EXPLICIT DECOMPOSITION OF A RATIONAL PRIME IN A CUBIC FIELD

ŞABAN ALACA, BLAIR K. SPEARMAN, AND KENNETH S. WILLIAMS

Received 19 June 2005; Revised 19 February 2006; Accepted 12 March 2006

We give the explicit decomposition of the principal ideal $\langle p\rangle$ (p prime) in a cubic field.

1. Introduction

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

$$D(\theta) = \big(\mathrm{ind}(\theta)\big)^2 d(K). \tag{1.1}$$

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 principal ideal $\langle p\rangle$ of O_K into prime ideals in terms of the irreducible factors of $\mathrm{irr}_{\mathbb{Q}}(\theta)$ modulo p; see, for example, [3, Theorem 10.5.1, page 257].

Theorem 1.1. *Let $K = \mathbb{Q}(\theta)$ be an algebraic number field with $\theta \in O_K$. Let p be a rational prime. Let*

$$f(x) = \mathrm{irr}_{\mathbb{Q}}(\theta) \in \mathbb{Z}[x]. \tag{1.2}$$

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

$$\bar{f}(x) = g_1(x)^{e_1} \cdots g_r(x)^{e_r}, \tag{1.3}$$

where $g_1(x),\dots,g_r(x)$ are distinct irreducible polynomials in $\mathbb{Z}_p[x]$, and $e_1,\dots,e_r$ are positive

Hindawi Publishing Corporation
International Journal of Mathematics and Mathematical Sciences
Volume 2006, Article ID 17641, Pages 1–11
DOI 10.1155/IJMMS/2006/17641

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*

$$P_i = \langle p, f_i(\theta)\rangle, \quad i = 1,2,\ldots,r. \tag{1.4}$$

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

$$\begin{aligned} \langle p\rangle &= P_1^{e_1}\cdots P_r^{e_r}, \\ N(P_i) &= p^{\deg f_i}, \quad i = 1,2,\ldots,r. \end{aligned} \tag{1.5}$$

On the other hand if p is a prime dividing $\operatorname{ind}(\theta)$, no such general theorem is known which gives the prime ideals explicitly, and all that is available in general is the Buchmann-Lenstra algorithm [4, page 315] for decomposing a prime in a number field. If p is not a common index divisor of K, then there exist elements $\phi \in O_K$ for which $K = \mathbb{Q}(\phi)$, and $p \nmid \operatorname{ind}(\phi)$, and we can apply Dedekind's theorem to obtain the prime ideal factorization of $\langle p\rangle$ from the minimal polynomial $\operatorname{irr}_{\mathbb{Q}}(\phi)$. However given θ it is not easy to determine such an element ϕ in general. Moreover when p is a common index divisor of K, no such element ϕ exists and Dedekind's theorem cannot be applied.

In this paper we treat the case when K is a cubic field and p is a prime dividing $\operatorname{ind}(\theta)$. When p is a common index divisor of K (the only possibility is $p = 2$), we quote the results in [2]. When p is not a common index divisor, we construct an element $\phi \in O_K$ such that $K = \mathbb{Q}(\phi)$ and $p \nmid \operatorname{ind}(\phi)$ and then apply Dedekind's theorem to obtain the prime ideal factorization of $\langle p\rangle$. Our construction of ϕ was guided by the p-integral bases of K given by Alaca [1]. We give explicitly the prime ideals in the factorization of $\langle p\rangle$ into prime ideals in O_K. The form of the prime ideal factorization has been given by Llorente and Nart [6, Theorem 1, page 580] and we make use of their results. A method for factoring all primes in a cubic field is given in [5, pages 119–121]. 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

$$f(x) = x^3 - ax + b, \quad a,b \in \mathbb{Z}, \tag{1.6}$$

so that $\operatorname{irr}_{\mathbb{Q}}(\theta) = f(x)$. 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 have

$$D(\theta) = 4a^3 - 27b^2. \tag{1.7}$$

Let $\nu_p(k)$ denote the largest nonnegative integer m such that p^m divides the nonzero integer k. From (1.1) we deduce that

$$\nu_p(\operatorname{ind}(\theta)) = \frac{\nu_p(D(\theta)) - \nu_p(d(K))}{2}. \tag{1.8}$$

We set

$$D_p(\theta) = \frac{D(\theta)}{p^{\nu_p(D(\theta))}}. \tag{1.9}$$

Table 1.1. $p = 2$.

