Far East J. Math. Sci. (FJMS) 12(2) (2004), 137-168

p-INTEGRAL BASES OF A QUARTIC FIELD DEFINED BY A TRINOMIAL $x^4 + ax + b$

ŞABAN ALACA and KENNETH S. WILLIAMS*

(Received July 18, 2003)

Submitted by K. K. Azad

Abstract

Let P be a prime ideal of an algebraic number field K, let p be a rational prime, and let $\alpha \in K$. If $v_P(\alpha) \geq 0$, then α is called a P-integral element of K, where $v_P(\alpha)$ denotes the exponent of P in the prime ideal decomposition of $\langle\alpha\rangle$. If α is P-integral for each prime ideal P of K such that $P \mid pO_K$, then α is called a p-integral element of K. Let $\{\omega_1, \omega_2, \ldots, \omega_n\}$ be a basis of K over $\mathbb{Q}$, where each ω_i $(1 \leq i \leq n)$ is a p-integral element of K. If every p-integral element α of K is given as $\alpha = a_1\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n$, where the a_i are p-integral elements of $\mathbb{Q}$, then $\{\omega_1, \omega_2, \ldots, \omega_n\}$ is called a p-integral basis of K. In this paper a p-integral basis of a quartic field K defined by a trinomial is determined for each rational prime p, and then the discriminant of K and an integral basis of K are obtained from its p-integral bases.

1. Introduction

In this paper we determine for each prime p a p-integral basis for a quartic field $K = \mathbb{Q}(\theta)$, where θ is a root of the irreducible quartic

2000 Mathematics Subject Classification: 11R16, 11R29.

Key words and phrases: quartic field, p-integral basis, integral basis, discriminant.

*Research supported by Natural Sciences and Engineering Research Council of Canada Grant A-7233.

trinomial $x^4 + ax + b$, $a, b \in \mathbb{Z}$. The discriminant of K and an integral basis of K are then obtained from its p-integral bases.

Let $K = \mathbb{Q}(\theta)$ be an algebraic number field of degree n, and let O_K denote the ring of integral elements of K. If $O_K = \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \cdots + \alpha_n\mathbb{Z}$, then $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is said to be an *integral basis* of K.

Let P be a prime ideal of K, let p be a rational prime, and let $\alpha \in K$. If $\nu_P(\alpha) \geq 0$, then α is called a *P-integral element* of K, where $\nu_P(\alpha)$ denotes the exponent of P in the prime ideal decomposition of $\langle\alpha\rangle$. If α is P-integral for each prime ideal P of K such that $P \mid pO_K$, then α is called a *p-integral element* of K.

Let $\{\omega_1, \omega_2, \ldots, \omega_n\}$ be a basis of K over $\mathbb{Q}$, where each ω_i $(1 \leq i \leq n)$ is a p-integral element of K. If every p-integral element α of K is given as $\alpha = a_1\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n$, where the a_i are p-integral elements of $\mathbb{Q}$, then $\{\omega_1, \omega_2, \ldots, \omega_n\}$ is called a *p-integral basis* of K.

In Theorem 2.1 a p-integral basis of a quartic field K is determined for every rational prime p, and in Theorem 3.1 the discriminant of K and an integral basis of K are obtained from its p-integral bases.

Let $K = \mathbb{Q}(\theta)$, where θ is a root of the irreducible trinomial

$$x^4 + ax + b, \quad a, b \in \mathbb{Z}.$$

If for any rational prime p we have $\nu_p(a) \geq 3$ and $\nu_p(b) \geq 4$, then θ/p is an algebraic integer whose minimal polynomial is $x^4 + (a/p^3)x + b/p^4 \in \mathbb{Z}[x]$ and $K = \mathbb{Q}(\theta/p)$. Hence we may assume that $K = \mathbb{Q}(\theta)$, where θ is a root of the irreducible trinomial

$$x^4 + ax + b, \; a, b \in \mathbb{Z} \text{ with } \nu_p(a) < 3 \text{ or } \nu_p(b) < 4 \text{ for every prime } p. \quad (1.1)$$

The discriminant of θ is $d(\theta) = \Delta = 2^8b^3 - 3^3a^4 \neq 0$ and $\Delta = i(\theta)^2 d(K)$, where $d(K)$ denotes the discriminant of K, and $i(\theta)$ is the index of θ. For each rational prime p, set $s_p = \nu_p(\Delta)$ and $\Delta_p = \Delta/p^{s_p}$.

The following three theorems are the special cases for $n = 4$ of Theorem 2.1, Theorem 3.1 and Theorem 3.3 respectively, given in [2].

Theorem 1.1. *Let $K = \mathbb{Q}(\theta)$ be a quartic field, where θ is a root of the irreducible trinomial* (1.1). *Let p be a rational prime, and let*

$$\alpha = \frac{x + y\theta + z\theta^2 + w\theta^3}{p^m}, \quad \text{where } x, y, z, w, m \in \mathbb{Z},\ m \geq 0.$$

Set

$$X = 4x - 3aw,$$

$$Y = 6x^2 - 9axw + 3ayz + 4byw + 2bz^2 + 3a^2w^2,$$

$$\begin{aligned} Z = {} & 4x^3 - 9ax^2w + 4bxz^2 + 8bxyw + 6axyz + 6a^2xw^2 - ay^3 \\ & - 4by^2z - 3a^2yzw + a^2z^3 - 5abyw^2 + abz^2w + 4b^2zw^2 - a^3w^3, \end{aligned}$$

$$\begin{aligned} W = {} & x^4 + 3ax^2yz + 2bx^2z^2 - axy^3 - 4bxy^2z - 3ax^3w + by^4 \\ & + b^2z^4 + b^3w^4 + 3a^2x^2w^2 - 3a^2xyzw + a^2xz^3 - 5abxyw^2 \\ & + abxz^2w + 4b^2xzw^2 - a^3xw^3 + 4bx^2yw + 3aby^2zw \\ & + 2b^2y^2w^2 - abyz^3 - 4b^2yz^2w + a^2byw^3 - ab^2zw^3. \end{aligned}$$

Then α is p-integral if and only if

$$X \equiv 0 \pmod{p^m}, \quad Y \equiv 0 \pmod{p^{2m}},$$

$$Z \equiv 0 \pmod{p^{3m}}, \quad W \equiv 0 \pmod{p^{4m}}.$$

Theorem 1.2. *Let $K = \mathbb{Q}(\theta)$ be a quartic field, where θ is a root of the irreducible trinomial* (1.1). *Let p be a rational prime, and let*

$$\frac{h + \theta}{p^i} \quad (h \in \mathbb{Z}),$$

$$\frac{u + v\theta + \theta^2}{p^j} \quad (u, v \in \mathbb{Z}),$$

$$\frac{x + y\theta + z\theta^2 + \theta^3}{p^k} \quad (x, y, z \in \mathbb{Z})$$

be p-integral elements of K having the integers i, j and k as large as possible. Then

$$\left\{1, \frac{h + \theta}{p^i}, \frac{u + v\theta + \theta^2}{p^j}, \frac{x + y\theta + z\theta^2 + \theta^3}{p^k}\right\}$$

is a p-integral basis of K, and

$$\nu_p(d(K)) = s_p - 2(i + j + k).$$

Theorem 1.3. *Let* $K = \mathbb{Q}(\theta)$ *be a quartic field, where* θ *is a root of the irreducible trinomial* (1.1). *If there are no rational primes dividing* $i(\theta)$, *then* $\{1, \theta, \theta^2, \theta^3\}$ *is an integral basis of K. Let* $p_1, p_2, \ldots, p_s$ *be the distinct primes dividing* $i(\theta)$. *Let*

$$\left\{1, \frac{h_r + \theta}{p_r^{i_r}}, \frac{u_r + v_r\theta + \theta^2}{p_r^{j_r}}, \frac{x_r + y_r\theta + z_r\theta^2 + \theta^3}{p_r^{k_r}}\right\}$$

be a p_r*-integral basis of* K $(r = 1, 2, \ldots, s)$ *as given in Theorem* 1.2. *Define the integers* h, u, v, x, y, z *by*

$$h \equiv h_r \pmod{p_r^{i_r}}, \quad u \equiv u_r \pmod{p_r^{j_r}}, \quad v \equiv v_r \pmod{p_r^{j_r}}, \quad (r = 1, 2, \ldots, s),$$

$$x \equiv x_r \pmod{p_r^{k_r}}, \quad y \equiv y_r \pmod{p_r^{k_r}}, \quad z \equiv z_r \pmod{p_r^{k_r}}, \quad (r = 1, 2, \ldots, s),$$

and let

$$R = \prod_{r=1}^{s} p_r^{i_r}, \; S = \prod_{r=1}^{s} p_r^{j_r}, \; T = \prod_{r=1}^{s} p_r^{k_r}.$$

Then an integral basis of K is

$$\left\{1, \frac{h + \theta}{R}, \frac{u + v\theta + \theta^2}{S}, \frac{x + y\theta + z\theta^2 + \theta^3}{T}\right\}.$$

