JP Jour. Algebra, Number Theory & Appl. 3(3) (2003), 477-505

A SIMPLE METHOD FOR FINDING AN INTEGRAL BASIS OF A QUARTIC FIELD DEFINED BY A TRINOMIAL $x^4 + ax + b$

ŞABAN ALACA
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

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

Abstract

Let K be an algebraic number field of degree n. The ring of integers of K is denoted by O_K. Let P be a prime ideal of O_K, let p be a rational prime, and let $\alpha(\neq 0) \in K$. 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 αO_K. 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 Q, where each $\omega_i (i \in \{1, 2, \ldots, n\})$ 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 a_i are p-integral elements of Q,

2000 Mathematics Subject Classification: 11R16, 11R29.

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

The research of the second author was supported by a grant from the Natural Sciences and Engineering Research Council of Canada.

Received July 9, 2003

then $\{\omega_1, \omega_2, \ldots, \omega_n\}$ is called a p-integral basis of K. In this paper for each prime p we determine a system of polynomial congruences modulo certain powers of p, which is such that a p-integral basis of K can be given very simply in terms of a simultaneous solution t of the congruences. These congruences are then put together to give a system of congruences in terms of whose solution an integral basis for K can be given.

1. Introduction

Let $K = Q(\theta)$ be an algebraic number field of degree n, and let O_K denote the ring of integral elements of K. Every algebraic number field K possesses an integral basis, that is K contains n elements $\alpha_1, \alpha_2, \ldots, \alpha_n$ such that $O_K = \alpha_1 Z + \alpha_2 Z + \cdots + \alpha_n Z$.

Let P be a prime ideal of O_K, let p be a rational prime, and let $\alpha(\neq 0) \in K$. 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 αO_K. If α is P-integral for each prime ideal P of O_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 Q, where each $\omega_i (i \in \{1, 2, \ldots, n\})$ 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 a_i are p-integral elements of Q, then $\{\omega_1, \omega_2, \ldots, \omega_n\}$ is called a *p-integral basis* of K.

Let K be the quartic field $Q(\theta)$, where θ is a root of the irreducible quartic trinomial

$$f(x) = x^4 + ax + b, \quad a, b \in Z. \tag{1.1}$$

In [2] Alaca and Williams determined a p-integral basis for K for each prime p, as well as the discriminant $d(K)$ of K. Making use of these results, we determine for each prime p a system of polynomial congruences modulo certain powers of p such that a p-integral basis for K can be given very simply in terms of a simultaneous solution of the congruences.

It can be assumed without loss of generality that for every prime p, either $\nu_p(a) < 3$ or $\nu_p(b) < 4$. The discriminant of θ is

$$\Delta = 2^8 b^3 - 3^3 a^4 \quad \text{and} \quad \Delta = i(\theta)^2 d(K), \tag{1.2}$$

where $d(K)$ denotes the discriminant of K and $i(\theta)$ denotes the index of θ.

For each prime p, we set $s_p = \nu_p(\Delta)$ and $\Delta_p = \Delta/p^{s_p}$.

The following two theorems are the special cases for $n = 4$ of Theorem 2.1 and Theorem 3.1, respectively in [1].

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

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

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 a p-integral element of K if and only if

$$\begin{aligned} & X \equiv 0 \pmod{p^m}, \quad Y \equiv 0 \pmod{p^{2m}}, \\ & Z \equiv 0 \pmod{p^{3m}}, \quad W \equiv 0 \pmod{p^{4m}}. \end{aligned} \tag{1.3}$$

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

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

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

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

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

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

The p-integral elements

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

in Theorem 1.2 are known as minimal p-integral elements of degrees 1, 2, 3, respectively. It is known that [2],

$$i = 0, \quad \text{for all } p,$$
$$j \in \{0, 1, 2\}, \quad \text{if } p = 2,$$
$$j \in \{0, 1\}, \quad \text{if } p \geq 3.$$

The following theorem is given by Alaca and Williams [2, Theorem 3.1].

Theorem 1.3. *Let* $K = Q(\theta)$ *be a quartic field, where* θ *is a root of the irreducible trinomial* (1.1). *Then the discriminant of K is*

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

where

$$\alpha = \begin{cases} 0 & \text{if } v_2(a) = 0, \\ 2 & \text{if } v_2(a) = 1 \text{ and } b \equiv 1(4) \\ & \text{or } v_2(a) = 1 \text{ and } v_2(b) \geq 2 \\ & \text{or } v_2(a) = 2 \text{ and } v_2(b) \geq 3 \\ & \text{or } v_2(a) \geq 3 \text{ and } b \equiv 7(8), \\ 3 & \text{if } v_2(a) = 2,\ b \equiv 3(16),\ \Delta_2 \equiv 3(4) \text{ and } s_2 \text{ odd} \\ & \text{or } v_2(a) = 2,\ b \equiv 11(16) \text{ and } \Delta_2 \equiv 1(4), \\ 4 & \text{if } v_2(a) = 1 \text{ and } b \equiv 3(4) \\ & \text{or } v_2(a) = 1 \text{ and } v_2(b) = 1 \\ & \text{or } v_2(a) = 2 \text{ and } v_2(b) = 2 \\ & \text{or } v_2(a) \geq 3 \text{ and } b \equiv 3(8) \\ & \text{or } a = 16A,\ b = 4 + 16B \text{ and } A + B \equiv 0(2), \\ 5 & \text{if } v_2(a) = 2,\ b \equiv 11(16) \text{ and } \Delta_2 \equiv 3(4) \\ & \text{or } v_2(a) = 2,\ b \equiv 3(16),\ \Delta_2 \equiv 1(4) \text{ and } s_2 \text{ odd}, \\ 6 & \text{if } v_2(a) = 3 \text{ and } v_2(b) = 2,\ 3 \\ & \text{or } v_2(a) \geq 4 \text{ and } b \equiv 12(16) \\ & \text{or } v_2(a) = 2 \text{ and } b \equiv 7(8) \\ & \text{or } v_2(a) = 2,\ b \equiv 3(16) \text{ and } s_2 \text{ even} \\ & \text{or } a = 16A,\ b = 4 + 16B \text{ and } A + B \equiv 1(2), \\ 8 & \text{if } v_2(a) = 2 \text{ and } v_2(b) = 1 \\ & \text{or } v_2(a) \geq 3 \text{ and } b \equiv 1(4), \\ 9 & \text{if } v_2(a) = 2 \text{ and } b \equiv 1(4), \\ 10 & \text{if } v_2(a) = 4 \text{ and } v_2(b) = 3, \\ 11 & \text{if } v_2(a) \geq 3 \text{ and } v_2(b) = 1 \\ & \text{or } v_2(a) \geq 5 \text{ and } v_2(b) = 3, \end{cases}$$

