Far East J. Math. Sci. (FJMS) 14(3) (2004), 273-282

THE FACTORIZATION OF 2 IN CUBIC FIELDS WITH INDEX 2

SABAN ALACA, BLAIR K. SPEARMAN

and

KENNETH S. WILLIAMS

(Received April 7, 2004)

Submitted by K. K. Azad

Abstract

We give the explicit factorization of the principal ideal $\langle 2 \rangle$ in cubic fields with index 2.

Let K be an algebraic number field. Let O_K denote the ring of integers of K. Let $d(K)$ denote the discriminant of K. Let $\theta \in O_K$ be such that $K = \mathbb{Q}(\theta)$. The minimal polynomial of θ over $\mathbb{Q}$ is denoted by $\mathrm{irr}_{\mathbb{Q}}(\theta)$. The discriminant $D(\theta)$ and the index $\mathrm{ind}(\theta)$ of θ are related by the equation

$$D(\theta) = (\mathrm{ind}(\theta))^2 d(K). \tag{1}$$

If p is a prime not dividing $\mathrm{ind}(\theta)$, then it is well known that the following theorem of Dedekind gives explicitly the factorization of the

2000 Mathematics Subject Classification: Primary 11R16, 11R29.

Key words and phrases: cubic field, discriminant, prime decomposition.

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

principal ideal $\langle p \rangle$ of O_K into prime ideals in terms of the irreducible factors of the minimal polynomial $\mathrm{irr}_{\mathbb{Q}}(\theta)$ modulo p, see for example [2, Theorem 10.5.1, p. 257].

Theorem 1. *Let $K = \mathbb{Q}(\theta)$ be an algebraic number field with $\theta \in O_K$. Let p be a rational prime. Let*

$$f(x) = \mathrm{irr}_{\mathbb{Q}}(\theta) \in \mathbb{Z}[x].$$

Let $\bar{}$ denote the natural map : $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$, where $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$. Let

$$\bar{f}(x) = g_1(x)^{e_1} \cdots g_r(x)^{e_r},$$

where $g_1(x)$, ..., $g_r(x)$ are distinct irreducible polynomials in $\mathbb{Z}_p[x]$ and e_1, ..., e_r are positive integers. For $i = 1, 2, \ldots, r$ let $f_i(x)$ be any polynomial of $\mathbb{Z}[x]$ such that $\bar{f}_i = g_i$ and $\deg(f_i) = \deg(g_i)$. Set

$$P_i = \langle p, f_i(\theta) \rangle, \quad i = 1, 2, \ldots, r.$$

If $\mathrm{ind}(\theta) \not\equiv 0 \pmod{p}$, then P_1, ..., P_r are distinct prime ideals of O_K with

$$\langle p \rangle = P_1^{e_1} \cdots P_r^{e_r}$$

and

$$N(P_i) = p^{\deg f_i}, \quad i = 1, 2, \ldots, r.$$

On the other hand if p is a prime dividing $\mathrm{ind}(\theta)$, then this theorem does not apply. One might try to change θ to obtain a different index but in the case where p is a common index divisor it is impossible to find an element θ for which p does not divide $\mathrm{ind}(\theta)$. The only approach left is the Buchmann-Lenstra algorithm [3, p. 315] for decomposing a prime in a number field.

In this paper we treat the case where K is a cubic field such that the prime $p = 2$ is a common index divisor. This is the only possible nontrivial common index divisor for a cubic field [4, p. 234], [5, p. 585]. In other words the cubic field K has index 2. We give explicitly the two-element representation of the prime ideals which appear in the

factorization of $\langle 2 \rangle$ in O_K. The form of the prime ideal factorization has been given by Llorente and Nart [5, Theorem 1, p. 580].