2. p-integral Bases of a Quartic Field Defined by a Trinomial

Theorem 2.1. *Let* $K = \mathbb{Q}(\theta)$ *be a quartic field, where* θ *is a root of the irreducible trinomial* (1.1). *Then a* 2*-integral basis, a* 3*-integral basis, and a* $p(>3)$*-integral basis of* K *are given in Table A, Table B, and Table C, respectively. (Note that the notation* $a \equiv b \pmod m$ *has been shortened to* $a \equiv b(m)$ *in the tables.)*

Table A

Case	Condition	s_2	2-integral basis	$v_2(d(K))$
A1	$v_2(a) = 0$	0	$\{1, \theta, \theta^2, \theta^3\}$	0
A2	$v_2(a) = 1$ and $b \equiv 3(4)$	4	$\{1, \theta, \theta^2, \theta^3\}$	4
A3	$v_2(a) = 1$ and $b \equiv 1(4)$	4	$\{1, \theta, \theta^2, (1 + \theta + \theta^2 + \theta^3)/2\}$	2
A4	$v_2(a) = 1$ and $v_2(b) = 1$	4	$\{1, \theta, \theta^2, \theta^3\}$	4
A5	$v_2(a) = 1$ and $v_2(b) \geq 2$	4	$\{1, \theta, \theta^2, \theta^3/2\}$	2
A6	$v_2(a) = 2$ and $v_2(b) = 1$	8	$\{1, \theta, \theta^2, \theta^3\}$	8
A7	$v_2(a) = 2$ and $v_2(b) = 2$	8	$\{1, \theta, \theta^2/2, \theta^3/2\}$	4
A8	$v_2(a) = 2$ and $v_2(b) \geq 3$	8	$\{1, \theta, \theta^2/2, \theta^3/2^2\}$	2
A9	$v_2(a) \geq 3$ and $b \equiv 1(4)$	8	$\{1, \theta, \theta^2, \theta^3\}$	8
A10	$v_2(a) \geq 3$ and $b \equiv 3(8)$	8	$\{1, \theta, (1 + \theta^2)/2, (\theta + \theta^3)/2\}$	4

A11	$v_2(a) \geq 3$ and $b \equiv 7(8)$	8	$\{1, \theta, (1+\theta^2)/2, (1+\theta+\theta^2+\theta^3)/2^2\}$	2
A12	$v_2(a) \geq 3$ and $v_2(b) = 1$	11	$\{1, \theta, \theta^2, \theta^3\}$	11
A13	$v_2(a) = 3$ and $v_2(b) = 2$	12	$\{1, \theta, \theta^2/2, (2\theta+\theta^3)/2^2\}$	6
A14	$a = 16A,\ b = 4+16B$ $A + B \equiv 1(2)$	14	$\{1, \theta, (2+2\theta+\theta^2)/2^2,$ $(2\theta+\theta^3)/2^2\}$	6
A15	$a = 16A,\ b = 4+16B$ $A + B \equiv 0(2)$	14	$\{1, \theta, (2+2\theta+\theta^2)/2^2,$ $((2+4B)\theta+2\theta^2+\theta^3)/2^3\}$	4
A16	$v_2(a) \geq 4$ and $b \equiv 12(16)$	14	$\{1, \theta, (2+\theta^2)/2^2, (2\theta+\theta^3)/2^2\}$	6
A17	$v_2(a) = 3$ and $v_2(b) = 3$	12	$\{1, \theta, \theta^2/2, \theta^3/2^2\}$	6
A18	$v_2(a) = 4$ and $v_2(b) = 3$	16	$\{1, \theta, \theta^2/2, \theta^3/2^2\}$	10
A19	$v_2(a) \geq 5$ and $v_2(b) = 3$	17	$\{1, \theta, \theta^2/2, \theta^3/2^2\}$	11
A20	$v_2(a) = 2$ and $b \equiv 1(4)$	9	$\{1, \theta, \theta^2, \theta^3\}$	9
A21	$v_2(a) = 2$ and $b \equiv 7(8)$	10	$\{1, \theta, (1+\theta^2)/2, (\theta+\theta^3)/2\}$	6
A22	$a \equiv 4(16),\ b \equiv 11(16)$ $\Delta_2 \equiv 1(4)$	11	$\{1, \theta, (1+\theta^2)/2,$ $(5+\theta+\theta^2+\theta^3)/2^3\}$	3
A23	$a \equiv 12(16),\ b \equiv 11(16)$ $\Delta_2 \equiv 1(4)$	11	$\{1, \theta, (1+\theta^2)/2,$ $(7+\theta+3\theta^2+\theta^3)/2^3\}$	3

A24	$v_2(a) = 2,\ b \equiv 11(16)$ $\Delta_2 \equiv 3(4)$	11	$\{1, \theta, (1+\theta^2)/2,$ $(1+\theta+\theta^2+\theta^3)/2^2\}$	5
A25	$v_2(a) = 2,\ b \equiv 3(16)$ $s_2 \equiv 0(2)$	$s_2 \geq 12$	$\{1, \theta, (1+\theta^2)/2,$ $(x+y\theta+z\theta^2+\theta^3)/2^m\}$ $m = (s_2-8)/2$ $4x-3a \equiv 0(\text{mod } 2^{m+2})$ $9a^2y-16b^2 \equiv 0(\text{mod } 2^{m+4})$ $3az+4b \equiv 0(\text{mod } 2^{m+2})$	6
A26	$v_2(a) = 2,\ b \equiv 3(16)$ $s_2 \equiv 1(2),\ \Delta_2 \equiv 1(4)$	$s_2 \geq 13$	$\{1, \theta, (1+\theta^2)/2,$ $(x+y\theta+z\theta^2+\theta^3)/2^m\}$ $m = (s_2-7)/2$ $4x-3a \equiv 0(\text{mod } 2^{m+2})$ $9a^2y-16b^2 \equiv 0(\text{mod } 2^{m+4})$ $3az+4b \equiv 0(\text{mod } 2^{m+2})$	5
A27	$a = 4+16A,$ $b = 3+16B$ $s_2 \equiv 1(2)$ $A+B \equiv 2(4)$ $\Delta_2 \equiv 3(4)$	13	$\{1, \theta, (1+\theta^2)/2,$ $(x+y\theta+z\theta^2+\theta^3)/2^4\}$ $x = 15+12B$ $y = 9+8B$ $z = 3+4B$	3
A28	$a = 4+16A,$ $b = 3+16B$ $s_2 \equiv 1(2)$ $A+B \equiv 0(4)$ $\Delta_2 \equiv 3(4)$	$s_2 \geq 15$	$\{1, \theta, (1+\theta^2)/2,$ $(x+y\theta+z\theta^2+\theta^3)/2^m\}$ $m = (s_2-5)/2$ $4x-3a = 2^m + r2^{m+1}$ $9a^2y-16b^2 \equiv 2^{m+3}(\text{mod } 2^{m+4})$ $3az+4b = 2^m + t2^{m+1}$ $r+t \equiv 0(2)$	3

A29	$a = 12 + 16A$, $b = 3 + 16B$ $s_2 \equiv 1(2)$ $A - B \equiv 1(4)$ $\Delta_2 \equiv 3(4)$	13	$\{1, \theta, (1 + \theta^2)/2,$ $(x + y\theta + z\theta^2 + \theta^3)/2^4\}$ $x = 9 + 12B$ $y = 9 + 8B$ $z = 5 + 4B$	3
A30	$a = 12 + 16A$, $b = 3 + 16B$ $s_2 \equiv 1(2)$ $A - B \equiv 3(4)$ $\Delta_2 \equiv 3(4)$	$s_2 \geq 15$	$\{1, \theta, (1 + \theta^2)/2,$ $(x + y\theta + z\theta^2 + \theta^3)/2^m\}$ $m = (s_2 - 5)/2$ $4x - 3a = 2^m + r2^{m+1}$ $9a^2y - 16b^2 \equiv 2^{m+3} (\text{mod } 2^{m+4})$ $3az + 4b = 2^m + t2^{m+1}$ $r + t \equiv 1(2)$	3

Table B

Case	Condition	s_3	3-integral basis	$v_3(d(K))$
B1	$v_3(b) = 0$	0	$\{1, \theta, \theta^2, \theta^3\}$	0
B2	$v_3(a) \geq 1$ and $v_3(b) = 1$	3	$\{1, \theta, \theta^2, \theta^3\}$	3
B3	$v_3(a) = 0$, $v_3(b) = 2$ and $a^2 \not\equiv 1 (\text{mod } 9)$	3	$\{1, \theta, \theta^2, \theta^3\}$	3
B4	$v_3(a) = 0$, $v_3(b) = 2$ and $a^2 \equiv 1 (\text{mod } 9)$	3	$\{1, \theta, \theta^2, (\theta - a\theta^2 + \theta^3)/3\}$	1
B5	$v_3(a) = 1$ and $v_3(b) = 2$	6	$\{1, \theta, \theta^2, \theta^3/3\}$	4
B6	$v_3(a) \geq 2$ and $v_3(b) = 2$	6	$\{1, \theta, \theta^2/3, \theta^3/3\}$	2