and

$$\beta = \begin{cases} 0 & \text{if } v_3(b) = 0 \\ & \text{or } v_3(a) = 0,\ b \equiv 3(9),\ a^4 \equiv 4b + 1(27) \text{ and } s_3 \text{ even}, \\ 1 & \text{if } v_3(a) = 0,\ a^2 \equiv 1(9) \text{ and } v_3(b) \geq 2 \\ & \text{or } v_3(a) = 0,\ b \equiv 6(9) \text{ and } a^4 \equiv 4b + 1(9) \\ & \text{or } v_3(a) = 0,\ b \equiv 3(9),\ a^4 \equiv 4b + 1(27) \text{ and } s_3 \text{ odd}, \\ 2 & \text{if } v_3(a) \geq 2 \text{ and } v_3(b) = 2, \\ 3 & \text{if } v_3(a) \geq 1 \text{ and } v_3(b) = 1 \\ & \text{or } v_3(a) = 0,\ a^2 \not\equiv 1(9) \text{ and } v_3(b) \geq 2 \\ & \text{or } v_3(a) \geq 2 \text{ and } v_3(b) = 3 \\ & \text{or } v_3(a) = 0,\ b \equiv 6(9) \text{ and } a^4 \not\equiv 4b + 1(9) \\ & \text{or } v_3(a) = 0,\ b \equiv 3(9),\ a^4 \equiv 4b + 1(9) \text{ and } a^4 \not\equiv 4b + 1(27), \\ 4 & \text{if } v_3(a) = 1 \text{ and } v_3(b) = 2 \\ & \text{or } v_3(a) = 0,\ b \equiv 3(9),\ a^4 \not\equiv 4b + 1(9), \\ 5 & \text{if } v_3(a) = 1 \text{ and } v_3(b) = 3 \\ & \text{or } v_3(a) = 1,\ 2 \text{ and } v_3(b) \geq 4. \end{cases}$$

2. A Simple Method for Finding a p-integral Basis of a Quartic Field defined by a Trinomial $x^4 + ax + b$

Let p be a rational prime. A p-integral basis of K comprises $1, \theta$, a minimal p-integral element of degree 2 in θ, and a minimal p-integral element of degree 3 in θ. A minimal p-integral element of degree 2 in θ is of the form $(u + v\theta + \theta^2)/p^j$, where $j \in \{0, 1, 2\}$ if $p = 2$ and $j \in \{0, 1\}$ if $p > 2$. Theorem 2.1 below gives a simple method for finding a minimal p-integral element of degree 2 in θ and a minimal p-integral element of degree 3 in θ. Hence a p-integral basis of K is given very simply in terms of a simultaneous solution t of a system of polynomial congruences. We begin with a simple result concerning this system of polynomial congruences.

Lemma 2.1. *Let p be a prime. Then there does not exist an integer t such that the congruences*

$$t^4 + at + b \equiv 0 \pmod{p^4},$$

$$4t^3 + a \equiv 0 \pmod{p^3},$$

$$6t^2 \equiv 0 \pmod{p^2}$$

are simultaneously solvable.

Proof. Suppose that the congruences above have a simultaneous solution t. From the third congruence we deduce that $p \mid t$. Then from the second one we obtain $p^3 \mid a$. Next from the first one we deduce that $p^4 \mid b$. This contradicts our assumption that $v_p(a) < 3$ or $v_p(b) < 4$.

Theorem 2.1. *Let $K = Q(\theta)$ be a quartic field, where θ is a root of the irreducible trinomial* (1.1).

(a) *Suppose that $p > 2$ or $p = 2$ and $v_2(a) \geq 3$, $v_2(b) = 2$ does not hold. Let j be the largest integer such that $p^{4j} \mid \Delta$, and the system of congruences*

$$t^4 + at + b \equiv 0 \pmod{p^{2j+\lambda(j)}}$$

$$4t^3 + a \equiv 0 \pmod{p^{2j}}$$

$$6t^2 \equiv 0 \pmod{p^j} \tag{2.1}$$

is solvable for t, where

$$\lambda(j) = \begin{cases} 0 & \text{if } \nu_p(a) \geq 2 \text{ and } \nu_p(b) = 2, \\ & \text{or } \nu_2(a) \geq 2 \text{ and } \nu_2(b) = 0, \\ j & \text{otherwise.} \end{cases} \tag{2.2}$$

Let k be the largest integer such that $p^{4j+2k} \mid \Delta$, and both the system of congruences (2.1) *and the system of congruences*

$$t^4 + at + b \equiv 0 \pmod{p^{j+2k}}$$

$$4t^3 + a \equiv 0 \pmod{p^{j+k}}$$

$$6t^2 \equiv 0 \pmod{p^j} \tag{2.3}$$

are simultaneously solvable for t.

Then a p-integral basis of K is given by

$$\left\{1,\ \theta,\ \frac{3t^2 + 2t\theta + \theta^2}{p^j},\ \frac{(t^3 + a) + t^2\theta + t\theta^2 + \theta^3}{p^{j+k}}\right\}, \tag{2.4}$$

where t is a simultaneous solution of (2.1) *and* (2.3), *and the p-part of the discriminant of K is given by*

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

(We remark that if $k \geq j$ a solution t of (2.3) *is also a solution of* (2.1) *and if $k = 0$ a solution t of* (2.1) *is also a solution of* (2.3).)

(b) *Suppose that $p = 2$ and $\nu_2(a) \geq 3$, $\nu_2(b) = 2$ holds. If $\nu_2(a) = 3$, then a 2-integral basis of K is given by*

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

If $a = 16A$, $b = 4 + 16B$ *and* $A + B \equiv 1 \pmod 2$, *then a* 2*-integral basis of K is given by*

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

If $a = 16A$, $b = 4 + 16B$ *and* $A + B \equiv 0 \pmod 2$, *then a* 2*-integral basis of K is given by*

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

If $v_2(a) \geq 4$ *and* $b \equiv 12 \pmod{16}$, *then a* 2*-integral basis of K is given by*

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

The 2*-part of the discriminant of K is*

$$v_2(d(K)) = \begin{cases} 4 & \text{if } a = 16A,\ b = 4 + 16B \text{ and } A + B \equiv 0 \pmod 2, \\ 6 & \text{otherwise.} \end{cases}$$

Proof. This theorem follows from Theorems 1.1, 1.2 and 1.3 by a case by case examination. Part (b) is a special case of Alaca and Williams [2, Theorem 2.1]. We give the details of the proof of part (a) in six representative cases. By Lemma 2.1 we have $j = 0$ or 1.

(i) Let $p = 2$ and $v_2(a) = v_2(b) = 2$. Let $a = 4a'$, $b = 4b'$, where a' and b' are odd integers. In this case $s_2 = 8$ and $v_2(d(K)) = 4$. By (2.2) $\lambda(j) = 0$. For $j = 1$, (2.1) has the solution $t = 0$, so $j = 1$. Since $2^{4j+2k} \mid \Delta$, $k \leq 2$. As the system of congruences

$$t^4 + at + b \equiv 0 \pmod{2^3},$$

$$4t^3 + a \equiv 0 \pmod{2^2},$$

$$6t^2 \equiv 0 \pmod 2,$$

has no solution we have $k = 0$.