Case	Conditions	$\nu_2(d(K))$	$\nu_2(\text{ind}(\theta))$	ϕ	Factors of $\langle 2\rangle$	Prime ideals	Norms
A1	$a \equiv 0(4)$, $b \equiv 4(8)$ $\nu_2(D(\theta)) = 4$	2	1	$\phi = \frac{\theta^2}{2}$	P^3	$P = \langle 2, \phi\rangle$	$N(P) = 2$
A2	$a \equiv 2(4)$, $b \equiv 0(8)$ $\nu_2(D(\theta)) = 5$	3	1	$\phi = 1 + \theta + \frac{\theta^2}{2}$	PQ^2	$P = \langle 2, 1+\phi\rangle$ $Q = \langle 2, \phi\rangle$	$N(P) = 2$ $N(Q) = 2$
A3	$a \equiv 2(4)$, $b \equiv 4(8)$ $\nu_2(D(\theta)) = 4$	2	1	$\phi = \frac{\theta^2}{2}$	PQ^2	$P = \langle 2, \phi\rangle$ $Q = \langle 2, 1+\phi\rangle$	$N(P) = 2$ $N(Q) = 2$
A4	$a \equiv 1(4)$, $b \equiv 0(4)$ $D_2(\theta) \equiv 1(8)$ $\nu_2(D(\theta)) = 2$	0	1	$\phi = \frac{\theta+\theta^2}{2}$	PQR	$P = \langle 2, \theta\rangle$ $Q = \langle 2, 1+\phi\rangle$ $R = \langle 2, 1+\theta+\phi\rangle$	$N(P) = 2$ $N(Q) = 2$ $N(R) = 2$
A5	$a \equiv 1(4)$, $b \equiv 0(4)$ $D_2(\theta) \equiv 5(8)$ $\nu_2(D(\theta)) = 2$	0	1	$\phi = \frac{\theta+\theta^2}{2}$	PQ	$P = \langle 2, \phi\rangle$ $Q = \langle 2, 1+\phi+\phi^2\rangle$	$N(P) = 2$ $N(Q) = 4$
A6	$a \equiv 3(4)$, $b \equiv 2(4)$ $\nu_2(D(\theta)) \equiv 1(2)$ $\nu_2(D(\theta)) \geq 5$	3	$\frac{\nu_2(D(\theta))-3}{2}$	$\phi = 1+\lambda+\frac{\lambda^2}{2}$ $\lambda = \frac{\alpha}{2^{m+1}}$ $m = \frac{\nu_2(D(\theta))-3}{2}$	PQ^2	$P = \langle 2, 1+\phi\rangle$ $Q = \langle 2, \phi\rangle$	$N(P) = 2$ $N(Q) = 2$
A7	$a \equiv 3(4)$, $b \equiv 2(4)$ $\nu_2(D(\theta)) \equiv 0(2)$ $\nu_2(D(\theta)) \geq 4$ $D_2(\theta) \equiv 3(4)$	2	$\frac{\nu_2(D(\theta))-2}{2}$	$\phi = \frac{\alpha}{2^{m+1}}$ $m = \frac{\nu_2(D(\theta))-2}{2}$	PQ^2	$P = \langle 2, \phi\rangle$ $Q = \langle 2, 1+\phi\rangle$	$N(P) = 2$ $N(Q) = 2$
A8	$a \equiv 3(4)$, $b \equiv 2(4)$ $\nu_2(D(\theta)) \equiv 0(2)$ $\nu_2(D(\theta)) \geq 4$ $D_2(\theta) \equiv 1(8)$	0	$\frac{\nu_2(D(\theta))}{2}$	$\phi = \frac{\alpha}{2^m}$ $m = \frac{\nu_2(D(\theta))}{2}$	PQR	$P = \langle 2, \phi\rangle$ $Q = \left\langle 2, \frac{2+\phi+\phi^2}{2}\right\rangle$ $R = \left\langle 2, \frac{2+3\phi+\phi^2}{2}\right\rangle$	$N(P) = 2$ $N(Q) = 2$ $N(R) = 2$
A9	$a \equiv 3(4)$, $b \equiv 2(4)$ $\nu_2(D(\theta)) \equiv 0(2)$ $\nu_2(D(\theta)) \geq 4$ $D_2(\theta) \equiv 5(8)$	0	$\frac{\nu_2(D(\theta))}{2}$	$\phi = \frac{\lambda+\lambda^2}{2}$ $\lambda = \frac{\alpha}{2^{m+1}}$ $m = \frac{\nu_2(D(\theta))-2}{2}$	PQ	$P = \langle 2, \phi\rangle$ $Q = \langle 2, 1+\phi+\phi^2\rangle$	$N(P) = 2$ $N(Q) = 4$