B7	$v_3(a) = 0,\ v_3(b) = 3$ and $a^2 \not\equiv 1 \pmod 9$	3	$\{1, \theta, \theta^2, \theta^3\}$	3
B8	$v_3(a) = 0,\ v_3(b) = 3$ and $a^2 \equiv 1 \pmod 9$	3	$\{1, \theta, \theta^2, (\theta - a\theta^2 + \theta^3)/3\}$	1
B9	$v_3(a) = 1$ and $v_3(b) = 3$	7	$\{1, \theta, \theta^2, \theta^3/3\}$	5
B10	$v_3(a) \geq 2$ and $v_3(b) = 3$	9	$\{1, \theta, \theta^2/3, \theta^3/3^2\}$	3
B11	$v_3(a) = 0,\ v_3(b) \geq 4$ and $a^2 \not\equiv 1 \pmod 9$	3	$\{1, \theta, \theta^2, \theta^3\}$	3
B12	$v_3(a) = 0,\ v_3(b) \geq 4$ and $a^2 \equiv 1 \pmod 9$	3	$\{1, \theta, \theta^2, (\theta - a\theta^2 + \theta^3)/3\}$	1
B13	$v_3(a) = 1$ and $v_3(b) \geq 4$	7	$\{1, \theta, \theta^2, \theta^3/3\}$	5
B14	$v_3(a) = 2$ and $v_3(b) \geq 4$	11	$\{1, \theta, \theta^2/3, \theta^3/3^2\}$	5
B15	$v_3(a) = 0$, $b \equiv 6 \pmod 9$ and $a^4 \not\equiv 4b + 1 \pmod 9$	3	$\{1, \theta, \theta^2, \theta^3\}$	3
B16	$v_3(a) = 0$, $b \equiv 6 \pmod 9$ and $a^4 \equiv 4b + 1 \pmod 9$	3	$\{1, \theta, \theta^2, (\theta - a\theta^2 + \theta^3)/3\}$	1
B17	$v_3(a) = 0$, $b \equiv 3 \pmod 9$ and $a^4 \not\equiv 4b + 1 \pmod 9$	4	$\{1, \theta, \theta^2, \theta^3\}$	4

B18	$v_3(a) = 0$, $b \equiv 3 \pmod 9$ $a^4 \equiv 4b + 1 \pmod 9$ and $a^4 \not\equiv 4b + 1 \pmod{27}$	5	$\{1, \theta, \theta^2, (\theta - a\theta^2 + \theta^3)/3\}$	3
B19	$v_3(a) = 0$, $b \equiv 3 \pmod 9$ and $a^4 \equiv 4b + 1 \pmod{27}$	$s_3 \geq 6$	$\{1, \theta, (a\theta + \theta^2)/3, (x + y\theta + z\theta^2 + \theta^3)/3^m\}$ $m = [(s_3 - 2)/2]$ $4x \equiv 3a \pmod{3^m}$ $9a^2y \equiv 16b^2 \pmod{3^{m+2}}$ $3az \equiv -4b \pmod{3^{m+1}}$	$s_3 - 2[s_3/2]$

Table C

Case	Condition	s_p	$p(> 3)$-integral basis	$v_p(d(K))$
C1	$v_p(a) \geq 1, v_p(b) = 0$ or $v_p(a) = 0, v_p(b) \geq 1$	0	$\{1, \theta, \theta^2, \theta^3\}$	0
C2	$v_p(a) \geq 1, v_p(b) = 1$	3	$\{1, \theta, \theta^2, \theta^3\}$	3
C3	$v_p(a) = 1, v_p(b) \geq 2$	4	$\{1, \theta, \theta^2, \theta^3/p\}$	2
C4	$v_p(a) \geq 2, v_p(b) = 2$	6	$\{1, \theta, \theta^2/p, \theta^3/p\}$	2
C5	$v_p(a) = 2, v_p(b) \geq 3$	8	$\{1, \theta, \theta^2/p, \theta^3/p^2\}$	2
C6	$v_p(a) \geq 3, v_p(b) = 3$	9	$\{1, \theta, \theta^2/p, \theta^3/p^2\}$	3
C7	$v_p(ab) = 0$	s_p	$\{1, \theta, \theta^2, (x + y\theta + z\theta^2 + \theta^3)/p^m\}$	$s_p - 2[s_p/2]$

			$m = [s_p/2]$ $4x \equiv 3a \pmod{p^m}$ $9a^2y \equiv 16b^2 \pmod{p^m}$ $3az \equiv -4b \pmod{p^m}$	

Proof. We give the details of the proof in eight representative cases.

A13. $\nu_2(a) = 3$ and $\nu_2(b) = 2$. Then $s_2 = 12$. By Theorem 1.1, the element $\dfrac{x + y\theta + z\theta^2 + \theta^3}{2^2}$ is 2-integral for some integers x, y and z if and only if the congruences

$$X \equiv 0 \pmod{2^2},\ Y \equiv 0 \pmod{2^4},\ Z \equiv 0 \pmod{2^6},\ W \equiv 0 \pmod{2^8}$$

are satisfied. Since these congruences are satisfied for $x = 0$, $y = 2$, $z = 0$ then $\dfrac{2\theta + \theta^2 + \theta^3}{2^2}$ is a 2-integral element of K. We now show that

$$\frac{x + y\theta + z\theta^2 + \theta^3}{2^3} \tag{2.1}$$

is not a 2-integral element for any integers x, y and z. If it is a 2-integral element for some integers x, y and z, then by Theorem 1.1,

$$X \equiv 0 \pmod{2^3},\ Y \equiv 0 \pmod{2^6},\ Z \equiv 0 \pmod{2^9},\ W \equiv 0 \pmod{2^{12}}. \tag{2.2}$$

It follows from $X \equiv 0 \pmod{2^3}$ and $W \equiv 0 \pmod{2^{12}}$ that $x \equiv 0 \pmod 2$ and $y \equiv 0 \pmod 2$, respectively. So, $x = 2r$ and $y = 2s$ for some integers r and s. From $Y \equiv 0 \pmod{2^6}$ we obtain, $z \equiv r \pmod 2$, and so $z = r + 2t$ for some integer t. Then from $Z \equiv 0 \pmod{2^9}$ and $W \equiv 0 \pmod{2^{12}}$, we see that $r \equiv 0 \pmod 2$ and $s \equiv 1 \pmod 2$, respectively. Hence

$$x = 4R,\quad y = 2 + 4S,\quad z = 2R + 2t$$

for some integers R, S and t. Substituting x, y and z into the congruences in (2.2), we obtain $Y \equiv 32 \equiv 0 \pmod{2^6}$ which is a contradiction. Hence the element given in (2.1) is not 2-integral. Similarly, it can be easily verified that $\theta^2/2$ is a 2-integral element but the element $(x + y\theta + \theta^2)/2^2$ cannot be 2-integral for any integers x and y. Note that $(x + \theta)/2$ cannot be a 2-integral element for any x either. Thus by Theorem 1.2,

$$\left\{1,\ \theta,\ \frac{\theta^2}{2},\ \frac{2\theta + \theta^3}{2^2}\right\}$$

is a 2-integral basis for K and

$$v_2(K) = s_2 - 2(i + j + k) = 12 - 2(1 + 2) = 6.$$

A25. $v_2(a) = 2$, $b \equiv 3 \pmod{16}$ and $s_2 \equiv 0 \pmod 2$. Then $s_2 \geq 12$. It can be easily verified that $\dfrac{x + \theta}{2}$ is not a 2-integral element for any integer x, $\dfrac{1 + \theta^2}{2}$ is a 2-integral element and $\dfrac{x + y\theta + \theta^2}{2^2}$ is not a 2-integral element for any pair of integers x, y. So by Theorem 1.2, a 2-integral basis for K is of the form

$$\left\{1,\ \theta,\ \frac{1 + \theta^2}{2},\ \frac{x + y\theta + z\theta^2 + \theta^3}{2^m}\right\},$$

where m is the largest integer such that $\dfrac{x + y\theta + z\theta^2 + \theta^3}{2^m}$ is 2-integral, and

$$v_2(d(K)) = s_2 - 2(m + 1).$$

Using MAPLE, we set $w = 1$, $X = 4x - 3a$, $U = 3^2a^2y - 2^4b^2$ and $V = 3az + 4b$ in Theorem 1.1, and obtain

$$Y = \frac{1}{2^3 3^2 a^2}[3^3a^2X^2 + 2^3(U + 2bV)V + \Delta],$$

$$Z = \frac{1}{2^4 3^6 a^5}[3^6 a^5 X^3 - 2^4 U^3 + 2^4 3^3 a^4 V^3 + 2^4 3^4 a^3 b V^2 X - 2^6 3 b U^2 V + 2^3 3^4 a^3 UVX - 2^3 3 \Delta UV + 3^4 a^3 \Delta X + 2^4 3 b \Delta U - 2^6 3 b^2 \Delta V + 2\Delta^2],$$

$$W = \frac{1}{2^8 3^8 a^8}[3^8 a^8 X^4 + 2^5 3^6 a^6 b V^2 X^2 + 2^4 3^6 a^6 UVX^2 + 2^6 3^5 a^7 V^3 X - 2^8 3^3 a^3 b U^2 VX - 2^6 3^2 a^3 U^3 X + 2^8 3^4 a^4 b^2 V^4 - 2^8 3^3 a^4 bUV^3 + 2^8 b U^4 - 2^5 3^3 a^3 \Delta UVX - 2^6 3^3 a^4 \Delta V^3 + 2^6 \Delta U^3 + 2 3^6 a^6 \Delta X^2 - 2^8 3^3 a^3 b^2 \Delta VX + 2^6 3^3 a^3 b \Delta UX + 2^5 3^5 a^4 b \Delta V^2 + 2^4 3^4 a^4 \Delta UV + 2^9 3 b^2 \Delta U^2 + 2^3 3^2 a^3 \Delta^2 X + 2^6 b \Delta^2 U + \Delta^3].$$