We now show that $\frac{3t^2+2t\theta+\theta^2}{2}$ and $\frac{(t^3+a)+t^2\theta+t\theta^2+\theta^3}{2}$ are 2-integral elements of K, where t is a solution of (2.1). The general solution of (2.1) is $t \equiv 0 \pmod 2$. Set $t = 2u$. Then

$$\frac{3t^2+2t\theta+\theta^2}{2} = 6u^2 + 2u\theta + \frac{\theta^2}{2}$$

and

$$\frac{(t^3+a)+t^2\theta+t\theta^2+\theta^3}{2} = 4u^3 + 2a' + 2u^2\theta + u\theta^2 + \theta^3/2,$$

and it suffices to show that $\theta^2/2$ and $\theta^3/2$ are 2-integral. This is clear as $\theta^2/2$ is a root of $x^4 + 2b'x^2 - 2a'^2x + b'^2 \in Z[x]$.

Since $\nu_2(d(K)) = 4$, by Theorem 1.2,

$$\left\{1,\ \theta,\ \frac{3t^2+2t\theta+\theta^2}{2},\ \frac{(t^3+a)+t^2\theta+t\theta^2+\theta^3}{2}\right\}$$

is a 2-integral basis of K, where t is a simultaneous solution of (2.1) and (2.3).

(ii) Let $p = 2$, $a \equiv 4 \pmod 8$, $b \equiv 3 \pmod 8$ and $s_2 \equiv 0 \pmod 2$. Here $s_2 \geq 12$. It is easily seen from (2.1) and (2.2) that $j = 1$ and $\lambda(j) = 0$. First we show that (2.3) has a solution for $k = \frac{s_2 - 10}{2}$, that is, we show that the congruences

$$t^4 + at + b \equiv 0 \pmod{2^{s_2-9}},$$

$$4t^3 + a \equiv 0 \pmod{2^{(s_2-8)/2}},$$

$$6t^2 \equiv 0 \pmod 2 \tag{2.5}$$

are simultaneously solvable for t. Note that the third congruence in (2.5) is always true. As $a/4$ is odd and $s_2 > 2$, we can define an integer t by $3\frac{a}{4}t \equiv -b \pmod{2^{s_2-2}}$ so that $3at \equiv -2^2 b \pmod{2^{s_2}}$. Then

$$3^4a^4(t^4+at+b) = (3at)^4 + 3^3a^4(3at) + 3^4a^4b$$
$$\equiv 2^8b^4 - 2^23^3a^4b + 3^4a^4b \pmod{2^{s_2}}$$
$$\equiv 2^8b^4 - 3^3a^4b \pmod{2^{s_2}}$$
$$\equiv \Delta b \pmod{2^{s_2}}$$
$$\equiv 0 \pmod{2^{s_2}}.$$

As $2^2 \parallel a$ we deduce that $t^4 + at + b \equiv 0 \pmod{2^{s_2-8}}$. Also

$$3^3a^3(4t^3+a) = 4(3at)^3 + 3^3a^4$$
$$\equiv -2^8b^3 + 3^3a^4 \pmod{2^{s_2}}$$
$$\equiv -\Delta \pmod{2^{s_2}}$$
$$\equiv 0 \pmod{2^{s_2}}.$$

As $2^2 \parallel a$ we have $4t^3 + a \equiv 0 \pmod{2^{s_2-6}}$. Thus t is the required solution of (2.5). So $k \geq \frac{s_2 - 10}{2}$.

Next we show that (2.3) does not have a solution for $k = \frac{s_2 - 8}{2}$, that is we show that the congruences

$$t^4 + at + b \equiv 0 \pmod{2^{s_2-7}},$$
$$4t^3 + a \equiv 0 \pmod{2^{(s_2-6)/2}} \tag{2.6}$$

are not simultaneously solvable for t.

Suppose that t is a solution of (2.6). Set $R = t^4 + at + b$ and $S = 4t^3 + a$. Then

$$\frac{4R - 4b}{3a + S} = \frac{4t^4 + 4at}{4t^3 + 4a} = t.$$

Hence

$$S = 4\left(\frac{4R - 4b}{3a + S}\right)^3 + a.$$

Expanding the cube and simplifying, we obtain

$$\Delta = 2^8(R^3 - 3bR^2 + 3b^2R) - 18a^2S^2 - 8aS^3 - S^4.$$

As t is a solution of (2.6) we have

$$2^{s_2-7} \mid R \quad \text{and} \quad 2^{\frac{s_2-6}{2}} \mid S$$

so as $s_2 \geq 12$,

$$\Delta \equiv -18a^2S^2 - S^4 \pmod{2^{s_2+1}}.$$

If $2^{\frac{s_2-4}{2}} \mid S$, then

$$\Delta \equiv 0 \pmod{2^{s_2+1}},$$

a contradiction. If $2^{\frac{s_2-6}{2}} \parallel S$, then

$$\Delta \equiv 2^{s_2-1} \pmod{2^{s_2}},$$

a contradiction. Hence the congruences (2.6) are insolvable. This completes the proof that $k = \dfrac{s_2 - 10}{2}$.

We now show that both $\dfrac{3t^2 + 2t\theta + \theta^2}{2}$ and $\dfrac{(t^3 + a) + t^2\theta + t\theta^2 + \theta^3}{2^{(s_2-8)/2}}$ are 2-integral elements of K, where t is a solution of (2.5). Clearly t is odd. To show that $\dfrac{3t^2 + 2t\theta + \theta^2}{2} = \dfrac{3t^2 - 1}{2} + t\theta + \dfrac{1 + \theta^2}{2}$ is a 2-integral element of K, it suffices to show that $\dfrac{1 + \theta^2}{2}$ is 2-integral. This is clear as $\dfrac{1 + \theta^2}{2}$ is a root of

$$x^4 - 2x^3 + \frac{(b + 3)}{2}x^2 - \frac{(4 + 4b + a^2)}{8}x + \frac{((1 + b)^2 + a^2)}{16} \in Z[x].$$

To show that $\frac{(t^3+a)+t^2\theta+t\theta^2+\theta^3}{2^{(s_2-8)/2}}$ is a 2-integral element of K, we substitute $x=t^3+a$, $y=t^2$, $z=t$ and $w=1$ into Theorem 1.1. We obtain $X=4t^3+a$, $Y=6t^2(t^4+at+b)$, $Z=4t(t^4+at+b)^2$, $W=(t^4+at+b)^3$. As $s_2\geq 12$, it follows from (2.5) that

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

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

where $m=\frac{s_2-8}{2}$. Thus $\frac{(t^3+a)+t^2\theta+t\theta^2+\theta^3}{2^{(s_2-8)/2}}$ is a 2-integral element of K. Since $\nu_2(d(K))=6$,

$$\left\{1,\ \theta,\ \frac{3t^2+2t\theta+\theta^2}{2},\ \frac{(t^3+a)+t^2\theta+t\theta^2+\theta^3}{2^{(s_2-8)/2}}\right\}$$

is a 2-integral basis of K, where t is a solution of (2.5). This is of the required form (2.4).

(iii) Let $p=2$, $a\equiv 4 \pmod 8$, $b\equiv 3 \pmod{16}$, $s_2\equiv 1 \pmod 2$ and $\Delta_2\equiv 3 \pmod 4$. Then $s_2\geq 13$. From (2.1) and (2.2) we see that $j=1$ and $\lambda(j)=0$, respectively. First we show that (2.3) has a solution for $k=\frac{s_2-7}{2}$, that is we show that the congruences

$$t^4+at+b\equiv 0 \pmod{2^{s_2-6}},$$

$$4t^3+a\equiv 0 \pmod{2^{(s_2-5)/2}},$$

$$6t^2\equiv 0 \pmod 2 \tag{2.7}$$

are simultaneously solvable for t. The third congruence in (2.7) is always true.