The determination of $\nu_p(d(K))$ was carried out by Llorente and Nart [6, Theorem 2, page 583] in 1983; see also Alaca [1]. The values of $\nu_p(D(\theta))$ and $\nu_p(d(K))$ are listed in tabular form in Alaca [1] depending on congruence conditions on a and b. From [1] we deduce that $p \mid \text{ind}(\theta)$ in precisely those cases listed in Tables 1.1, 1.2, 1.3, and no others. We abbreviate $r \equiv s \pmod{m}$ by $r \equiv s(m)$. In the sixth column of each table we give the form of the prime ideal factorization from the work of Llorente and Nart [6, Theorem 1, page 580]. However, Llorente and Nart did not give the prime ideals explicitly. We give explicit formulae for these prime ideals in the seventh column of each of Tables 1.1, 1.2, and 1.3. It is convenient to set

$$\alpha = -4a^2 + 9b\theta + 6a\theta^2 \in O_K. \tag{1.10}$$

Table 1.2. $p = 3$.

Case	Conditions	$\nu_3(d(K))$	$\nu_3(\text{ind}(\theta))$	ϕ	Factors of $\langle 3\rangle$	Prime ideals	Norms
B1	$2 = \nu_3(b)$ $= \nu_3(a)$ $\nu_3(D(\theta)) = 6$	4	1	$\phi = \frac{\theta^2}{3}$	P^3	$P = \langle 3, \phi\rangle$	$N(P) = 3$
B2	$2 = \nu_3(b)$ $< \nu_3(a)$ $\nu_3(D(\theta)) = 7$	5	1	$\phi = \frac{\theta^2}{3}$	P^3	$P = \langle 3, \phi\rangle$	$N(P) = 3$
B3	$1 = \nu_3(a)$ $< \nu_3(b)$ $\nu_3(D(\theta)) = 3$	1	1	$\phi = \begin{cases} \theta + \frac{\theta^2}{3}, & (\dagger), \\ -\theta + \frac{\theta^2}{3}, & (\dagger\dagger). \end{cases}$ $(\dagger)$ if $3a - b \not\equiv 0(27)$ $(\dagger\dagger)$ if $3a + b \not\equiv 0(27)$ see Note	PQ^2	$P = \langle 3, \phi\rangle$ $Q = \left\langle 3, \phi - \frac{a}{3}\right\rangle$	$N(P) = 3$ $N(Q) = 3$
B4	$\nu_3(a) \geq 1$, $\nu_3(b) = 0$ $a \not\equiv 3(9)$, $b^2 \equiv a + 1(9)$ $\nu_3(D(\theta)) = 3$	1	1	$\phi = \begin{cases} \frac{1 - b\theta + \theta^2}{3}, & (\ddagger), \\ \frac{1 + 2b\theta + \theta^2}{3}, & (\ddagger\ddagger). \end{cases}$ $(\ddagger)$ if $9 \parallel a + 1 - b^2$ $(\ddagger\ddagger)$ if $27 \mid a + 1 - b^2$	PQ^2	$P = \left\langle 3, \frac{-(2a+3)}{3} + \phi\right\rangle$ $Q = \langle 3, \phi\rangle$, $(\ddagger)$ $P = \left\langle 3, \frac{a}{3} + \phi\right\rangle$ $Q = \langle 3, 1 + \phi\rangle$, $(\ddagger\ddagger)$	$N(P) = 3$ $N(Q) = 3$
B5	$a \equiv 3(9)$, $\nu_3(b) = 0$ $b^2 \equiv 4(9)$, $b^2 \not\equiv a + 1(27)$ $\nu_3(D(\theta)) = 5$	3	1	$\phi = \frac{1 - b\theta + \theta^2}{3}$	P^3	$P = \langle 3, \phi\rangle$	$N(P) = 3$
B6	$a \equiv 3(9)$, $\nu_3(b) = 0$ $b^2 \equiv a + 1(27)$ $\nu_3(D(\theta)) \equiv 1(2)$ $\nu_3(D(\theta)) \geq 7$	1	$\frac{\nu_3(D(\theta)) - 1}{2}$	$\phi = \begin{cases} -\lambda + \frac{\lambda^2}{3}, & (*) \\ \lambda + \frac{\lambda^2}{3}, & (**) \end{cases}$ $\lambda = \frac{\alpha}{3^{m+2}}$ $m = \frac{\nu_3(D(\theta)) - 3}{2}$ $(*)$ if $a \not\equiv -3^{m-1}D_3(\theta)(9)$ $(**)$ if $a \not\equiv 3^{m-1}D_3(\theta)(9)$ see Note	PQ^2	$P = \langle 3, \phi\rangle$ $Q = \left\langle 3, \phi - \frac{aD_3(\theta)}{3}\right\rangle$	$N(P) = 3$ $N(Q) = 3$
B7	$a \equiv 3(9)$, $\nu_3(b) = 0$ $b^2 \equiv a + 1(27)$ $\nu_3(D(\theta)) \equiv 0(2)$ $\nu_3(D(\theta)) \geq 6$ $D_3(\theta) \equiv 2(3)$	0	$\frac{\nu_3(D(\theta))}{2}$	$\phi = \frac{\alpha}{3^{m+2}}$ $m = \frac{\nu_3(D(\theta)) - 2}{2}$	PQ	$P = \langle 3, 2 + \phi\rangle$ $Q = \langle 3, 2 + \phi + \phi^2\rangle$ if $m = 2$, $P = \langle 3, \phi\rangle$ $Q = \langle 3, 1 + \phi^2\rangle$ if $m \geq 3$	$N(P) = 3$ $N(Q) = 9$
B8	$a \equiv 3(9)$, $\nu_3(b) = 0$ $b^2 \equiv a + 1(27)$ $\nu_3(D(\theta)) \equiv 0(2)$ $\nu_3(D(\theta)) = 6$ $D_3(\theta) \equiv 1(3)$	0	3		P	$P = \langle 3\rangle$	$N(P) = 27$