Let $m = \frac{s_2 - 8}{2}$. Note that $2^{2m+8} \,\|\, \Delta$. Define integers x, y and z by

$$X \equiv 0 \pmod{2^{m+2}}, \quad U \equiv 0 \pmod{2^{m+4}} \quad \text{and} \quad V \equiv 0 \pmod{2^{m+2}},$$

respectively. Then substituting

$$X = r2^{m+2}, \quad U = s2^{m+4}, \quad V = t2^{m+2} \quad \text{and} \quad \Delta = 2^{2m+8} + k2^{2m+9}$$

into Y, Z and W with MAPLE, we obtain

$$Y \equiv 0 \pmod{2^{2m}}, \quad Z \equiv 0 \pmod{2^{3m}} \text{ and } W \equiv 0 \pmod{2^{4m}}.$$

Thus, by Theorem 1.1, $\frac{x + y\theta + z\theta^2 + \theta^3}{2^m}$ is a 2-integral element of K, and by Theorem 1.2,

$$\nu_2(d(K)) \le 6.$$

Let $m = \frac{s_2 - 6}{2}$. Note that $2^{2m+6} \,\|\, \Delta$. We now show that the element $\frac{x + y\theta + z\theta^2 + \theta^3}{2^m}$ cannot be 2-integral for any integers x, y and z. It is 2-integral if and only if

$$X \equiv 0 \pmod{2^m}, \quad Y \equiv 0 \pmod{2^{2m}}, \quad Z \equiv 0 \pmod{2^{3m}}, \quad W \equiv 0 \pmod{2^{4m}}.$$

It follows from $Y \equiv 0 \pmod{2^{2m}}$ and $Z \equiv 0 \pmod{2^{3m}}$ that

$$2^{2m+7} \mid 3^3a^2X^2 + 2^3(U + 2bV)V + \Delta \tag{2.3}$$

and

$$2^{3m+14} \mid 3^6a^5X^3 - 2^4U^3 + 2^43^3a^4V^3 + 2^43^4a^3bV^2X - 2^63bU^2V - 2^33\Delta UV$$

$$+ 2^33^4a^3UVX + 3^4a^3\Delta X + 2^43b\Delta U - 2^63b^2\Delta V + 2\Delta^2, \tag{2.4}$$

respectively. We consider the following three subcases.

(i) $2^{m+2} \mid X$, (ii) $2^{m+1} \parallel X$, (iii) $2^m \parallel X$.

(i) Let $2^{m+2} \mid X$. It follows from (2.3) that

$$2^{2m+3} \parallel (U + 2bV)V. \tag{2.5}$$

If $2^{m+2} \parallel U$, then the expression (2.5) would not hold. Hence either $2^{m+1-i} \parallel U$ or $2^{m+3+i} \parallel U$, where $i \geq 0$.

If $2^{m+1-i} \parallel U$, then either $2^{m-i} \parallel V$ or $2^{m+2+i} \parallel V$. It follows from (2.4) that $2^{3m-3i+8} \mid 2^4U^3$, which is a contradiction.

If $2^{m+3+i} \parallel U$, then $2^{m+1} \parallel V$. Thus we have

$$2^{m+2} \mid X, \quad 2^{m+3} \mid U, \quad 2^{m+1} \parallel V \quad \text{and} \quad 2^{2m+6} \parallel \Delta.$$

Substituting

$$X = r2^{m+2}, \quad U = s2^{m+3},$$

$$V = 2^{m+1} + t2^{m+2}, \quad \Delta = 2^{2m+6} + k2^{2m+7}$$

into Y, Z and W with MAPLE, we obtain $2^{4m} \nmid W$, which is a contradiction.

(ii) Let $2^{m+1} \parallel X$. It follows from (2.3) that

$$2^{2m+4} \parallel (U + 2bV)V. \tag{2.6}$$

If $2^{m+3} \mid U$, then the expression (2.6) would not hold. Hence $2^{m+2-i} \parallel U$, where $i \geq 0$. Then (2.6) implies that either $2^{m+1-i} \parallel V$ or $2^{m+2+i} \parallel V$. It follows from (2.4) that $2^{3m-3i+11} \mid 2^4 U^3$, which is a contradiction.

(iii) Let $2^m \parallel X$. It follows from (2.3) that

$$2^{2m+1} \parallel (U + 2bV)V. \tag{2.7}$$

If $2^{m+1} \parallel U$, then the expression (2.7) would not hold. Hence either $2^{m-i} \parallel U$ or $2^{m+2+i} \parallel U$, where $i \geq 0$.

If $2^{m-i} \parallel U$, then (2.7) implies that either $2^{m-1-i} \parallel V$ or $2^{m+1+i} \parallel V$. Then it follows from (2.4) that $2^{3m-3i+5} \mid 2^4 U^3$, which is a contradiction.

If $2^{m+2+i} \parallel U$, then (2.7) implies that $2^m \parallel V$. So we have

$$2^m \parallel X, \quad 2^{m+2+i} \parallel U, \quad 2^m \parallel V \quad \text{and} \quad 2^{2m+6} \parallel \Delta.$$

Substituting

$$X = 2^m + r2^{m+1}, \quad U = 2^{m+2+i} + s2^{m+3+i},$$

$$V = 2^m + t2^{m+1}, \quad \Delta = 2^{2m+6} + k2^{2m+7}$$

into $Y \equiv 0 \pmod{2^{2m}}$ we obtain

$$1 + 2^i + 2^{1+i}(s + t) \equiv 0 \pmod{4}.$$

Hence $i = 0$ and $s + t \equiv 1 \pmod{2}$. Thus we have

$$2^m \parallel X, \quad 2^{m+2} \parallel U, \quad 2^m \parallel V, \quad U_2 V_2 \equiv 3 \pmod{4} \quad \text{and} \quad 2^{2m+6} \parallel \Delta,$$

where $U_2 = U/2^{m+2}$ and $V_2 = V/2^m$. Substituting

$$X = 2^m + r2^{m+1}, \quad U = 2^{m+2} + s2^{m+3},$$

$$V = 2^m + t2^{m+1}, \quad \Delta = 2^{2m+6} + k2^{2m+7}, \quad s + t \equiv 1 \pmod{2}$$

into Z with MAPLE, we obtain $2^{3m} \nmid Z$, which is a contradiction.

Thus a 2-integral basis for K is

$$\left\{1,\ \theta,\ \frac{1+\theta^2}{2},\ \frac{x+y\theta+z\theta^2+\theta^3}{2^m}\right\}$$

and

$$m=(s_2-8)/2 \quad \text{and} \quad \nu_2(d(K))=s_2-2(m+1)=6,$$

where the integers x, y and z are given by

$$4x-3a\equiv 0 \pmod{2^{m+2}},$$

$$3^2a^2y-2^4b^2\equiv 0 \pmod{2^{m+4}},$$

$$3az+4b\equiv 0 \pmod{2^{m+2}}.$$

Cases A26, A28 and A30. $\nu_2(a)=2$, $b\equiv 3 \pmod{16}$ and $s_2\equiv 1 \pmod 2$. Then $s_2\geq 13$.

As in case A25, a 2-integral basis for K is of the form

$$\left\{1,\ \theta,\ \frac{1+\theta^2}{2},\ \frac{x+y\theta+z\theta^2+\theta^3}{2^m}\right\},$$

where m is the largest integer such that $\dfrac{x+y\theta+z\theta^2+\theta^3}{2^m}$ is 2-integral, and

$$\nu_2(d(K))=s_2-2(m+1).$$

Let $m=\dfrac{s_2-7}{2}$. Define integers x, y and z by

$$X\equiv 0 \pmod{2^{m+2}},\quad U\equiv 0 \pmod{2^{m+4}} \quad \text{and} \quad V\equiv 0 \pmod{2^{m+2}},$$

respectively. Then substituting

$$X=r2^{m+2},\quad U=s2^{m+4},\quad V=t2^{m+2} \quad \text{and} \quad \Delta=2^{2m+7}+k2^{2m+8}$$

into Y, Z and W with MAPLE, we obtain

$$Y\equiv 0 \pmod{2^{2m}},\quad Z\equiv 0 \pmod{2^{3m}} \quad \text{and} \quad W\equiv 0 \pmod{2^{4m}}.$$

Hence, by Theorem 1.1, $\dfrac{x + y\theta + z\theta^2 + \theta^3}{2^m}$ is a 2-integral element, and by Theorem 1.2, $\nu_2(d(K)) \le 5$.