It is well known that K can be given in the form $K = \mathbb{Q}(\theta)$, where θ is a root of the irreducible polynomial

$$f(x) = x^3 - ax + b, \quad a, b \in \mathbb{Z}, \tag{2}$$

so that $\mathrm{irr}_{\mathbb{Q}}(\theta) = f(x)$. Moreover it is further known that a and b can be chosen so that there are no primes p with $p^2 \mid a$ and $p^3 \mid b$. We set

$$\Delta := D(\theta) = 4a^3 - 27b^2, \quad s_p = v_p(\Delta), \quad \Delta_p = \Delta/p^{s_p},$$

where $v_p(k)$ denotes the largest nonnegative integer m such that p^m divides the nonzero integer k. From (1) we deduce that

$$v_p(\mathrm{ind}(\theta)) = \frac{1}{2}(s_p - v_p(d(K))).$$

The determination of $v_p(d(K))$ was carried out by Llorente and Nart [5, Theorem 2, p. 583] in 1983, see also Alaca [1]. We need the following result of Llorente and Nart [5, Theorem 4, p. 585] giving a necessary and sufficient condition for the index of K to be 2.

Theorem 2. *Let $K = \mathbb{Q}(\theta)$ be a cubic field, where θ is a root of $x^3 - ax + b$ and the integers a and b are such that there does not exist a rational prime p with $p^2 \mid a$ and $p^3 \mid b$. Then the index of the field K equals 2 if and only if*

$$a \equiv 1 \pmod 2, \quad b \equiv 0 \pmod 2, \quad s_2 \equiv 0 \pmod 2 \quad \textit{and} \quad \Delta_2 \equiv 1 \pmod 8. \tag{3}$$

We note that condition (3) splits into two cases:

$$a \equiv 1 \pmod 4, \quad b \equiv 0 \pmod 4, \quad \Delta_2 \equiv 1 \pmod 8, \tag{4}$$

and

$$a \equiv 3 \pmod 4, \quad b \equiv 2 \pmod 4, \quad s_2 \equiv 0 \pmod 2, \quad \Delta_2 \equiv 1 \pmod 8. \tag{5}$$

If (4) holds, we have $s_2 = 2$ and if (5) holds, then $s_2 \geq 4$. When K is a

cubic field of index 2, we know from [5, p. 585] that

$$\langle 2\rangle = PQR, \text{ where } P, Q \text{ and } R \text{ are distinct prime ideals.} \tag{6}$$

Clearly $N(P) = N(Q) = N(R) = 2$. We prove the following theorem, which gives the prime ideals P, Q and R explicitly.

Theorem 3. *Let $K = \mathbb{Q}(\theta)$ be a cubic field, where θ is a root of $x^3 - ax + b$ and a and b are integers such that there are no primes p with $p^2 \mid a$ and $p^3 \mid b$. Suppose that the index of the field K is equal to 2 so that (6) holds and either (4) or (5) holds.*

If (4) holds, then

$$P = \langle 2, \theta\rangle, \quad Q = \left\langle 2, \frac{2 + \theta + \theta^2}{2}\right\rangle, \quad R = \left\langle 2, \frac{2 + 3\theta + \theta^2}{2}\right\rangle.$$

If (5) holds, then

$$P = \langle 2, \theta\rangle, \quad Q = \langle 2, \alpha\rangle, \quad R = \langle 2, \theta + \alpha\rangle,$$

where

$$\alpha = \frac{x + y\theta + \theta^2}{2^{m+1}}, \quad m = \frac{s_2 - 2}{2} \geq 1,$$

and x and y are integers satisfying

$$3x \equiv -2a \pmod{2^{2m+3}}, \quad ay \equiv \frac{3b}{2} + 2^m \pmod{2^{2m+3}}.$$

Proof. Let $K = \mathbb{Q}(\theta)$ be a cubic field of index 2, where θ is a root of $x^3 - ax + b$ with the restriction that there are no rational primes p such that $p^2 \mid a$ and $p^3 \mid b$. By the remarks following Theorem 2, (6) holds and either (4) or (5) holds.