As $2^2 \parallel a$, s_2 odd and $s_2\geq 13$, we can define an integer t by

$$3\frac{a}{4}t\equiv -b+2^{(s_2-9)/2} \pmod{2^{(s_2-7)/2}}.$$

Thus

$$3at \equiv -2^2 b + 2^{(s_2-5)/2} \pmod{2^{(s_2-3)/2}}.$$

Hence

$$3at = -2^2 b + A2^{(s_2-5)/2}$$

for some odd integer A. Then

$$\begin{aligned}
&3^4 a^4 (t^4 + at + b)\\
&= (3at)^4 + 3^3 a^4 (3at) + 3^4 a^4 b\\
&= (-2^2 b + A2^{(s_2-5)/2})^4 + 3^3 a^4 (-2^2 b + A2^{(s_2-5)/2}) + 3^4 a^4 b\\
&= 2^8 b^4 - 2^{(s_2+11)/2} b^3 A + 3 \cdot 2^{s_2} b^2 A^2 - 2^{(3s_2-7)/2} b A^3\\
&\quad + 2^{2s_2-10} A^4 - 3^3 2^2 a^4 b + 3^3 2^{(s_2-5)/2} a^4 A + 3^4 a^4 b\\
&= \Delta b - \Delta 2^{(s_2-5)/2} A + 3 \cdot 2^{s_2} b^2 A^2 - 2^{(3s_2-7)/2} b A^3 + 2^{2s_2-10} A^4\\
&\equiv 2^{s_2} + 0 + 3 \cdot 2^{s_2} + 0 + 0 \pmod{2^{s_2+2}}\\
&\equiv 0 \pmod{2^{s_2+2}},
\end{aligned}$$

as $\Delta b = 2^{s_2} \Delta_2 b \equiv 2^{s_2} \pmod{2^{s_2+2}}$, $A^2 \equiv b^2 \equiv 1 \pmod 4$, and $s_2 \geq 13$. As $2^2 \parallel a$ we deduce that $t^4 + at + b \equiv 0 \pmod{2^{s_2-6}}$. Also

$$\begin{aligned}
3^3 a^3 (4t^3 + a) &= 4(3at)^3 + 3^3 a^4\\
&= 4(-2^2 b + A2^{(s_2-5)/2})^3 + 3^3 a^4\\
&= -2^8 b^3 + 3b^2 A 2^{(s_2+7)/2} - 3bA^2 2^{s_2-1} + A^3 2^{(3s_2-11)/2} + 3^3 a^4\\
&\equiv -\Delta \pmod{2^{(s_2+7)/2}} \text{ (as } s_2 \geq 13)\\
&\equiv 0 \pmod{2^{(s_2+7)/2}}.
\end{aligned}$$

As $2^2 \parallel a$ we see that $4t^3 + a \equiv 0 \pmod{2^{(s_2-5)/2}}$. Hence t is a solution of (2.7), and $k \geq \frac{s_2 - 7}{2}$.

Next we show that (2.3) does not have a solution for $k = \frac{s_2 - 5}{2}$, i.e., we show that the congruences

$$t^4 + at + b \equiv 0 \pmod{2^{s_2-4}},$$
$$4t^3 + a \equiv 0 \pmod{2^{(s_2-3)/2}} \tag{2.8}$$

are not simultaneously solvable for t. Suppose that t is a solution of the pair of congruences (2.8). As in (ii) we have

$$\Delta = 2^8(R^3 - 3bR^2 + 3b^2R) - 18a^2S^2 - 8aS^3 - S^4,$$

where $R = t^4 + at + b$ and $S = 4t^3 + a$. Now

$$2^{s_2-4} \mid R, \; 2^{(s_2-3)/2} \mid S,$$

so, as $s_2 \geq 13$, we have

$$\Delta \equiv 0 \pmod{2^{s_2+1}},$$

a contradiction. We have shown that $k = \frac{s_2 - 7}{2}$.

Finally if t is a solution of (2.3), as in case (ii), it follows from Theorem 1.1 that $\frac{3t^2 + 2t\theta + \theta^2}{2^j}$ and $\frac{(t^3 + a) + t^2\theta + t\theta^2 + \theta^3}{2^{j+k}}$ are both 2-integral elements of K, where $j = 1$ and $k = (s_2 - 7)/2$. Since $v_2(d(K)) = 3$,

$$\left\{1, \theta, \frac{3t^2 + 2t\theta + \theta^2}{2}, \frac{(t^3 + a) + t^2\theta + t\theta^2 + \theta^3}{2^{(s_2-5)/2}}\right\}$$

is a 2-integral basis of K, in agreement with (2.4).

(iv) Let $p = 3$, $v_3(a) \geq 2$ and $v_3(b) = 2$. In this case $s_3 = 6$ and $v_3(d(K)) = 2$. Since $3^{4j} \mid \Delta$, $j \leq 1$. For $j = 1$, $\lambda(j) = 0$, and (2.1) has a solution if and only if $t \equiv 0 \pmod 3$. So $j = 1$. Since $3^{4j+2k} \mid \Delta$, $k \leq 1$. If $k = 1$, then (2.3) gives a contradiction. So $k = 0$. Note that if t is a simultaneous solution of (2.1) and (2.3), then by Theorem 1.1, $\frac{3t^2 + 2t\theta + \theta^2}{3}$ and $\frac{(t^3 + a) + t^2\theta + t\theta^2 + \theta^3}{3}$ are both 3-integral elements.

Since $\nu_2(d(K)) = 2$,

$$\left\{1,\ \theta,\ \frac{3t^2 + 2t\theta + \theta^2}{3},\ \frac{(t^3 + a) + t^2\theta + t\theta^2 + \theta^3}{3}\right\}$$

is a 3-integral basis of K, in agreement with (2.4).

(v) Let $p > 3$, $\nu_p(a) \geq 2$ and $\nu_p(b) = 2$. In this case $s_p = 6$ and $\nu_p(d(K)) = 2$. Since $p^{4j} \mid \Delta$, $j \leq 1$. For $j = 1$, $\lambda(j) = 0$, and (2.1) has a solution if and only if $t \equiv 0 \pmod{p}$. So $j = 1$. Since $p^{4j+2k} \mid \Delta$, $k \leq 1$. If $k = 1$, then (2.3) gives a contradiction. So $k = 0$. As θ^2/p is a root of $x^4 + \frac{2b}{p^2}x^2 - \frac{a^2}{p^3}x + \frac{b^2}{p^4} \in Z[x]$ we see that $\theta^2/p \in O_K$ and $\theta^3/p \in O_K$. Let t be a simultaneous solution of (2.1) and (2.3). Then $t \equiv 0 \pmod{p}$, say $t = pu$, where $u \in Z$. Thus $\frac{3t^2 + 2t\theta + \theta^2}{p} = 3pu^2 + 2u\theta + \frac{\theta^2}{p} \in O_K$ and

$$\frac{(t^3 + a) + t^2\theta + t\theta^2 + \theta^3}{p} = (p^2u^3 + \frac{a}{p}) + pu^2\theta + u\theta^2 + \frac{\theta^3}{p} \in O_K.$$

Since $\nu_p(d(K)) = 2$,

$$\left\{1,\ \theta,\ \frac{3t^2 + 2t\theta + \theta^2}{p},\ \frac{(t^3 + a) + t^2\theta + t\theta^2 + \theta^3}{p}\right\}$$

is a p-integral basis of K, in agreement with (2.4).