Now let $m = \dfrac{s_2 - 3}{2}$. Note that $2^{2m+3} \parallel \Delta$. It follows from $Y \equiv 0 \pmod{2^{2m}}$ that

$$2^{2m} \parallel (U + 2bV)V. \tag{2.8}$$

It follows from (2.8) that $2^{m+1} \nmid U$. So $2^{m-i} \parallel U$, where $i \ge 0$. Then (2.8) implies that either $2^{m-1-i} \parallel V$ or $2^{m+i} \parallel V$. Then $Z \equiv 0 \pmod{2^{3m}}$ implies that $2^{3m-3i+5} \mid 2^4 U^3$, which is a contradiction. Thus, by Theorem 1.2, $\nu_2(d(K)) \ge 3$, and so,

$$\nu_2(d(K)) = 3 \text{ or } 5.$$

Let $m = \dfrac{s_2 - 5}{2}$. Note that $2^{2m+5} \parallel \Delta$. As in case A25, it follows from $Y \equiv 0 \pmod{2^{2m}}$ and $Z \equiv 0 \pmod{2^{3m}}$ that

$$2^{2m+7} \mid 3^3 a^2 X^2 + 2^3 (U + 2bV)V + \Delta \tag{2.9}$$

and

$$2^{3m+14} \mid 3^6 a^5 X^3 - 2^4 U^3 + 2^4 3^3 a^4 V^3 + 2^4 3^4 a^3 b V^2 X - 2^6 3 b U^2 V$$
$$- 2^3 3 \Delta UV + 2^3 3^4 a^3 UVX + 3^4 a^3 \Delta X + 2^4 3 b \Delta U - 2^6 3 b^2 \Delta V + 2\Delta^2, \tag{2.10}$$

respectively.

If $2^{m+1} \mid X$, then (2.9) implies that

$$2^{2m+2} \parallel (U + 2bV)V. \tag{2.11}$$

If $2^{m+2} \mid U$, then (2.11) would not hold. Hence $2^{m+1-i} \parallel U$, where $i \ge 0$. Then (2.11) implies that either $2^{m-i} \parallel V$ or $2^{m+1+i} \parallel V$. Then it follows from (2.10) that $2^{3m-3i+8} \mid 2^4 U^3$, which is a contradiction. So $2^{m+1} \nmid X$.

We now assume that $2^m \parallel X$. It follows from (2.9) that

$$2^{2m+1} \parallel (U + 2bV)V. \tag{2.12}$$

If $2^{m+1} \parallel U$, then (2.12) would not hold. Hence either $2^{m-i} \parallel U$ or $2^{m+2+i} \parallel U$, where $i \geq 0$.

If $2^{m-i} \parallel U$, then (2.12) implies that either $2^{m-1-i} \parallel V$ or $2^{m+1+i} \parallel V$. Then it follows from (2.10) that $2^{3m-3i+5} \mid 2^4 U^3$, which is a contradiction.

If $2^{m+2+i} \parallel U$, then it follows from (2.12) that $2^m \parallel V$. Thus we have

$$2^m \parallel X, \quad 2^{m+2+i} \parallel U, \quad 2^m \parallel V \quad \text{and} \quad 2^{2m+5} \parallel \Delta.$$

Substituting

$$X = 2^m + r2^{m+1}, \quad U = 2^{m+2+i} + s2^{m+3+i},$$

$$V = 2^m + t2^{m+1}, \quad \Delta = 2^{2m+5} + k2^{2m+6}$$

into $Y \equiv 0 \pmod{2^{2m}}$, we obtain

$$\Delta_2 + 3 + 2^i + 2^{1+i}(s + t) \equiv 0 \pmod 4. \tag{2.13}$$

If $\Delta_2 \equiv 1 \pmod 4$, then it follows from (2.13) that $i \geq 2$ that is $2^{m+4} \mid U$. If $\Delta_2 \equiv 3 \pmod 4$, then it follows from (2.13) that $i = 1$ that is $2^{m+3} \parallel U$.

We have shown that the only cases such that $Y \equiv 0 \pmod{2^{2m}}$ with a possibility of $2^{3m} \mid Z$ and $2^{4m} \mid W$ are

(i) $2^m \parallel X$, $2^{m+4} \mid U$, $2^m \parallel V$ and $\Delta_2 \equiv 1 \pmod 4$,

(ii) $2^m \parallel X$, $2^{m+3} \parallel U$, $2^m \parallel V$ and $\Delta_2 \equiv 3 \pmod 4$.

The first one corresponds to Case A26, and the second one corresponds to Cases A28 and A30.

Case A26. $\nu_2(a) = 2$, $b \equiv 3 \pmod{16}$, $s_2 \equiv 1 \pmod 2$ and $\Delta_2 \equiv 1 \pmod 4$. Then $s_2 \geq 13$. For $m = (s_2 - 5)/2$, we substitute

$$X = 2^m + r2^{m+1}, \quad U = s2^{m+4},$$

$$V = 2^m + t2^{m+1}, \quad \Delta = 2^{2m+5} + k2^{2m+7}$$

into Y, Z and W with MAPLE, and obtain $2^{3m} \nmid Z$. Thus for this case,

$$\left\{1,\ \theta,\ \frac{1+\theta^2}{2},\ \frac{x + y\theta + z\theta^2 + \theta^3}{2^m}\right\}$$

is a 2-integral basis for K, and

$$m = (s_2 - 7)/2 \quad \text{and} \quad \nu_2(d(K)) = s_2 - 2(m+1) = 5,$$

where the integers x, y and z are given by

$$4x - 3a \equiv 0 \pmod{2^{m+2}},$$

$$3^2a^2y - 2^4b^2 \equiv 0 \pmod{2^{m+4}},$$

$$3az + 4b \equiv 0 \pmod{2^{m+2}}.$$

Case A28. $a = 4 + 16A$, $b = 3 + 16B$, $s_2 \equiv 1 \pmod 2$, $\Delta_2 \equiv 3 \pmod 4$ and $A + B \equiv 0 \pmod 4$. Then $s_2 \geq 15$. For $m = (s_2 - 5)/2$, we substitute

$$X = 2^m + r2^{m+1}, \quad U = 2^{m+3} + s2^{m+4},$$

$$V = 2^m + t2^{m+1}, \quad \Delta = 3 \cdot 2^{2m+5} + k2^{2m+7},$$

$$r + t \equiv 0 \pmod 2, \quad A + B \equiv 0 \pmod 4$$

into Y, Z and W with MAPLE, and obtain $2^{2m} \mid Y$, $2^{3m} \mid Z$ and $2^{4m} \mid W$. Thus for this case,

$$\left\{1,\ \theta,\ \frac{1+\theta^2}{2},\ \frac{x + y\theta + z\theta^2 + \theta^3}{2^m}\right\}$$

is a 2-integral basis for K, and

$$m = (s_2 - 5)/2 \quad \text{and} \quad v_2(d(K)) = s_2 - 2(m+1) = 3,$$

where the integers x, y and z are given by

$$4x - 3a = 2^m + r2^{m+1},$$

$$3^2a^2y - 2^4b^2 = 2^{m+3} + s2^{m+4},$$

$$3az + 4b = 2^m + t2^{m+1},$$

$$r + t \equiv 0 \pmod 2.$$

Case A30. $a = 12 + 16A$, $b = 3 + 16B$, $s_2 \equiv 1 \pmod 2$, $\Delta_2 \equiv 3 \pmod 4$ and $A - B \equiv 3 \pmod 4$. Then $s_2 \geq 15$. For $m = (s_2 - 5)/2$, we substitute

$$X = 2^m + r2^{m+1}, \quad U = 2^{m+3} + s2^{m+4},$$

$$V = 2^m + t2^{m+1}, \quad \Delta = 3 \cdot 2^{2m+5} + k2^{2m+7},$$

$$r + t \equiv 1 \pmod 2), \quad A - B \equiv 3 \pmod 4)$$

into Y, Z and W with MAPLE, and obtain $2^{2m} \mid Y$, $2^{3m} \mid Z$ and $2^{4m} \mid W$. Thus for this case,

$$\left\{1, \theta, \frac{1+\theta^2}{2}, \frac{x + y\theta + z\theta^2 + \theta^3}{2^m}\right\}$$

is a 2-integral basis for K, and

$$m = \frac{s_2 - 5}{2} \quad \text{and} \quad v_2(d(K)) = s_2 - 2(m+1) = 3,$$

where the integers x, y and z are given by

$$4x - 3a = 2^m + r2^{m+1},$$

$$3^2a^2y - 2^4b^2 = 2^{m+3} + s2^{m+4},$$

$$3az + 4b = 2^m + t2^{m+1},$$

$$r + t \equiv 1 \pmod 2.$$

Case B16. $\nu_3(a) = 0$, $b \equiv 6 \pmod 9$ and $a^4 \equiv 4b + 1 \pmod 9$. Then $s_3 = 3$. Substituting $x = 0$, $y = 1$ and $z = -a$ into X, Y, Z and W, we obtain

$$X \equiv 0 \pmod 3),\ Y \equiv 0 \pmod{3^2},\ Z \equiv 0 \pmod{3^3},\ W \equiv 0 \pmod{3^4}.$$

Hence $\frac{\theta - a\theta^2 + \theta^3}{3}$ is a 3-integral element of K. Thus

$$\left\{1, \theta, \theta^2, \frac{\theta - a\theta^2 + \theta^3}{3}\right\}$$

is a 3-integral basis for K and $\nu_3(d(K)) = 3 - 2 = 1$.