Table 1.2. Continued.

Case	Conditions	$\nu_3(d(K))$	$\nu_3(\text{ind}(\theta))$	ϕ	Factors of $\langle 3\rangle$	Prime ideals	Norms
B9	$a \equiv 3(9)$, $\nu_3(b)=0$, $b^2 \equiv a+1(27)$, $\nu_3(D(\theta)) \equiv 0(2)$, $\nu_3(D(\theta)) \geq 8$, $D_3(\theta) \equiv 1(3)$	0	$\dfrac{\nu_3(D(\theta))}{2}$	$\phi = \dfrac{\alpha}{3^{m+2}}$, $m = \dfrac{\nu_3(D(\theta))-2}{2}$	PQR	$P=\langle 3,\phi\rangle$, $Q=\langle 3,-1+\phi\rangle$, $R=\langle 3,1+\phi\rangle$	$N(P)=3$, $N(Q)=3$, $N(R)=3$

Note: In case B3 (resp., B6) if $b \equiv 0(27)$ (resp., $m \geq 3$), both choices for ϕ are valid.

Table 1.3. $p > 3$.

Case	Conditions	$\nu_p(d(K))$	$\nu_p(\text{ind}(\theta))$	ϕ	Factors of $\langle p\rangle$	Prime ideals	Norms
C1	$2=\nu_p(b) \leq \nu_p(a)$, $\nu_p(D(\theta))=4$	2	1	$\phi = \dfrac{\theta^2}{p}$	P^3	$P=\langle p,\phi\rangle$	$N(P)=p$
C2	$1=\nu_p(a) < \nu_p(b)$, $\nu_p(D(\theta))=3$	1	1	$\phi = \begin{cases} \dfrac{\theta^2}{p}, & \text{if } p^2 \parallel b, \\ \theta+\dfrac{\theta^2}{p}, & \text{if } p^3 \mid b. \end{cases}$	PQ^2	$P=\langle p,\phi\rangle$, $Q=\left\langle p,-\dfrac{a}{p}+\phi\right\rangle$	$N(P)=p$, $N(Q)=p$
C3	$\nu_p(a)=\nu_p(b)=0$, $\nu_p(D(\theta)) \equiv 1(2)$, $\nu_p(D(\theta)) \geq 3$	1	$\dfrac{\nu_p(D(\theta))-1}{2}$	$\phi = \lambda+\dfrac{\lambda^2}{p}$, $\lambda = \dfrac{\alpha}{p^m}$, $m = \dfrac{\nu_p(D(\theta))-1}{2}$	PQ^2	$P=\langle p,\phi\rangle$, $Q=\langle p,-3aD_p(\theta)+\phi\rangle$	$N(P)=p$, $N(Q)=p$
C4	$\nu_p(a)=\nu_p(b)=0$, $\nu_p(D(\theta)) \equiv 0(2)$, $\nu_p(D(\theta)) \geq 2$, $\left(\dfrac{D_p(\theta)}{p}\right)=1$	0	$\dfrac{\nu_p(D(\theta))}{2}$	$\phi = \dfrac{\alpha}{p^m}$, $m = \dfrac{\nu_p(D(\theta))}{2}$, $t^2 \equiv 3aD_p(\theta)(p)$	PQR	$P=\langle p,\phi\rangle$, $Q=\langle p,-t+\phi\rangle$, $R=\langle p,t+\phi\rangle$	$N(P)=p$, $N(Q)=p$, $N(R)=p$