(vi) Let $p > 3$ and $\nu_p(ab) = 0$. In this case $\nu_p(d(K)) = s_p - 2[s_p/2]$. It is easily seen that $j = 0$. We show that (2.3) has a solution for $k = [s_p/2]$, that is, we show that the congruences

$$t^4 + at + b \equiv 0 \pmod{p^{2k}},$$

$$4t^3 + a \equiv 0 \pmod{p^k} \tag{2.9}$$

are simultaneously solvable for t. As $p > 3$ and $p \nmid a$ there is an integer t such that

$$3at \equiv -4b \pmod{p^{2k}},$$

where $k = [s_p/2]$. We note that $2k \le s_p$. Then

$$\begin{aligned} 3^4a^4(t^4 + at + b) &= (3at)^4 + 3^3a^4(3at) + 3^4a^4b \\ &\equiv (-4b)^4 + 3^3a^4(-4b) + 3^4a^4b \pmod{p^{2k}} \\ &\equiv \Delta b \pmod{p^{2k}} \\ &\equiv 0 \pmod{p^{2k}} \end{aligned}$$

so that $t^4 + at + b \equiv 0 \pmod{p^{2k}}$. Also

$$\begin{aligned} 3^3a^3(4t^3 + a) &= 4(3at)^3 + 3^3a^4 \\ &\equiv 4(-4b)^3 + 3^3a^4 \pmod{p^{2k}} \\ &\equiv -\Delta \pmod{p^{2k}} \\ &\equiv 0 \pmod{p^{2k}} \end{aligned}$$

so that $4t^3 + a \equiv 0 \pmod{p^k}$. Thus t is a solution of (2.9).

We now show that (2.3) does not have a solution for $k = [s_p/2] + 1$. We note that $2k > s_p$. Suppose that t is a solution of the pair of congruences (2.9) with $k = [s_p/2] + 1$. As in (ii) we have

$$\Delta = 2^8(R^3 - 3bR^2 + 3b^2R) - 18a^2S^2 - 8aS^3 - S^4,$$

where $R = t^4 + at + b$ and $S = 4t^3 + a$. Now

$$p^{2k} \mid R, \quad p^k \mid S,$$

so

$$\Delta \equiv 0 \pmod{p^{2k}},$$

contradicting $p^{s_p} \parallel \Delta$. We have proved that $k = [s_p/2]$. Note that if t is a solution of (2.3), then it follows from Theorem 1.1 that $\frac{(t^3+a)+t^2\theta+t\theta^2+\theta^3}{p^k}$ is a p-integral element of K. Since $\nu_p(d(K)) = s_p - 2[s_p/2]$,

$$\left\{1,\ \theta,\ \theta^2,\ \frac{(t^3+a)+t^2\theta+t\theta^2+\theta^3}{p^k}\right\}$$

is a p-integral basis of K, in agreement with (2.4).

We show next that in the case $\nu_2(a) \geq 3$, $\nu_2(b) = 2$, a 2-integral basis of K cannot be given in the form (2.4) for any integer t. First we treat the case $\nu_2(a) = 3$. Suppose that there exists a 2-integral basis of the form (2.4) with $j = k = 1$ for some integer t. (Theorem 2.1(b) ensures that $j = k = 1$.) Then there exist integers C, D and E such that

$$\frac{(t^3+a)+t^2\theta+t\theta^2+\theta^3}{2^2} = \frac{2\theta+\theta^3}{2^2} + \frac{C\theta^2}{2} + D\theta + E.$$

Equating coefficients of θ we obtain $t^2 = 2+4D$, so that $t^2 \equiv 2 \pmod 4$, a contradiction. Next we treat the case $\nu_2(a) \geq 4$. Suppose that there exists a 2-integral basis of the form (2.4) with $j = 2$ and

$$k = \begin{cases} 1, & \text{if } a = 16A,\ b = 4+16B,\ A+B \equiv 0 \pmod 2, \\ 0, & \text{otherwise,} \end{cases}$$

in accordance with Theorem 2.1(b), for some integer t. Then there exist integers R and S such that

$$\frac{3t^2+2t\theta+\theta^2}{2^2} = \frac{2+\mu\theta+\theta^2}{2^2} + R\theta + S,$$

where

$$\mu = \begin{cases} 2, & \text{if } b \equiv 4 \pmod{16}, \\ 0, & \text{if } b \equiv 12 \pmod{16}. \end{cases}$$

Equating constant terms, we obtain $3t^2 = 2+4S$, so that $t^2 \equiv 2 \pmod 4$, a contradiction.

3. A Simple Method for finding an Integral Basis of a Quartic Field defined by a Trinomial $x^4 + ax + b$

In this section we give a system of polynomial congruences, which is such that an integral basis of K is given very simply in terms of a simultaneous solution t of the congruences. We use Theorem 2.1 and the following two lemmas in order to give an integral basis of K in Theorem 3.1. We treat a special case in Theorem 3.2. The following lemma is an immediate consequence of Theorem 2.1.

Lemma 3.1. *Suppose that* $v_2(a) \geq 3,\ v_2(b) = 2$ *does not hold. For each prime p, let* j_p *and* k_p *denote the maximum j and k in Theorem* 2.1(a), *respectively. Then*

(a) *The largest positive integer m such that* $m^4 \mid \Delta$ *and the system of congruences*

$$t^4 + at + b \equiv 0 \pmod{m^2 m'},$$

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

$$6t^2 \equiv 0 \pmod{m} \tag{3.1}$$

is solvable for t, is $m = \prod p^{j_p}$, *where*

$$m' = \frac{m}{\displaystyle\prod_{\substack{v_p(a)\geq 2 \text{ and } v_p(b)=2, \text{ or} \\ v_2(a)\geq 2 \text{ and } v_2(b)=0}} p^{j_p}}. \tag{3.2}$$

(b) *Let* $m = \prod p^{j_p}$ *be as in part* (a). *The largest positive integer n such that* $n^2 \mid \Delta/m^4$ *and both the system of congruences* (3.1) *and the system of congruences*

$$t^4 + at + b \equiv 0 \pmod{mn^2},$$

$$4t^3 + a \equiv 0 \pmod{mn},$$

$$6t^2 \equiv 0 \pmod{m} \tag{3.3}$$

are simultaneously solvable for t, *is* $n = \prod p^{k_p}$.

By Lemma 2.1 we have $j_p \leq 1$ for each p. If $k_p \geq j_p$ for each p, then $m \mid n$ and a solution t of (3.3) is also a solution of (3.1). If $n = 1$, then a solution t of (3.1) is also a solution of (3.3). If $n \neq 1$ and there is a prime such that $j_p = 1$ and $k_p = 0$, then a solution t of (3.3) may not be a solution of (3.1), or vice versa. For this reason, when we refer to a solution t of (3.1) or (3.3), we always mean a simultaneous solution t of (3.1) and (3.3).