Case B19. $\nu_3(a) = 0$, $b \equiv 3 \pmod 9$ and $a^4 \equiv 4b + 1 \pmod{27}$. Then $s_3 \geq 6$. It can be easily verified that $\frac{a\theta + \theta^2}{3}$ is a 3-integral element of K and the element $\frac{x + y\theta + \theta^2}{3^2}$ cannot be 3-integral for any integers x and y. Let $m = [(s_3 - 2)/2]$. Define integers x, y and z by

$$X \equiv 0 \pmod{3^m},\quad U \equiv 0 \pmod{3^{m+2}} \quad \text{and} \quad V \equiv 0 \pmod{3^{m+1}},$$

respectively. Then substituting

$$X = r3^m,\ U = s3^{m+2},\ V = t3^{m+1},\ \Delta = \begin{cases} 3^{2m+2} + k2^{2m+3}, & \text{if } s_3 \text{ is even}, \\ 3^{2m+3} + k2^{2m+4}, & \text{if } s_3 \text{ is odd}, \end{cases}$$

into Y, Z and W with MAPLE, we obtain

$$Y \equiv 0 \pmod{3^{2m}},\quad Z \equiv 0 \pmod{3^{3m}} \quad \text{and} \quad W \equiv 0 \pmod{3^{4m}}.$$

Hence, by Theorem 1.1, $\frac{x + y\theta + z\theta^2 + \theta^3}{3^m}$ is a 3-integral element of K. Thus, by Theorem 1.2,

$$\left\{1, \theta, \frac{a\theta + \theta^2}{3}, \frac{x + y\theta + z\theta^2 + \theta^3}{3^m}\right\}$$

is a 3-integral basis for K, and

$$m = [(s_3 - 2)/2] \text{ and } \nu_3(d(K)) = s_3 - 2(1 + m) = s_3 - 2[s_3/2],$$

where the integers x, y and z are given by

$$4x - 3a \equiv 0 \pmod{3^m},$$

$$3^2a^2y - 2^4b^2 \equiv 0 \pmod{3^{m+2}},$$

$$3az + 4b \equiv 0 \pmod{3^{m+1}}.$$

Case C7. $\nu_p(ab) = 0$. Then $s_p \geq 0$. Let $m = [s_p/2]$. Note that $p^{2m} \mid \Delta$. Define integers x, y, z by

$$X \equiv 0 \pmod{p^m}, \quad U \equiv 0 \pmod{p^m} \text{ and } V \equiv 0 \pmod{p^m},$$

respectively. Then substituting

$$X = rp^m,\ U = sp^m,\ V = tp^m,\ \Delta = \begin{cases} p^{2m} + k2^{2m+1}, & \text{if } s_p \text{ is even,} \\ p^{2m+1} + k2^{2m+2}, & \text{if } s_p \text{ is odd,} \end{cases}$$

into Y, Z and W with MAPLE, we obtain

$$Y \equiv 0 \pmod{p^{2m}}, \quad Z \equiv 0 \pmod{p^{3m}} \text{ and } W \equiv 0 \pmod{p^{4m}}.$$

Hence, by Theorem 1.1, $\dfrac{x + y\theta + z\theta^2 + \theta^3}{p^m}$ is a p-integral element of K. Thus, by Theorem 1.2,

$$\left\{1, \theta, \theta^2, \frac{x + y\theta + z\theta^2 + \theta^3}{p^m}\right\}$$

is a p-integral basis of K, and

$$m = [s_p/2] \text{ and } \nu_p(d(K)) = s_p - 2m = s_p - 2[s_p/2],$$

where the integers x, y and z are given by

$$4x - 3a \equiv 0 \pmod{p^m},$$

$$3^2a^2y - 2^4b^2 \equiv 0 \pmod{p^m},$$

$$3az + 4b \equiv 0 \pmod{p^m}.$$

3. An Integral Basis and the Discriminant of a Quartic Field Defined by a Trinomial

The following theorem follows from Theorem 1.3 and Theorem 2.1.

Theorem 3.1. *Let $K = \mathbb{Q}(\theta)$ be a quartic field, where θ is a root of the irreducible trinomial* (1.1). *If there are no rational primes dividing $i(\theta)$, then $\{1, \theta, \theta^2, \theta^3\}$ is an integral basis of K. Let $p_1, p_2, \ldots, p_s$ be the distinct primes dividing $i(\theta)$. Let*

$$\left\{1,\ \theta,\ \frac{u_r + v_r\theta + \theta^2}{p_r^{j_r}},\ \frac{x_r + y_r\theta + z_r\theta^2 + \theta^3}{p_r^{k_r}}\right\}$$

be a p_r-integral basis of K $(r = 1, 2, \ldots, s)$ as given in Theorem 1.2. *Define the integers u, v, x, y, z by*

$$u \equiv u_r \pmod{p_r^{j_r}},\quad v \equiv v_r \pmod{p_r^{j_r}},\quad r = 1, 2, \ldots, s,$$

$$x \equiv x_r \pmod{p_r^{k_r}},\quad y \equiv y_r \pmod{p_r^{k_r}},\quad z \equiv z_r \pmod{p_r^{k_r}},\quad r = 1, 2, \ldots, s,$$

and let

$$S = \prod_{r=1}^{s} p_r^{j_r},\quad T = \prod_{r=1}^{s} p_r^{k_r}.$$

Then an integral basis of K is

$$\left\{1,\ \theta,\ \frac{u + v\theta + \theta^2}{S},\ \frac{x + y\theta + z\theta^2 + \theta^3}{T}\right\},$$

and the discriminant of K is

$$d(K) = \operatorname{sgn}(\Delta) 2^{\alpha} 3^{\beta} \prod_{\substack{p>3 \\ p \nmid ab \\ s_p \text{ odd}}} p \prod_{\substack{p>3 \\ p \| a,\ p^2 | b \\ \text{or } p^2 | a,\ p^2 \| b \\ \text{or } p^2 \| a,\ p^3 | b}} p^2 \prod_{\substack{p>3 \\ p | a,\ p \| b \\ \text{or } p^3 | a,\ p^3 \| b}} p^3,$$

where

$$\alpha = \begin{cases} 0 & \text{if } \nu_2(a) = 0, \\ 2 & \text{if } \nu_2(a) = 1 \text{ and } b \equiv 1(4) \\ & \text{or } \nu_2(a) = 1 \text{ and } \nu_2(b) \geq 2 \\ & \text{or } \nu_2(a) = 2 \text{ and } \nu_2(b) \geq 3 \\ & \text{or } \nu_2(a) \geq 3 \text{ and } b \equiv 7(8), \\ 3 & \text{if } \nu_2(a) = 2,\ b \equiv 3(16),\ \Delta_2 \equiv 3(4) \text{ and } s_2 \text{ odd} \\ & \text{or } \nu_2(a) = 2,\ b \equiv 11(16) \text{ and } \Delta_2 \equiv 1(4), \\ 4 & \text{if } \nu_2(a) = 1 \text{ and } b \equiv 3(4) \\ & \text{or } \nu_2(a) = 1 \text{ and } \nu_2(b) = 1 \\ & \text{or } \nu_2(a) = 2 \text{ and } \nu_2(b) = 2 \\ & \text{or } \nu_2(a) \geq 3 \text{ and } b \equiv 3(8) \\ & \text{or } a = 16A,\ b = 4 + 16B \text{ and } A + B \equiv 0(2), \\ 5 & \text{if } \nu_2(a) = 2,\ b \equiv 11(16) \text{ and } \Delta_2 \equiv 3(4) \\ & \text{or } \nu_2(a) = 2,\ b \equiv 3(16),\ \Delta_2 \equiv 1(4) \text{ and } s_2 \text{ odd}, \\ 6 & \text{if } \nu_2(a) = 3 \text{ and } \nu_2(b) = 2, 3 \\ & \text{or } \nu_2(a) \geq 4 \text{ and } b \equiv 12(16) \\ & \text{or } \nu_2(a) = 2 \text{ and } b \equiv 7(8) \\ & \text{or } \nu_2(a) = 2,\ b \equiv 3(16) \text{ and } s_2 \text{ even} \\ & \text{or } a = 16A,\ b = 4 + 16B \text{ and } A + B \equiv 1(2), \\ 8 & \text{if } \nu_2(a) = 2 \text{ and } \nu_2(b) = 1 \\ & \text{or } \nu_2(a) \geq 3 \text{ and } b \equiv 1(4), \\ 9 & \text{if } \nu_2(a) = 2 \text{ and } b \equiv 1(4), \\ 10 & \text{if } \nu_2(a) = 4 \text{ and } \nu_2(b) = 3, \\ 11 & \text{if } \nu_2(a) \geq 3 \text{ and } \nu_2(b) = 1 \\ & \text{or } \nu_2(a) \geq 5 \text{ and } \nu_2(b) = 3, \end{cases}$$