C5	$\nu_p(a)=\nu_p(b)=0$, $\nu_p(D(\theta)) \equiv 0(2)$, $\nu_p(D(\theta)) \geq 2$, $\left(\dfrac{D_p(\theta)}{p}\right)=-1$	0	$\dfrac{\nu_p(D(\theta))}{2}$	$\phi = \dfrac{\alpha}{p^m}$, $m = \dfrac{\nu_p(D(\theta))}{2}$	PQ	$P=\langle p,\phi\rangle$, $Q=\langle p,-3aD_p(\theta)+\phi^2\rangle$	$N(P)=p$, $N(Q)=p^2$

It is easy to show that the minimal polynomial of α over $\mathbb{Q}$ is

$$q(x) = x^3 - 3aD(\theta)x + D(\theta)^2 \tag{1.11}$$

and that

$$\text{disc}\,(q(x)) = 3^6 b^2 D(\theta)^3. \tag{1.12}$$

2. Case A1

In this case we can define integers A and B by $a = 4A$ and $b = 8B+4$. Set $\phi = \theta^2/2$. The minimal polynomial of ϕ over $\mathbb{Q}$ is

$$p(x) = x^3 - 4Ax^2 + 4A^2x - (8B^2+8B+2) \tag{2.1}$$

so that $\phi \in O_K$. Further

$$\operatorname{disc}(p(x)) = -4(2B+1)^2(108B^2+108B-16A^3+27). \tag{2.2}$$

We have $p(x) \equiv x^3 \pmod 2$. As $2^2 \parallel \operatorname{disc}(p(x))$, $2^2 \parallel d(K)$, we have $2 \nmid \operatorname{ind}(\phi)$, so that by Theorem 1.1,

$$\langle 2\rangle = \langle 2,\phi\rangle^3. \tag{2.3}$$

3. Cases A2, A3, A5, A7, B1, B2, B5, B7, B9, C1, C2

These cases can be treated similarly to case A1.

4. Cases A4, A8

In these cases 2 is a common index divisor and we can appeal to [6, Theorem 4, page 585] for the results.

5. Case A6

We let $\lambda = \alpha/2^{m+1}$, where $\nu_2(D(\theta)) = 2m+3 \geq 5$, and $\phi = 1+\lambda+\lambda^2/2$. By (1.11), the minimal polynomial of α over $\mathbb{Q}$ is $x^3 - 3aD(\theta)x + D(\theta)^2$ so that the minimal polynomial of λ over $\mathbb{Q}$ is

$$x^3 - \frac{3aD(\theta)}{2^{2m+2}}x + \frac{D(\theta)^2}{2^{3m+3}} = x^3 - 6aD_2(\theta)x + 2^{m+3}D_2(\theta)^2. \tag{5.1}$$