First we suppose that (4) holds. Then

$$a - b \equiv a - 4\left(\frac{b}{4}\right) \equiv a - 4\left(\frac{b}{4}\right)^2 \equiv a - 108\left(\frac{b}{4}\right)^2 \equiv a^3 - 27\left(\frac{b}{2}\right)^2$$

$$\equiv \frac{4a^3 - 27b^2}{4} \equiv \frac{\Delta}{4} \equiv \Delta_2 \equiv 1 \pmod 8,$$

so we can define integers A and B by

$$a = 8A + 4B + 1, \quad b = 4B.$$

From the work of Alaca [1, Table A, p. 1951] we know that $\{1, \theta, \phi\}$ is a 2-integral basis of O_K, where

$$\phi = \frac{\theta + \theta^2}{2}.$$

Set

$$\alpha = \theta, \quad \beta = 1 + \phi, \quad \gamma = 1 + \theta + \phi.$$

We have

$$\theta^2 = -\theta + 2\phi,$$

$$\theta^3 = -4B + (8A + 4B + 1)\theta,$$

$$\theta^4 = -(8A + 8B + 1)\theta + (16A + 8B + 2)\phi.$$

Hence

$$\theta\phi = \frac{\theta^2 + \theta^3}{2} = -2B + (4A + 2B)\theta + \phi$$

and

$$\phi^2 = \frac{\theta^2 + 2\theta^3 + \theta^4}{4} = -2B + 2A\theta + (4A + 2B + 1)\phi.$$

Thus

$$\alpha\beta = \theta + \theta\phi = -2B + (4A + 2B + 1)\theta + \phi$$

and

$$\begin{aligned}\gamma + \gamma^2 &= 2 + \theta^2 + \phi^2 + 3\theta + 3\phi + 2\theta\phi \\ &= (2 - 6B) + (2 + 10A + 4B)\theta + (8 + 4A + 2B)\phi\end{aligned}$$

so that $(\gamma + \gamma^2)/2 \in O_K$. Hence

$$\langle 2, \gamma\rangle\langle 2, \gamma + 1\rangle = \langle 4, 2\gamma, 2\gamma + 2, \gamma + \gamma^2\rangle = \langle 2, \gamma + \gamma^2\rangle = \langle 2\rangle.$$

Similarly

$$\langle 2, \alpha\rangle\langle 2, \alpha + 1\rangle = \langle 2, \beta\rangle\langle 2, \beta + 1\rangle = \langle 2\rangle.$$

Next

$$\begin{aligned}\langle 2, \alpha\rangle\langle 2, \beta\rangle &= \langle 4, 2\alpha, 2\beta, \alpha\beta\rangle \\ &= \langle 4, 2\theta, 2 + 2\phi, -2B + (4A + 2B + 1)\theta + \phi\rangle \\ &= \langle 4, 2\theta, 2 + 2\phi, -2B + \theta + \phi\rangle \\ &= \langle 4, 2\theta, 2 + 2\phi - 2(-2B + \theta + \phi), -2B + \theta + \phi\rangle \\ &= \langle 4, 2\theta, 2, -2B + \theta + \phi\rangle \\ &= \langle 2, \theta + \phi\rangle \\ &= \langle 2, \gamma + 1\rangle.\end{aligned}$$

Thus

$$\langle 2, \alpha\rangle\langle 2, \beta\rangle\langle 2, \gamma\rangle = \langle 2, \gamma + 1\rangle\langle 2, \gamma\rangle = \langle 2\rangle.$$

Suppose that $\langle 2, \alpha\rangle = \langle 1\rangle$. Then $\langle 2, \alpha + 1\rangle = \langle 2\rangle$ so that $\alpha + 1 \in \langle 2\rangle$ and thus

$$\frac{1 + \theta}{2} = \frac{1 + \alpha}{2} \in O_K.$$

This contradicts that $(1 + \theta)/2$ is not a 2-integral element of O_K. Hence we have $\langle 2, \alpha\rangle \neq \langle 1\rangle$. Similarly we can show that $\langle 2, \beta\rangle \neq \langle 1\rangle$ and $\langle 2, \gamma\rangle \neq \langle 1\rangle$. Thus we can choose

$$P = \langle 2, \alpha\rangle = \langle 2, \theta\rangle,$$

$$Q = \langle 2, \beta\rangle = \langle 2, 1 + \phi\rangle = \left\langle 2, \frac{2 + \theta + \theta^2}{2}\right\rangle,$$

$$R = \langle 2, \gamma\rangle = \langle 2, 1 + \theta + \phi\rangle = \left\langle 2, \frac{2 + 3\theta + \theta^2}{2}\right\rangle,$$

as asserted.