and

$$\beta = \begin{cases} 0 & \text{if } \nu_3(b) = 0 \\ & \text{or } \nu_3(a) = 0,\ b \equiv 3(9),\ a^4 \equiv 4b + 1(27) \text{ and } s_3 \text{ even}, \\ 1 & \text{if } \nu_3(a) = 0,\ a^2 \equiv 1(9) \text{ and } \nu_3(b) \geq 2 \\ & \text{or } \nu_3(a) = 0,\ b \equiv 6(9) \text{ and } a^4 \equiv 4b + 1(9) \\ & \text{or } \nu_3(a) = 0,\ b \equiv 3(9),\ a^4 \equiv 4b + 1(27) \text{ and } s_3 \text{ odd}, \\ 2 & \text{if } \nu_3(a) \geq 2 \text{ and } \nu_3(b) = 2, \\ 3 & \text{if } \nu_3(a) \geq 1 \text{ and } \nu_3(b) = 1 \\ & \text{or } \nu_3(a) = 0,\ a^2 \not\equiv 1(9) \text{ and } \nu_3(b) \geq 2 \\ & \text{or } \nu_3(a) \geq 2 \text{ and } \nu_3(b) = 3 \\ & \text{or } \nu_3(a) = 0,\ b \equiv 6(9) \text{ and } a^4 \not\equiv 4b + 1(9) \\ & \text{or } \nu_3(a) = 0,\ b \equiv 3(9),\ a^4 \equiv 4b + 1(9) \text{ and } a^4 \not\equiv 4b + 1(27), \\ 4 & \text{if } \nu_3(a) = 1 \text{ and } \nu_3(b) = 2 \\ & \text{or } \nu_3(a) = 0,\ b \equiv 3(9),\ a^4 \not\equiv 4b + 1(9), \\ 5 & \text{if } \nu_3(a) = 1 \text{ and } \nu_3(b) = 3 \\ & \text{or } \nu_3(a) = 1, 2 \text{ and } \nu_3(b) \geq 4. \end{cases}$$

Remark 3.1. Llorente, Nart and Vila [4] determined the discriminant of a number field defined by an irreducible trinomial

$$x^n + ax^s + b, \quad a, b \in Z$$

in terms of n, s, a, b except for some cases. When $n = 4$ and $s = 1$, the work of Llorente, Nart and Vila [4] does not cover the cases given in the following theorem which is a special case of Theorem 3.1.

Theorem 3.2. *Let* $K = \mathbb{Q}(\theta)$ *be a quartic field, where* θ *is a root of the irreducible trinomial* (1.1).

(i) *If* $\nu_2(a) \geq 1$ *and* $\nu_2(b) = 0$, *then*

$$\nu_2(d(K)) = \begin{cases} 2 & \text{if } \nu_2(a) = 1 \text{ and } b \equiv 1(4) \\ & \text{or } \nu_2(a) \geq 3 \text{ and } b \equiv 7(8), \\ 3 & \text{if } \nu_2(a) = 2,\ b \equiv 3(16),\ \Delta_2 \equiv 3(4) \text{ and } s_2 \text{ odd} \\ & \text{or } \nu_2(a) = 2,\ b \equiv 11(16) \text{ and } \Delta_2 \equiv 1(4), \\ 4 & \text{if } \nu_2(a) = 1 \text{ and } b \equiv 3(4) \\ & \text{or } \nu_2(a) \geq 3 \text{ and } b \equiv 3(8), \\ 5 & \text{if } \nu_2(a) = 2,\ b \equiv 11(16) \text{ and } \Delta_2 \equiv 3(4) \\ & \text{or } \nu_2(a) = 2,\ b \equiv 3(16),\ \Delta_2 \equiv 1(4) \text{ and } s_2 \text{ odd}, \\ 6 & \text{if } \nu_2(a) = 2 \text{ and } b \equiv 7(8) \\ & \text{or } \nu_2(a) = 2,\ b \equiv 3(16) \text{ and } s_2 \text{ even}, \\ 8 & \text{if } \nu_2(a) \geq 3 \text{ and } b \equiv 1(4), \\ 9 & \text{if } \nu_2(a) = 2 \text{ and } b \equiv 1(4). \end{cases}$$

(ii) *If* $\nu_2(a) \geq 3$ *and* $\nu_2(b) = 2$, *then*

$$\nu_2(d(K)) = \begin{cases} 4 & \text{if } a = 16A,\ b = 4 + 16B \text{ and } A + B \equiv 0(2), \\ 6 & \text{if } \nu_2(a) = 3 \text{ and } \nu_2(b) = 2 \\ & \text{or } \nu_2(a) \geq 4 \text{ and } b \equiv 12(16) \\ & \text{or } a = 16A,\ b = 4 + 16B \text{ and } A + B \equiv 1(2). \end{cases}$$

(iii) *If* $v_3(a) = 0$ *and* $v_3(b) \geq 1$, *then*

$$v_3(d(K)) = \begin{cases} 0 & \text{if } v_3(a) = 0,\ b \equiv 3(9),\ a^4 \equiv 4b + 1(27) \text{ and } s_3 \text{ even}, \\ 1 & \text{if } v_3(a) = 0,\ v_3(b) \geq 2 \text{ and } a^2 \equiv 1(9) \\ & \text{or } v_3(a) = 0,\ b \equiv 6(9) \text{ and } a^4 \equiv 4b + 1(9) \\ & \text{or } v_3(a) = 0,\ b \equiv 3(9),\ a^4 \equiv 4b + 1(27) \text{ and } s_3 \text{ odd}, \\ 3 & \text{if } v_3(a) = 0,\ v_3(b) \geq 2 \text{ and } a^2 \not\equiv 1(9) \\ & \text{or } v_3(a) = 0,\ b \equiv 6(9) \text{ and } a^4 \not\equiv 4b + 1(9) \\ & \text{or } v_3(a) = 0,\ b \equiv 3(9),\ a^4 \equiv 4b + 1(9) \text{ and } a^4 \not\equiv 4b + 1(27), \\ 4 & \text{if } v_3(a) = 0,\ b \equiv 3(9),\ a^4 \not\equiv 4b + 1(9). \end{cases}$$

In the remaining cases the evaluation of $d(K)$ by Llorente, Nart and Vila [4] agrees with that in Theorem 3.1.

Remark 3.2. Llorente, Nart and Vila [5] determined the discriminant of a number field defined by an irreducible trinomial

$$x^{p^m} + ax + b, \quad a, b \in \mathbb{Z}.$$

When $p = 2$ and $m = 2$, the work of Llorente, Nart and Vila [5] does not cover part (iii) in Theorem 3.2. In the remaining cases the evaluation of $d(K)$ by Llorente, Nart and Vila [5] agrees with that in Theorem 3.2.

Remark 3.3. The discriminant of a cubic field was completely determined in [3] by Llorente and Nart, and then in [1] by Alaca using p-integral bases.

Example 3.1. Let $K = \mathbb{Q}(\theta)$, where $\theta^4 + a\theta + b = 0$. Let $a = 48 = 2^4 \cdot 3$ and $b = 188 = 2^2 \cdot 47$. Since $v_2(a) = 4$ and $b \equiv 12 \pmod{16}$, by case A16, a 2-integral basis for K is

$$\left\{1, \theta, \frac{2 + \theta^2}{2^2}, \frac{2\theta + \theta^3}{2^2}\right\}.$$

Since $v_3(b) = 0$, by case B1, a 3-integral basis for K is

$$\{1, \theta, \theta^2, \theta^3\}.$$

Since $\nu_{47}(a) = 0$ and $\nu_{47}(b) = 1$, by case C1, a 47-integral basis is

$$\{1,\ \theta,\ \theta^2,\ \theta^3\}.$$

Since $\nu_5(ab) = 0$, we find a 5-integral basis for K using case C7. Note that

$$\Delta = 2^8 b^3 - 3^3 a^4 = 2^{14} \cdot 5^2 \cdot 3803.$$

So, $s_5 = 2$ and $m = s_5/2 = 2/2 = 1$. We need to solve the congruences

$$4x \equiv 3a \pmod 5,\quad 9a^2 y \equiv 16b^2 \pmod 5,\quad 3az \equiv -4b \pmod 5.$$

A solution is $x = 1$, $y = 4$ and $z = 2$. So, a 5-integral basis for K is

$$\left\{1,\ \theta,\ \theta^2,\ \frac{1 + 4\theta + 2\theta^2 + \theta^3}{5}\right\}.$$

For $p \neq 2, 3, 5, 47$, by case C7, a p-integral basis for K is

$$\{1,\ \theta,\ \theta^2,\ \theta^3\}.$$

Then, by Theorem 3.1, an integral basis for K is

$$\left\{1,\ \theta,\ \frac{2 + \theta^2}{2^2},\ \frac{x + y\theta + z\theta^2 + \theta^3}{2^2 \cdot 5}\right\},$$

where

$$x \equiv 0 \pmod 4,\quad y \equiv 2 \pmod 4,\quad z \equiv 0 \pmod 4,$$
$$x \equiv 1 \pmod 5,\quad y \equiv 4 \pmod 5,\quad z \equiv 2 \pmod 5.$$