Hence $\lambda \in O_K$. We are now in case A2 with

$$\begin{aligned} a' &= 6aD_2(\theta) \equiv 2 \pmod 4, \\ b' &= 2^{m+3}D_2(\theta)^2 \equiv 0 \pmod 8, \\ D(\theta)' &= \frac{3^6b^2D(\theta)^3}{2^{6m+6}}, \\ \nu_2(D(\theta))' &= 2+3(2m+3)-(6m+6) = 5. \end{aligned} \tag{5.2}$$

Thus by case A2 we obtain

$$\langle 2\rangle = \langle 2,\phi+1\rangle\langle 2,\phi\rangle^2. \tag{5.3}$$

6. Case A9

In this case we set $\nu_2(D(\theta)) = 2m+2$ (so that $m \geq 1$), $\lambda = \alpha/2^{m+1}$, and $\phi = (\lambda+\lambda^2)/2$. Then proceeding as in case A6 we can reduce this case to case A5.

7. Case B3

In this case we have

$$1 = \nu_3(a) < \nu_3(b), \qquad \nu_3(D(\theta)) = 3. \tag{7.1}$$

Clearly $9 \mid 3a-b$ and $9 \mid 3a+b$. However 27 cannot divide both of $3a-b$ and $3a+b$ as their sum $6a$ is not divisible by 27. Hence we can define

$$\phi = \begin{cases} \dfrac{\theta^2}{3}+\theta & \text{if } 3a-b \not\equiv 0 \pmod{27}, \\ \dfrac{\theta^2}{3}-\theta & \text{if } 3a+b \not\equiv 0 \pmod{27}. \end{cases} \tag{7.2}$$

We note that if $27 \mid b$ we can choose either value of $\theta^2/3 \pm \theta$ for ϕ. Set

$$\varepsilon = \begin{cases} +1 & \text{if } 3a-b \not\equiv 0 \pmod{27}, \\ -1 & \text{if } 3a+b \not\equiv 0 \pmod{27}, \end{cases} \tag{7.3}$$

subject to the remark above, so that

$$\phi = \frac{\theta^2}{3}+\varepsilon\theta. \tag{7.4}$$

The minimal polynomial of ϕ is

$$p(x) = x^3 - \frac{2a}{3}x^2 + \left(-a+\frac{a^2}{9}+\varepsilon b\right)x + \varepsilon b - \frac{b^2}{27} - \frac{\varepsilon ab}{9} \tag{7.5}$$

so that $\phi \in O_K$. We have

$$p(x) \equiv x^3 - \frac{2a}{3}x^2 + \frac{a^2}{9}x \equiv x\left(x-\frac{a}{3}\right)^2 \pmod{3}. \tag{7.6}$$

Further

$$\operatorname{disc}(p(x)) = \frac{D(\theta)(3a-\varepsilon b-27)^2}{3^6}. \tag{7.7}$$

As $3 \parallel \operatorname{disc}(p(x))$, $3 \parallel d(K)$, we have $3 \nmid \operatorname{ind}(\phi)$, so that by Theorem 1.1, we obtain

$$\langle 3\rangle = \langle 3,\phi\rangle\left\langle 3,\phi-\frac{a}{3}\right\rangle^2. \tag{7.8}$$

8. Case B4

In this case we have $9 \mid a+1-b^2$. We set

$$\phi = \begin{cases} \dfrac{(\theta^2 - b\theta + 1)}{3} & \text{if } 9 \parallel a+1-b^2, \\ \dfrac{(\theta^2 + 2b\theta + 1)}{3} & \text{if } 27 \mid a+1-b^2. \end{cases} \tag{8.1}$$

First we consider the case $9 \parallel a+1-b^2$. The minimal polynomial of ϕ is

$$p(x) = x^3 - \frac{(2a+3)}{3}x^2 + \frac{(a+3)(a+1-b^2)}{9}x - \frac{(a+1-b^2)^2}{27} \tag{8.2}$$

so that $p(x) \in \mathbb{Z}[x]$ and $\phi \in O_K$. We have

$$p(x) \equiv x^2\left(x - \frac{2a+3}{3}\right) \pmod 3. \tag{8.3}$$

Further

$$\operatorname{disc}(p(x)) = b^2 D(\theta)\frac{(a+1-b^2)^2}{3^6} \tag{8.4}$$

so that $3 \parallel \operatorname{disc}(p(x))$, $3 \parallel d(K)$, thus $3 \nmid \operatorname{ind}(\phi)$, and by Theorem 1.1 we have

$$\langle 3\rangle = \langle 3,\phi\rangle^2 \left\langle 3, \phi - \frac{2a+3}{3}\right\rangle. \tag{8.5}$$