We now suppose that (5) holds. It is convenient to set $b = 2B$ so that B is an odd integer. As s_2 is an even integer greater than or equal to 4, we can define an integer m by

$$m = \frac{s_2 - 2}{2},$$

so that

$$m \geq 1, \quad s_2 = 2m + 2, \quad a^3 - 27B^2 \equiv 2^{2m} \pmod{2^{2m+3}}.$$

Let x and y be integers such that

$$3x \equiv -2a \pmod{2^{2m+3}}, \quad ay \equiv 3B + 2^m \pmod{2^{2m+3}}.$$

We note that

$$x \equiv 0 \pmod 2, \quad y \equiv B + 2^m \pmod 4.$$

By [1, Table A, p. 1951] $\{1, \theta, \alpha\}$ is a 2-integral basis of O_K, where

$$\alpha = \frac{x + y\theta + \theta^2}{2^{m+1}}.$$

Thus

$$\theta^2 = -x - y\theta + 2^{m+1}\alpha \equiv \theta \pmod{2O_K}.$$

We show that there exists an integer M such that

$$b + xy = (8M - 3)2^{m+1}.$$

Let v and w be integers such that $3v \equiv 1 \pmod{2^{2m+3}}$ and $aw \equiv 1 \pmod{2^{2m+3}}$, so that $x \equiv -2av \pmod{2^{2m+3}}$, $y \equiv w(3B + 2^m) \pmod{2^{2m+3}}$, and $xy \equiv -b - 2^{m+1}v \pmod{2^{2m+3}}$. Hence $2^{m+1} \mid b + xy$ and $(b + xy)/2^{m+1} \equiv -v \pmod{2^{m+2}}$. Thus $(b + xy)/2^{m+1} + 3 \equiv 3 - v \equiv 0 \pmod 8$. Therefore there is an integer M such that

$$\frac{b + xy}{2^{m+1}} + 3 = 8M,$$

which is the asserted result. Similarly we can show that there exist integers N, P, Q and R such that

$$a + x - y^2 = -3 \cdot 2^{2m+1} - 3B2^{m+1} + 2^{m+4}N,$$

$$a + 2x + y^2 = 3 \cdot 2^{2m+1} + 3B2^{m+1} + 2^{m+4}P,$$

$$y^3 - ay + b = 2^{2m+3}Q,$$

$$x^2 + ax + 2by + xy^2 = 2^{2m+3}R.$$

Next, as

$$\theta\alpha = -\frac{(b + xy)}{2^{m+1}} + \frac{(a + x - y^2)}{2^{m+1}}\theta + y\alpha,$$

we obtain

$$\theta\alpha = -(8M - 3) + (-3B + 8N - 3 \cdot 2^m)\theta + y\alpha$$

so that

$$\theta\alpha \equiv -1 + (B + 2^m)\theta + (B + 2^m)\alpha \pmod{4O_K}.$$

Further, as

$$\alpha^2 = -\frac{(x^2 + ax + 2by + xy^2)}{2^{2m+2}} - \frac{(y^3 - ay + b)}{2^{2m+2}}\theta + \frac{(a + 2x + y^2)}{2^{m+1}}\alpha,$$

we obtain

$$\alpha^2 = -2R - 2Q\theta + (8P + 3B + 3 \cdot 2^m)\alpha,$$

so that

$$\alpha^2 \equiv \alpha \pmod{2O_K}.$$

Hence

$$\theta^2 + \alpha^2 + \theta + \alpha \equiv 0 \pmod{2O_K}.$$

Next

$$\begin{aligned}\langle 2, \theta\rangle\langle 2, \alpha\rangle &= \langle 4, 2\theta, 2\alpha, \theta\alpha\rangle \\ &= \langle 4, 2\theta, 2\alpha, -1 + (B + 2^m)\theta + (B + 2^m)\alpha\rangle \\ &= \langle 4, 2\theta, 2\alpha, -1 + \theta + \alpha\rangle \\ &= \langle 4, 2\theta, 2\alpha, -1 + \theta + \alpha, 2(-1 + \theta + \alpha) - 2\theta - 2\alpha + 4\rangle \\ &= \langle 4, 2\theta, 2\alpha, -1 + \theta + \alpha, 2\rangle\end{aligned}$$