A solution is given by $x = 16$, $y = 14$ and $z = 12$. Thus an integral basis for K is

$$\left\{1,\ \theta,\ \frac{2 + \theta^2}{2^2},\ \frac{16 + 14\theta + 12\theta^2 + \theta^3}{2^2 \cdot 5}\right\}$$

and the discriminant of K is

$$d(K) = 2^6 \cdot 3803.$$

Example 3.2. Let $K = \mathbb{Q}(\theta)$, where $\theta^4 + a\theta + b = 0$. Let $a = 360 = 2^3 \cdot 3^2 \cdot 5$ and $b = 360 = 2^3 \cdot 3^2 \cdot 5$. Since $\nu_2(a) = 3$ and $\nu_2(b) = 3$, by case A17, a 2-integral basis for K is

$$\left\{1, \theta, \frac{\theta^2}{2}, \frac{\theta^3}{2^2}\right\}.$$

Since $\nu_3(a) = 2$ and $\nu_3(b) = 2$, by case B6, a 3-integral basis for K is

$$\left\{1, \theta, \frac{\theta^2}{3}, \frac{\theta^3}{3}\right\}.$$

Since $\nu_5(a) = 1$ and $\nu_5(b) = 1$, by case C2, a 5-integral basis for K is

$$\{1, \theta, \theta^2, \theta^3\}.$$

Since $\nu_{13}(ab) = 0$, we find a 13-integral basis for K using case C7. Note that

$$\Delta = 2^8 b^3 - 3^3 a^4 = -2^{12} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 13^2.$$

So, $s_{13} = 2$ and $m = s_{13}/2 = 2/2 = 1$. We need to solve the congruences

$$4x \equiv 3a \pmod{13}, \quad 9a^2 y \equiv 16b^2 \pmod{13}, \quad 3az \equiv -4b \pmod{13}.$$

A solution is $x = 10$, $y = 9$ and $z = 3$. So, a 13-integral basis of K is

$$\left\{1, \theta, \theta^2, \frac{10 + 9\theta + 3\theta^2 + \theta^3}{13}\right\}.$$

Since $\nu_p(ab) = 0$ for $p \neq 2, 3, 5, 13$, by case C7, a p-integral basis for K is

$$\{1, \theta, \theta^2, \theta^3\}.$$

Then, by Theorem 3.1, an integral basis for K is

$$\left\{1, \theta, \frac{\theta^2}{2 \cdot 3}, \frac{x + y\theta + z\theta^2 + \theta^3}{2^2 \cdot 3 \cdot 13}\right\},$$

where

$$x \equiv 0 \pmod 4, \quad y \equiv 0 \pmod 4, \quad z \equiv 0 \pmod 4,$$

$$x \equiv 0 \pmod 3, \quad y \equiv 0 \pmod 3, \quad z \equiv 0 \pmod 3,$$

$$x \equiv 10 \pmod{13}, \quad y \equiv 9 \pmod{13}, \quad z \equiv 3 \pmod{13}.$$

A solution is given by $x = 36$, $y = 48$ and $z = 120$. Thus an integral basis for K is

$$\left\{1,\ \theta,\ \frac{\theta^2}{6},\ \frac{36 + 48\theta + 120\theta^2 + \theta^3}{2^2 \cdot 3 \cdot 13}\right\}$$

and the discriminant of K is

$$d(K) = -2^6 \cdot 3^2 \cdot 5^3 \cdot 7.$$

Example 3.3. Let $K = \mathbb{Q}(\theta)$, where $\theta^4 + a\theta + b = 0$. Let $a = 28 = 2^2 \cdot 7$ and $b = 189 = 3^3 \cdot 7$. Then

$$\Delta = 2^8 b^3 - 3^3 a^4 = 2^9 \cdot 3^3 \cdot 7^3 \cdot 19^2.$$

Since $v_2(a) = 2$ and $b \equiv 1 \pmod 4$, by case A20, a 2-integral basis for K is

$$\{1,\ \theta,\ \theta^2,\ \theta^3\}.$$

Since $v_3(a) = 0$, $v_3(b) = 3$ and $a^2 \equiv 1 \pmod 9$, by case B8, a 3-integral basis for K is

$$\left\{1,\ \theta,\ \theta^2,\ \frac{\theta + 2\theta^2 + \theta^3}{3}\right\}.$$

Since $v_7(a) = 1$ and $v_7(b) = 1$, by case C2, a 7-integral basis for K is

$$\{1,\ \theta,\ \theta^2,\ \theta^3\}.$$

Since $v_{19}(ab) = 0$, using case C7, we find that a 19-integral basis for K is

$$\left\{1,\ \theta,\ \theta^2,\ \frac{2 + 5\theta + 10\theta^2 + \theta^3}{19}\right\}.$$

Since $v_p(ab) = 0$ for $p \neq 2, 3, 7, 19$, by case C7, a p-integral basis for K is

$$\{1,\ \theta,\ \theta^2,\ \theta^3\}.$$

Then, by Theorem 3.1, we find that an integral basis for K is

$$\left\{1,\ \theta,\ \theta^2,\ \frac{21 + 43\theta + 29\theta^2 + \theta^3}{3 \cdot 19}\right\}$$

and the discriminant of K is

$$d(K) = 2^9 \cdot 3 \cdot 7^3.$$

In the following example we illustrate how to combine the cases from Table A, Table B and Table C in general.

Example 3.4. Let $K = \mathbb{Q}(\theta)$, where $\theta^4 + a\theta + b = 0$. We consider the cases A7, B19 and C7.

Case A7. $v_2(a) = 2$ and $v_2(b) = 2$.

Case B19. $v_3(a) = 0$, $b \equiv 3 \pmod 9$ and $a^4 \equiv 4b + 1 \pmod{27}$.

Case C7. $v_p(ab) = 0$.

A 2-integral basis of K is $\left\{1, \theta, \frac{\theta^2}{2}, \frac{\theta^3}{2}\right\}$.

A 3-integral basis of K is

$$\left\{1, \theta, \frac{a\theta + \theta^2}{3}, \frac{x + y\theta + z\theta^2 + \theta^3}{3^m}\right\},$$

where the integers x, y, z, m are given by

$$m = [(s_3 - 2)/2],$$

$$4x \equiv 3a \pmod{3^m},$$

$$9a^2 y \equiv 16b^2 \pmod{3^{m+2}},$$

$$3az \equiv -4b \pmod{3^{m+1}}.$$

A $p(> 3)$-integral basis of K is

$$\left\{1, \theta, \theta^2, \frac{x + y\theta + z\theta^2 + \theta^3}{p^m}\right\},$$

where the integers x, y, z, m are given by

$$m = [s_p/2],$$

$$4x \equiv 3a \pmod{p^m},$$

$$9a^2 y \equiv 16b^2 \pmod{p^m},$$

$$3az \equiv -4b \pmod{p^m}.$$

Then an integral basis of K is

$$\left\{1,\ \theta,\ \frac{a\theta + \theta^2}{6},\ \frac{x + y\theta + z\theta^2 + \theta^3}{T}\right\},$$

where

$$T = 2 \cdot 3^{[(s_3-2)/2]} \prod_{p>3} p^{[s_p/2]},$$

and the integers x, y and z are given by

$$x,\ y,\ z \equiv 0 \pmod 2,$$

$$4x \equiv 3a\left(\operatorname{mod} 3^{[(s_3-2)/2]} \prod_{p>3} p^{[s_p/2]}\right),$$

$$9a^2 y \equiv 16b^2\left(\operatorname{mod} 3^{[(s_3+2)/2]} \prod_{p>3} p^{[s_p/2]}\right),$$

$$3az \equiv -4b\left(\operatorname{mod} 3^{[s_3/2]} \prod_{p>3} p^{[s_p/2]}\right). \tag{3.1}$$

The discriminant of K is

$$d(K) = 2^4 \prod_{p \neq 2} p^{s_p - 2[s_p/2]}.$$

We illustrate this example with some numerical values. Let $K = \mathbb{Q}(\theta)$, $\theta^4 + 76\theta + 2748 = 0$. Then

$$a = 76,\quad b = 2748,\quad \Delta = 2^8 \cdot 3^8 \cdot 5^2 \cdot 126493 \quad \text{and} \quad T = 2 \cdot 3^3 \cdot 5.$$

The system of congruences (3.1) becomes

$$x,\ y,\ z \equiv 0 \pmod 2,$$

$$4x \equiv 3a \pmod{3^3 \cdot 5},$$

$$9a^2y \equiv 16b^2 \pmod{3^5 \cdot 5},$$

$$3az \equiv -4b \pmod{3^4 \cdot 5}. \tag{3.2}$$

By solving the system of congruences (3.2) we find that

$$\left\{1,\ \theta,\ \frac{4\theta+\theta^2}{6},\ \frac{-78+76\theta-34\theta^2+\theta^3}{2\cdot 3^3\cdot 5}\right\}$$

is an integral basis of K and the discriminant of K is $d(K) = 2^4 \cdot 126493$.

Note that the last two examples are not covered by the results of [5].

References

[1] Ş. Alaca, *p*-integral bases of a cubic field, Proc. Amer. Math. Soc. 126(7) (1998), 1949-1953.

[2] Ş. Alaca, *p*-integral bases of algebraic number fields, Utilitas Math. 56 (1999), 97-106.

[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.

[4] P. Llorente, E. Nart and N. Vila, Discriminants of number fields defined by trinomials, Acta Arith. 43 (1984), 367-373.

[5] P. Llorente, E. Nart and N. Vila, Decomposition of primes in number fields defined by trinomials, Séminare de Théorie des Nombres, Bordeaux 3 (1991), 27-41.

Centre for Research in Algebra and Number Theory
School of Mathematics and Statistics
Carleton University
Ottawa, Ontario, Canada K1S 5B6
e-mail: salaca@math.carleton.ca
williams@math.carleton.ca