Now we turn to the case $27 \mid a+1-b^2$. The minimal polynomial of ϕ is

$$p(x) = x^3 + p_2x^2 + p_1x + p_0, \tag{8.6}$$

where

$$\begin{aligned} p_2 &= -\frac{(2a+3)}{3}, \\ p_1 &= \frac{(a^2+4a-4ab^2+6b^2+3)}{9}, \\ p_0 &= \frac{(-a^2-2a+2ab^2+8b^4-7b^2-1)}{27}. \end{aligned} \tag{8.7}$$

Clearly

$$\begin{aligned} &p_2 \in \mathbb{Z}, \\ &p_1 = (12a-18)\left(\frac{a+1-b^2}{27}\right) - 3\left(\frac{a}{3}\right)^2 + 2\left(\frac{a}{3}\right) + 1 \in \mathbb{Z}, \\ &p_0 = \frac{a(a+1)}{3} + 9\left(\frac{a+1-b^2}{27}\right)\left(24\left(\frac{a+1-b^2}{27}\right) - (2a+1)\right) \in \mathbb{Z}, \end{aligned} \tag{8.8}$$

so that $\phi \in O_K$. Further

$$\begin{aligned} p_2 &\equiv \frac{a}{3} + 2 \pmod 3, \\ p_1 &\equiv \frac{2a}{3} + 1 \pmod 3, \\ p_0 &\equiv \frac{a}{3} \pmod 3. \end{aligned} \tag{8.9}$$

Hence

$$p(x) \equiv \left(x + \frac{a}{3}\right)(x+1)^2 \pmod 3. \tag{8.10}$$

Further

$$\operatorname{disc}\left(p(x)\right) = b^2 D(\theta) \frac{\left(8b^2 - 2a + 1\right)^2}{3^6}. \tag{8.11}$$

As $a \equiv 0, 6 \pmod 9$, $a + 1 - b^2 \equiv 0 \pmod{27}$, and

$$8b^2 - 2a + 1 = 6(a-3) - 8\left(a + 1 - b^2\right) + 27; \tag{8.12}$$

we see that

$$3^2 \parallel 8b^2 - 2a + 1 \tag{8.13}$$

so that $3 \parallel \operatorname{disc}(p(x))$, $3 \parallel d(K)$, and thus $3 \nmid \operatorname{ind}(\phi)$. Hence by Theorem 1.1 we have

$$\langle 3 \rangle = \left\langle 3, \phi + \frac{a}{3} \right\rangle \langle 3, \phi + 1 \rangle^2. \tag{8.14}$$

9. Case B6

In this case we set $v_3(D(\theta)) = 2m + 3$ so that $m \geq 2$. Let

$$\begin{aligned} \lambda &= \frac{\alpha}{3^{m+2}}, \\ \phi &= \begin{cases} \dfrac{\lambda^2}{3} + \lambda & \text{if } a \not\equiv 3^{m-1} D_3(\theta) \pmod 9, \\ \dfrac{\lambda^2}{3} - \lambda & \text{if } a \not\equiv -3^{m-1} D_3(\theta) \pmod 9. \end{cases} \end{aligned} \tag{9.1}$$

The minimal polynomial of λ is

$$\begin{aligned} p(x) &= x^3 - aD_3(\theta)x + 3^m D_3(\theta)^2, \\ \operatorname{disc}\left(p(x)\right) &= 3^3 b^2 D_3(\theta)^3. \end{aligned} \tag{9.2}$$

We are now in case B3 with

$$\begin{aligned} a' &= aD_3(\theta), \qquad \nu_3(a') = 1, \\ b' &= 3^m D_3(\theta)^2 \equiv 0 \pmod{9}, \\ 4a'^3 - 27b'^2 &= 3^3 b^2 D_3(\theta)^3, \qquad \nu_3\left(4a'^3 - 27b'^2\right) = 3. \end{aligned} \tag{9.3}$$

Hence

$$\langle 3\rangle = \langle 3,\phi\rangle \left\langle 3,\phi - \frac{aD_3(\theta)}{3}\right\rangle^2. \tag{9.4}$$

10. Case B8

Here $\langle 3\rangle$ is a prime ideal.