$$= \langle 2, -1 + \theta + \alpha \rangle$$

$$= \langle 2, 1 + \theta + \alpha \rangle.$$

Also

$$\langle 2, \theta + \alpha \rangle \langle 2, 1 + \theta + \alpha \rangle$$

$$= \langle 4, 2\theta + 2\alpha, 2\theta + 2\alpha + 2, \theta^2 + 2\theta\alpha + \alpha^2 + \theta + \alpha \rangle$$

$$= \langle 2, \theta^2 + \alpha^2 + \theta + \alpha \rangle$$

$$= \langle 2 \rangle.$$

Hence

$$\langle 2, \theta \rangle \langle 2, \alpha \rangle \langle 2, \theta + \alpha \rangle = \langle 2 \rangle.$$

Next we show that $\langle 2, \theta \rangle \neq 1$. Suppose that $\langle 2, \theta \rangle = \langle 1 \rangle$. Then $\langle 2, \alpha \rangle \langle 2, \theta + \alpha \rangle = \langle 2 \rangle$. Hence $\alpha(\theta + \alpha) \in \langle 2 \rangle$ so that

$$-(8M - 3 + 2R) + (8N - 3B - 3 \cdot 2^m + 2Q)\theta$$

$$+ (8P + 3B + 3 \cdot 2^m + y)\alpha \in \langle 2 \rangle.$$

As B and y are both odd, we deduce that $1 + \theta \in \langle 2 \rangle$ so that $(1 + \theta)/2 \in O_K$, contradicting that $(1 + \theta)/2$ is not a 2-integral element of O_K. Similarly we can show that $\langle 2, \alpha \rangle \neq \langle 1 \rangle$ and $\langle 2, \theta + \alpha \rangle \neq \langle 1 \rangle$. Thus we can choose

$$P = \langle 2, \theta \rangle, \quad Q = \langle 2, \alpha \rangle, \quad R = \langle 2, \theta + \alpha \rangle,$$

as asserted.

Example. Let $d \equiv 1 \pmod 8$ be a squarefree integer with $d = 1$ allowed. In [6] infinite parametric families of cubic fields with index 2 whose splitting fields contain $\mathbb{Q}(\sqrt{d})$ were given in terms of a defining polynomial of the form $x^3 - ax + b$. If θ denotes a root of this polynomial then, since it is proved in [6, p. 334] that $a \equiv 1 \pmod 2$, $b \equiv 0 \pmod 2$, $s_2 = 2$ and $\Delta_2 \equiv 1 \pmod 8$, Theorem 3 gives for all of these fields the prime ideal decomposition of 2 as

$$\langle 2 \rangle = \langle 2, \theta \rangle \left\langle 2, \frac{2 + \theta + \theta^2}{2} \right\rangle \left\langle 2, \frac{2 + 3\theta + \theta^2}{2} \right\rangle.$$

References

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

[2] S. Alaca and K. S. Williams, Introductory Algebraic Number Theory, Cambridge University Press, 2004.

[3] H. Cohen, A Course in Computational Algebraic Number Theory, Springer-Verlag, 2000.

[4] H. T. Engstrom, On the common index divisors of an algebraic field, Trans. Amer. Math. Soc. 32 (1930), 223-237.

[5] 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.

[6] B. K. Spearman and K. S. Williams, Cubic fields with index 2, Monatsh. Math. 134 (2002), 331-336.

Saban Alaca and Kenneth S. Williams
School of Mathematics and Statistics, Carleton University
Ottawa, Ontario, Canada K1S 5B6
e-mail: salaca@math.carleton.ca
williams@math.carleton.ca

Blair K. Spearman
Department of Mathematics and Statistics
Okanagan University College, Kelowna
B. C., Canada V1V 1V7
e-mail: bspearman@ouc.bc.ca