the discriminant of the cubic field defined by  $g_d(x)$  is given in column 3.

TABLE 5

$d \in \mathbf{Z}$	$g_d(x)$	field discriminant
$4d^2 + 2d + 7$ squarefree	$x^3 + (2d + 2)x^2 + (2d - 1)x - 1$	$(4d^2 + 2d + 7)^2$
$4d^2 + 2d + 7$ squarefree	$x^3 - (2d + 2)x^2 + (2d - 1)x + 1$	$(4d^2 + 2d + 7)^2$
$d \equiv 1 \pmod{2}, d > 3, 4d^3 - 27$ squarefree	$x^3 - dx - 1$	$4d^3 - 27$
$d \equiv 1 \pmod{2}, d > 3, 4d^3 - 27$ squarefree	$x^3 - dx + 1$	$4d^3 - 27$
$d \equiv 1 \pmod{2}, d > 3, 4d^3 - 27$ squarefree	$x^3 + 2dx^2 + d^2x + 1$	$4d^3 - 27$

*Proof.* We give the proof of the assertion of the second row of TABLE 5. Irreducibility is a consequence of the rational root theorem. For the field discriminant, first we reduce the polynomial  $g_d(x)$  using the transformation

$$x \rightarrow x + \frac{2d + 2}{3},$$

followed by the scaling transformation

$$x \rightarrow \frac{x}{3}.$$

We obtain the polynomial

$$h_d(x) = x^3 - 3(4d^2 + 2d + 7)x - (4d + 1)(4d^2 + 2d + 7),$$

with discriminant  $\Delta$  given by

$$\Delta = 3^6(4d^2 + 2d + 7)^2.$$

Now we evaluate the field discriminant in the form

$$d(K) = \text{sgn}(\Delta)2^\alpha 3^\beta \prod_{\substack{p>3 \\ s_p \text{ odd}}} p \prod_{\substack{p>3 \\ 1 \leq v_p(b) \leq v_p(a)}} p^2.$$

Clearly  $2 \nmid \Delta$  so  $\alpha = 0$ . Next, since

$$4d^2 + 2d + 7 = \frac{(4d + 1)^2 + 27}{4}$$

and  $4d^2 + 2d + 7$  is squarefree, we deduce that  $3 \nmid 4d^2 + 2d + 7$  so that  $d \equiv 0, 1 \pmod{3}$ . Referring to the table of values for  $\beta$  in Lemma 3.1 with

$$a = 3(4d^2 + 2d + 7), \quad b = -(4d + 1)(4d^2 + 2d + 7),$$

we note that  $a \equiv 3 \pmod{9}$ ,  $b^2 \equiv a + 1 \pmod{9}$  for all  $d \equiv 0, 1 \pmod{3}$ . Finally  $s_3 = 6$  so that  $s_3 \equiv 0 \pmod{2}$ . Therefore  $\beta = 0$ . Hence

$$\prod_{\substack{p>3 \\ 1 \leq v_p(b) \leq v_p(a)}} p^2 = (4d^2 + 2d + 7)^2$$

and the proof is complete. □

We are now ready to prove Theorem 1.1.

*Proof.* The case  $(A_4)$ : This part is done in [4].

The case  $(A_4 \times C_2)$ : By Nagel's theorem [6] we can choose infinitely many  $d \in \mathbf{Z}$  such that  $4d^2 + 2d + 7$  is squarefree. Set  $g_d(x) = x^3 - (2d + 2)x^2 + (2d - 1)x + 1$ . Let  $\alpha_d \in \mathbf{C}$  be a root of  $g_d(x)$ . Set  $C_d = \mathbf{Q}(\alpha_d)$ . By the rational root theorem  $g_d(x)$  is irreducible over  $\mathbf{Q}$  so  $C_d$  is a cubic field. As

$$\text{disc}(g_d(x)) = (4d^2 + 2d + 7)^2 = d(C_d),$$

we deduce that  $\{1, \alpha_d, \alpha_d^2\}$  is a power basis for  $C_d$ . From TABLE 1  $f_d(x) = x^6 - (2d + 2)x^4 + (2d - 1)x^2 + 1$ . Let  $\theta_d$  be a root of  $f_d(x)$  and set  $K_d = \mathbf{Q}(\theta_d)$ . By Lemma 2.3  $f_d(x)$  is irreducible,  $[K_d : \mathbf{Q}] = 6$  and  $\text{Gal}(f_d) = A_4 \times C_2$ . The cubic fields  $C_d$  have distinct discriminants. Thus they are distinct fields and so the sextic fields  $K_d$  are also distinct. By Lemma 2.1  $K_d$  is monogenic with power basis  $\{1, \theta_d, \theta_d^2, \theta_d^3, \theta_d^4, \theta_d^5\}$ .

The cases  $((S_4, +), S_4 \times C_2, D_6)$ : These follow in a similar manner.

The last part of the theorem follows from Lemma 2.4. □

The authors would like to thank the referee for his/her careful reading of two drafts of this paper.

## REFERENCES

- [ 1 ] W. BOSMA, J. CANNON AND C. PLAYOUST, The Magma algebra system, I, The user language, *J. Symbolic Comput.* **24** (1997), 235–265.
- [ 2 ] H. COHEN, A course in computational algebraic number theory, Springer-Verlag, 2000.
- [ 3 ] D. S. DUMMIT AND R. M. FOOTE, Abstract algebra, Prentice-Hall, 1991.
- [ 4 ] D. ELOFF, B. K. SPEARMAN AND K. S. WILLIAMS,  $A_4$  sextic fields with a power basis, *Missouri J. Math. Sci.* **19** (2007), 188–194.
- [ 5 ] P. LORENTE AND E. NART, Effective determination of the decomposition of rational primes in a cubic field, *Proc. Amer. Math. Soc.* **87** (1983), 579–585.
- [ 6 ] T. NAGEL, Zur Arithmetik der Polynome, *Abh. Math. Sem. Hamburg* **1** (1922), 179–194.

Melisa J. Lavallee  
MATHEMATICS AND STATISTICS  
UNIVERSITY OF BRITISH COLUMBIA OKANAGAN  
KELOWNA, BC  
CANADA, V1V 1V7  
E-mail: melisa-lavallee@hotmail.com

Blair K. Spearman  
MATHEMATICS AND STATISTICS  
UNIVERSITY OF BRITISH COLUMBIA OKANAGAN  
KELOWNA, BC  
CANADA, V1V 1V7  
E-mail: Blair.Spearman@ubc.ca

Kenneth S. Williams  
SCHOOL OF MATHEMATICS AND STATISTICS  
CARLETON UNIVERSITY  
OTTAWA, ONTARIO  
CANADA, K1S 5B6  
E-mail: kwilliam@connect.carleton.ca