11. Case C3

Similarly to case B6 this case can be reduced to case C2.

12. Cases C4, C5

Here

$$\begin{gathered} p \nmid a,\ p \nmid b, \quad \nu_p(D(\theta)) \equiv 0 \pmod{2}, \quad \nu_p(D(\theta)) \geq 2, \\ \left(\frac{D_p(\theta)}{p}\right) = \begin{cases} +1, & \text{case C4}, \\ -1, & \text{case C5}. \end{cases} \end{gathered} \tag{12.1}$$

Set $\nu_p(D(\theta)) = 2m$ so that $m \geq 1$. Let $\phi = \alpha/p^m$. The minimal polynomial of ϕ is

$$\begin{aligned} p(x) &= x^3 - 3aD_p(\theta)x + p^m D_p(\theta)^2, \\ \operatorname{disc}\left(p(x)\right) &= \frac{3^6 b^2 D(\theta)^3}{p^{6m}}. \end{aligned} \tag{12.2}$$

Clearly $p \nmid \operatorname{disc}(p(x))$ so that $p \nmid \operatorname{ind}(\phi)$. Now

$$p(x) \equiv x\left(x^2 - 3aD_p(\theta)\right) \pmod{p}. \tag{12.3}$$

As

$$4a^3 - 27b^2 \equiv 0 \pmod{p}, \quad p \nmid a,\ p \nmid b,\ p > 3, \tag{12.4}$$

we have

$$\left(\frac{3a}{p}\right) = 1. \tag{12.5}$$

Thus

$$x^2 - 3aD_p(\theta) \equiv \begin{cases} (x-t)(x+t) \pmod{p}, & \text{case C4,} \\ \text{irreducible} \pmod{p}, & \text{case C5,} \end{cases} \tag{12.6}$$

where $t^2 \equiv 3aD_p(\theta) \pmod{p}$. Hence

$$\langle p \rangle = \begin{cases} \langle p,\phi\rangle\langle p,\phi - t\rangle\langle p,\phi + t\rangle, & \text{case C4,} \\ \langle p,\phi\rangle\langle p,\phi^2 - 3aD_p(\theta)\rangle, & \text{case C5,} \end{cases} \tag{12.7}$$

where $N(\langle p,\phi^2 - 3aD_p(\theta)\rangle) = p^2$.

Acknowledgment

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

References

[1] Ş. Alaca, *p-integral bases of a cubic field*, Proceedings of the American Mathematical Society **126** (1998), no. 7, 1949–1953.
[2] Ş. Alaca, B. K. Spearman, and K. S. Williams, *The factorization of 2 in cubic fields with index 2*, Far East Journal of Mathematical Sciences (FJMS) **14** (2004), no. 3, 273–282.
[3] Ş. Alaca and K. S. Williams, *Introductory Algebraic Number Theory*, Cambridge University Press, Cambridge, 2004.
[4] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer, New York, 2000.
[5] B. N. Delone and D. K. Faddeev, *The Theory of Irrationalities of the Third Degree*, Translations of Mathematical Monographs, vol. 10, American Mathematical Society, Rhode Island, 1964.
[6] P. Llorente and E. Nart, *Effective determination of the decomposition of the rational primes in a cubic field*, Proceedings of the American Mathematical Society **87** (1983), no. 4, 579–585.

Şaban Alaca: Centre for Research in Algebra and Number Theory, School of Mathematics and Statistics, Carleton University Ottawa, ON, Canada K1S 5B6
E-mail address: salaca@math.carleton.ca

Blair K. Spearman: Department of Mathematics and Statistics, University of British Columbia Okanagan, Kelowna, BC, Canada V1V 1V7
E-mail address: blair.spearman@ubc.ca

Kenneth S. Williams: Centre for Research in Algebra and Number Theory, School of Mathematics and Statistics, Carleton University Ottawa, ON, Canada K1S 5B6
E-mail address: kwilliam@connect.carleton.ca