In the proof of Theorem 3.1, we make use of the simple properties given in the following lemma. We use the same notation as in Lemma 3.1.

Lemma 3.2. *Suppose that* $\nu_2(a) \geq 3$, $\nu_2(b) = 2$ *does not hold. Let* m, m' *and* n *be given by* (3.1), (3.2) *and* (3.3), *respectively. Then*

(a) $\left(\prod_{\substack{\nu_p(a) \geq 2 \text{ and } \nu_p(b) = 2, \text{ or} \\ \nu_2(a) \geq 2 \text{ and } \nu_2(b) = 0}} p^{j_p} \right) \Big| \, 2t,$

(b) $m \mid 2tn$,

(c) $m^3 \mid 2t(t^4 + at + b)$,

where t *is a simultaneous solution of* (3.1) *and* (3.3).

Proof. (a) Note that if $\nu_2(a) \geq 2$ and $\nu_2(b) = 0, 2$, then it follows from (2.1) that $j_2 \in \{0, 1\}$. If $\nu_p(b) = 2$ and $\nu_p(a) \geq 2$ for $p \neq 2$, then it follows from (3.1) (or (2.1)) that $j_p = 1$ and $p \mid t$. This completes the proof of part (a).

(b) Let p be a prime which does not satisfy

$$\nu_p(a) \geq 2,\ \nu_p(b) = 2 \text{ or } \nu_2(a) \geq 2,\ \nu_2(b) = 0.$$

Then, by (3.2), we have $p^{j_p} \parallel m'$. From (3.1) the system of congruences

$$t^4 + at + b \equiv 0 \pmod{p^{3j_p}},$$

$$4t^3 + a \equiv 0 \pmod{p^{2j_p}},$$

$$6t^2 \equiv 0 \pmod{p^{j_p}}$$

is solvable for t. From (3.3) the largest integer k such that the system of congruences

$$t^4 + at + b \equiv 0 \pmod{p^{j_p+2k}},$$

$$4t^3 + a \equiv 0 \pmod{p^{j_p+k}},$$

$$6t^2 \equiv 0 \pmod{p^{j_p}}$$

is solvable for t, is $k = k_p$. Hence $j_p \leq k_p$, and so $m' \mid n$. By part (a) $\frac{m}{m'} \mid 2t$. So $m \mid 2tm'$. Thus $m \mid 2tn$.

(c) From (3.1), we have $m'm^2 \mid t^4 + at + b$. Since by part (a) we have $m \mid 2tm'$, $m^3 \mid 2t(t^4 + at + b)$.

We now use Lemmas 3.1 and 3.2 to give a simple method for finding an integral basis for K in Theorem 3.1 when $\nu_2(a) \geq 3$, $\nu_2(b) = 2$ does not hold. We treat the case $\nu_2(a) \geq 3$, $\nu_2(b) = 2$ in Theorem 3.2.

Theorem 3.1. *Suppose that* $\nu_2(a) \geq 3$, $\nu_2(b) = 2$ *does not hold.*

Let m^4 *be the largest fourth power dividing* Δ *for which the system of congruences* (3.1) *is solvable for* t.

Let n^2 *be the largest square dividing* Δ / m^4 *for which the systems of congruences* (3.1) *and* (3.3) *are simultaneously solvable for* t.

Then an integral basis for K *is given by*

$$\left\{1,\ \theta,\ \frac{3t^2 + 2t\theta + \theta^2}{m},\ \frac{(t^3 + a) + t^2\theta + t\theta^2 + \theta^3}{mn}\right\},$$

and the discriminant of K is

$$d(K) = \frac{\Delta}{m^4 n^2},$$

where t is a simultaneous solution of the systems of congruences (3.1) *and* (3.3).

Proof. Let t be a simultaneous solution of the systems of the congruences (3.1) and (3.3). It can be verified that $\frac{(t^3 + a) + t^2\theta + t\theta^2 + \theta^3}{mn}$ is a root of

$$p(x) = x^4 - \frac{(4t^3 + a)}{mn} x^3 + \frac{6t^2(t^4 + at + b)}{m^2 n^2} x^2 - \frac{4t(t^4 + at + b)^2}{m^3 n^3} x + \frac{(t^4 + at + b)^3}{m^4 n^4}$$

and that $\frac{3t^2 + 2t\theta + \theta^2}{m}$ is a root of

$$q(x) = x^4 - \frac{12t^2}{m} x^3 + \frac{54t^4 + 6at + 2b}{m^2} x^2 - \frac{108t^6 - 4bt^2 + 28at^3 + a^2}{m^3} x + \frac{81t^8 + 30at^5 - 14bt^4 + b^2 + 3a^2t^2 - 2abt}{m^4}.$$

We first show that the coefficients of $p(x)$ are integers. Since $mn \mid 4t^3 + a$, $\frac{4t^3 + a}{mn}$ is an integer. Since $m \mid 6t^2$ and $mn^2 \mid t^4 + at + b$, $\frac{6t^2(t^4 + at + b)}{m^2 n^2}$ is an integer. Since $mn^2 \mid t^4 + at + b$ and $m \mid 2tn$ (by Lemma 3.2(b)), $\frac{4t(t^4 + at + b)^2}{m^3 n^3}$ is an integer. Since $m^2 n^4 \mid (t^4 + at + b)^2$ and $m^2 \mid t^4 + at + b$, $\frac{(t^4 + at + b)^3}{m^4 n^4}$ is an integer. Hence all the coefficients of $p(x)$ are integers. Thus $\frac{(t^3+a)+t^2\theta+t\theta^2+\theta^3}{mn}$ is an integral element of K.

To show that the coefficients of $q(x)$ are integers, we rewrite $q(x)$ as

$$q(x) = x^4 - \frac{12t^2}{m}x^3 + \frac{4t(4t^3+a)+2(t^4+at+b)+(6t^2)^2}{m^2}x^2$$

$$-\frac{4t(6t^2)(4t^3+a)+(4t^3+a)^2-4t^2(t^4+at+b)}{m^3}x$$

$$+\frac{-4t(t^4+at+b)(4t^3+a)+6t^2(4t^3+a)^2+(t^4+at+b)^2}{m^4}.$$

As $m \mid 6t^2$, $\frac{12t^2}{m}$ is an integer. Since $m^2 \mid 4t^3+a$, $m^2 \mid t^4+at+b$ and $m \mid 6t^2$,

$$\frac{4t(4t^3+a)+2(t^4+at+b)+(6t^2)^2}{m^2}$$

is an integer. By Lemma 3.2(c), $m^3 \mid 2t(t^4+at+b)$. Since $m \mid 6t^2$ and $m^2 \mid 4t^3+a$,

$$\frac{4t(6t^2)(4t^3+a)+(4t^3+a)^2-4t^2(t^4+at+b)}{m^3}$$

is an integer. Since $m^2 \mid 4t^3+a$ and $m^2 \mid t^4+at+b$,

$$\frac{-4t(t^4+at+b)(4t^3+a)+6t^2(4t^3+a)^2+(t^4+at+b)^2}{m^4}$$

is an integer. Hence all the coefficients of $q(x)$ are integers. Thus, $\frac{3t^2+2t\theta+\theta^2}{m}$ is an integral element of K. Next we have

$$d(K) = \operatorname{sgn}(d(K))|\, d(K)\,|$$

$$= \operatorname{sgn}(\Delta/i(\theta)^2)\prod_p p^{\nu_p(d(K))} \quad \text{(by (1.2))}$$

$$= \operatorname{sgn}(\Delta)\prod_p p^{s_p - 2(2j_p + k_p)} \quad \text{(by Theorem 2.1)}$$

$$= \operatorname{sgn}(\Delta)\frac{\prod_p p^{s_p}}{\left(\prod_p p^{j_p}\right)^4 \left(\prod_p p^{k_p}\right)^2}$$

$$= \frac{\operatorname{sgn}(\Delta)|\,\Delta\,|}{m^4 n^2} \quad \text{(by Lemma 3.1)}$$

so that

$$d(K) = \frac{\Delta}{m^4 n^2}$$

as asserted. Since

$$d\left(1,\ \theta,\ \frac{3t^2 + 2t\theta + \theta^2}{m},\ \frac{(t^3 + a) + t^2\theta + t\theta^2 + \theta^3}{mn}\right)$$

$$= \frac{d(1,\ \theta,\ \theta^2,\ \theta^3)}{m^4 n^2} = \frac{\Delta}{m^4 n^2} = d(K),$$

we deduce that

$$\left\{1,\ \theta,\ \frac{3t^2 + 2t\theta + \theta^2}{m},\ \frac{(t^3 + a) + t^2\theta + t\theta^2 + \theta^3}{mn}\right\}$$

is an integral basis for K. This completes the proof of the theorem.

In the following theorem we give a simple method for finding an integral basis for K when $\nu_2(a) \geq 3$, $\nu_2(b) = 2$. The proof can be given similarly to the proof of Theorem 3.1.

Note that when $\nu_2(a) \geq 3$, $\nu_2(b) = 2$, an integral basis for K cannot be given using Theorem 3.1. See the explanation at the end of Section 2.

Theorem 3.2. *Suppose that* $\nu_2(a) \geq 3$, $\nu_2(b) = 2$, *and let*

$$\left\{1,\ \theta,\ \frac{u_2 + v_2\theta + \theta^2}{2^j},\ \frac{x_2 + y_2\theta + z_2\theta^2 + \theta^3}{2^{j+k}}\right\}$$

be a 2*-integral basis of K as given in Theorem* 2.1(b).

Let m^4 *be the largest fourth power dividing* $\frac{\Delta}{2^{4j+2k}}$ *for which the system of congruences* (3.1) *is solvable for* t.

Let n^2 *be the largest square dividing* $\frac{\Delta}{2^{4j+2k}m^4}$ *for which the systems of congruences* (3.1) *and* (3.3) *are simultaneously solvable for* t.

Then an integral basis for K is given by

$$\left\{1,\ \theta,\ \frac{u + v\theta + \theta^2}{2^j \cdot m},\ \frac{x + y\theta + z\theta^2 + \theta^3}{2^{j+k} \cdot mn}\right\},$$

where

$$u \equiv u_2 \pmod{2^j}, \quad u \equiv 3t^2 \pmod{m},$$

$$v \equiv v_2 \pmod{2^k}, \quad v \equiv 2t \pmod{m},$$

and

$$x \equiv x_2 \pmod{2^{j+k}}, \quad x \equiv t^3 + a \pmod{mn},$$

$$y \equiv y_2 \pmod{2^{j+k}}, \quad y \equiv t^2 \pmod{mn},$$

$$z \equiv z_2 \pmod{2^{j+k}}, \quad z \equiv t \pmod{mn},$$

where t is a simultaneous solution of (3.1) *and* (3.3), *and the discriminant of K is*

$$d(K) = \frac{\Delta}{2^{4j+2k}m^4n^2}.$$

4. Examples

Example 4.1. Let $K = Q(\theta)$, where $\theta^4 + a\theta + b = 0$, with $a = 72 = 2^3 \cdot 3^2$ and $b = 27 = 3^3$. Thus $\Delta = -2^8 \cdot 3^9 \cdot 11 \cdot 13$. Since $v_2(a) \geq 3$, $v_2(b) = 2$ does not hold, we can use Theorem 3.1 to give an integral basis for K. The system of congruences (3.1) is solvable when $m = 6$ and $m' = 3$, and a solution is $t = 3$. Note that $6^4 \mid \Delta$, and $m = 6$ is the largest integer such that $m^4 \mid \Delta$ and the system of congruences (3.1) is solvable for t. The system of congruences (3.3) is solvable when $m = 6$ and $n = 3$, and a solution is $t = 3$. Note that $3^2 \mid \Delta/6^4$, and $n = 3$ is the largest integer such that $n^2 \mid \Delta/m^4$ and the system of congruences (3.3) is solvable for t. Hence by Theorem 3.1 an integral basis for K is given by

$$\left\{1,\ \theta,\ \frac{3+\theta^2}{6},\ \frac{9+9\theta+3\theta^2+\theta^3}{6\cdot 3}\right\}$$

and

$$d(K) = \Delta/m^4n^2 = -2^8 \cdot 3^9 \cdot 11 \cdot 13/6^4 \cdot 3^2 = -2^4 \cdot 3^3 \cdot 11 \cdot 13.$$

Example 4.2. Let $K = Q(\theta)$, where $\theta^4 + a\theta + b = 0$, with $a = 4 = 2^2$ and $b = 4 = 2^2$. Thus $\Delta = 2^8 \cdot 37$. Since $v_2(a) \geq 3$, $v_2(b) = 2$ does not hold, we can use Theorem 3.1 to give an integral basis for K. The system of congruences (3.1) is solvable when $m = 2$, $m' = 1$, and a solution is $t = 0$. Note that $2^4 \mid \Delta$, and $m = 2$ is the largest integer such that $m^4 \mid \Delta$ and the system of congruences (3.1) is solvable for t. The system of congruences (3.3) is solvable when $m = 2$ and $n = 1$, and a solution is $t = 0$. Note that the largest integer n such that $n^2 \mid \Delta/m^4$ and the system of congruences (3.3) is solvable for t is $n = 1$. Hence by Theorem 3.1 an integral basis for K is given by

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

and

$$d(K) = \Delta/m^4n^2 = 2^8 \cdot 37/2^4 = 2^4 \cdot 37.$$

Example 4.3. Let $K = Q(\theta)$, where $\theta^4 + a\theta + b = 0$, with $a = 100 = 2^2 \cdot 5^2$ and $b = 375 = 3 \cdot 5^3$. Thus $\Delta = 2^{10} \cdot 3^3 \cdot 5^8$. Since $v_2(a) \geq 3$, $v_2(b) = 2$ does not hold, we can use Theorem 3.1 to give an integral basis for K. The system of congruences (3.1) is solvable when $m = 10$, $m' = 5$, and a solution is $t = 5$. Note that $10^4 \mid \Delta$, and $m = 10$ is the largest integer such that $m^4 \mid \Delta$ and the system of congruences (3.1) is solvable for t. The system of congruences (3.3) is solvable when $m = 10$ and $n = 5$, and a solution is $t = 5$. Note that $5^2 \mid \Delta/10^4$, and $n = 5$ is the largest integer such that $n^2 \mid \Delta/m^4$ and the system of congruences (3.3) is solvable for t. Hence by Theorem 3.1 an integral basis for K is given by

$$\left\{1, \theta, \frac{5 + \theta^2}{10}, \frac{25 + 25\theta + 5\theta^2 + \theta^3}{10 \cdot 5}\right\}$$

and

$$d(K) = \Delta/m^4n^2 = 2^{10} \cdot 3^3 \cdot 5^8/10^4 \cdot 5^2 = 2^6 \cdot 3^3 \cdot 5^2.$$

Example 4.4. Let $K = Q(\theta)$, where $\theta^4 + a\theta + b = 0$, with $a = 225 = 3^2 \cdot 5^2$ and $b = 10125 = 3^4 \cdot 5^3$. Thus $\Delta = 3^{11} \cdot 5^8 \cdot 11 \cdot 349$. Since $v_2(a) \geq 3$, $v_2(b) = 2$ does not hold, we can use Theorem 3.1 to give an integral basis for K. The system of congruences (3.1) is solvable when $m = 15$, $m' = 15$, and a solution is $t = 0$. Note that $15^4 \mid \Delta$, and $m = 15$ is the largest integer such that $m^4 \mid \Delta$ and the system of congruences (3.1) is solvable for t. The system of congruences (3.3) is solvable when $m = 15$ and $n = 15$, and a solution is $t = 0$. Note that $15^2 \mid \Delta/15^4$, and $n = 15$ is the largest integer such that $n^2 \mid \Delta/m^4$ and the system of congruences (3.3) is solvable for t. Hence by Theorem 3.1 an integral basis for K is given by

$$\left\{1,\ \theta,\ \frac{\theta^2}{15},\ \frac{\theta^3}{15 \cdot 15}\right\}$$

and

$$d(K) = \Delta/m^4n^2 = 3^{11} \cdot 5^8 \cdot 11 \cdot 349/15^4 \cdot 15^2 = 3^5 \cdot 5^2 \cdot 11 \cdot 349.$$

Example 4.5. Let $K = Q(\theta)$, where $\theta^4 + a\theta + b = 0$, with $a = 56 = 2^3 \cdot 7$ and $b = 196 = 2^2 \cdot 7^2$. Thus $\Delta = 2^{12} \cdot 7^4 \cdot 13^2$. Since $\nu_2(a) \geq 3$ and $\nu_2(b) = 2$, we cannot use Theorem 3.1. We make use of Theorem 3.2. Since $\nu_2(a) = 3$, by Theorem 2.1(b), a 2-integral basis of K is

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

So $j = k = 1$. Then with the notation of Theorem 3.2 and Lemma 3.1, $m = m' = 1$, $n = 91$ and $t = 56$. Hence, by Theorem 3.2, an integral basis for K is given by

$$\left\{1,\ \theta,\ \frac{\theta^2}{2},\ \frac{224 + 42\theta + 56\theta^2 + \theta^3}{2^2 \cdot 91}\right\}$$

and

$$d(K) = \frac{\Delta}{2^{4j+2k}m^4n^2} = 2^{12} \cdot 7^4 \cdot 13^2/2^6 \cdot 91^2 = 2^6 \cdot 7^2.$$

Note that

$$224 \equiv 0 \pmod{2^2}, \quad 224 \equiv t^3 + a \pmod{mn},$$

$$42 \equiv 2 \pmod{2^2}, \quad 42 \equiv t^2 \pmod{mn},$$

$$56 \equiv 0 \pmod{2^2}, \quad 56 \equiv t \pmod{mn}.$$

Example 4.6. Let $K = Q(\theta)$, where $\theta^4 + a\theta + b = 0$, with $a = 80 = 2^4 \cdot 5$ and $b = 20 = 2^2 \cdot 5$. Thus $\Delta = -2^{14} \cdot 5^3 \cdot 7^2 \cdot 11$. Since $\nu_2(a) \geq 3$ and $\nu_2(b) = 2$, we cannot use Theorem 3.1. We make use of Theorem 3.2. Since $a = 16A$, $b = 4 + 16B$ and $A + B \equiv 0 \pmod 2$ with $A = 5$ and

$B = 1,$ by Theorem 2.1(b), a 2-integral basis of K is

$$\left\{1,\ \theta,\ \frac{2+2\theta+\theta^2}{2^2},\ \frac{6\theta+2\theta^2+\theta^3}{2^3}\right\}.$$

So $j = 2$ and $k = 1$. Then with the notation of Theorem 3.2 and Lemma 3.1, $m = m' = 1$, $n = 7$ and $t = 2$. Hence, by Theorem 3.2, an integral basis for K is given by

$$\left\{1,\ \theta,\ \frac{2+2\theta+\theta^2}{2^2},\ \frac{32+46\theta+2\theta^2+\theta^3}{2^3\cdot 7}\right\}$$

and

$$d(K) = \frac{\Delta}{2^{4j+2k}m^4n^2} = -2^{14}\cdot 5^3\cdot 7^2\cdot 11/2^{10}\cdot 7^2 = -2^4\cdot 5^3\cdot 11.$$

Note that

$$32 \equiv 0 \ (\text{mod } 2^3),\quad 32 \equiv t^3 + a \ (\text{mod } mn),$$

$$46 \equiv 6 \ (\text{mod } 2^3),\quad 46 \equiv t^2 \ (\text{mod } mn),$$

$$2 \equiv 2 \ (\text{mod } 2^3),\quad 2 \equiv t \ (\text{mod } mn).$$

Remark 4.1. The formulation of an integral basis of a quartic field given in [4] is incorrect. Counterexamples can be produced easily. For example, for $a = 4$ and $b = 4$, the results in [4] assert that $\{1, \theta, \theta^2, \theta^3\}$ is an integral basis. However, in Example 4.2 we showed that an integral basis is

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

Note that $\theta^2/2$ and $\theta^3/2$ are integral elements since $\theta^2/2$ is a root of the monic polynomial

$$p(x) = x^4 + 2x^2 - 2x + 1.$$

Indeed it is easily seen that for $\nu_2(a) = \nu_2(b) = 2,$ the formulation of an integral basis of a quartic field given in [4] is always incorrect.

References

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

[2] Ş. Alaca and K. S. Williams, p-integral bases of a quartic field defined by a trinomial $x^4 + ax + b$, Far East J. Math. Sci. (FJMS) 12 (2004), to appear.

[3] H. Cohen, A Course in Computational Algebraic Number Theory, Fourth Printing, Springer-Verlag, Berlin, Heidelberg, New York, 2000.

[4] D. G. Grebenyuk, On the theory of algebraic integers depending on a root of an irreducible equation of fourth degree, Izv. Akad. Nauk. UzSSR Ser. Fiz-Mat. 6 (1958), 27-47 (Russian, Uzbek summary).

■