Int. J. Contemp. Math. Sciences, Vol. 3, 2008, no. 29, 1427 - 1432

A Normal Relative Integral Basis for the Normal Closure of a Pure Cubic Field over $\mathbb{Q}(\sqrt{-3})$

Blair K. Spearman

Department of Mathematics and Statistics
University of British Columbia Okanagan
Kelowna, BC, Canada V1V 1V7
blair.spearman@ubc.ca

Kenneth S. Williams

School of Mathematics and Statistics
Carleton University, Ottawa, ON, Canada K1S 5B6
kwilliam@connect.carleton.ca

Abstract

An explicit normal relative integral basis is given for the normal closure of a pure cubic field over $\mathbb{Q}(\sqrt{-3})$. This basis is shown to be unique up to permutation and units.

1 Introduction

In [1] Carter proved that $k = \mathbb{Q}(\sqrt{-3})$ is a Hilbert-Speiser field of type C_3. This means that if E is a tamely ramified normal extension of k with $\mathrm{Gal}(E/k) \cong C_3$ then E has a normal relative integral basis over k.

Let K be a pure cubic field. Let $L = K(\sqrt{-3})$ so that L is the normal closure of K. By Carter's theorem we know that if L/k is tamely ramified then L/k possesses a normal relative integral basis (NRIB). We prove that in this case the converse holds, that is, if L/k possesses a NRIB then L/k is tamely ramified. When L/k is tamely ramified we use the relative integral basis (RIB) given in [2] to give explicitly a NRIB for L/k. Further we show that this NRIB is unique up to permutation and units of k. We prove

Theorem 1.1. *Let K be a pure cubic field so that $K = \mathbb{Q}\left(\sqrt[3]{ab^2}\right)$ for some coprime squarefree integers a and b. Let L be the normal closure of K. Let*

$k=\mathbb{Q}(\sqrt{-3})$.

(i) *The extension L/k is tamely ramified if and only if*

$$3 \nmid a, \quad 3 \nmid b, \quad 9 \mid a^2-b^2. \tag{1.1}$$

(ii) *A NRIB exists for L/k if and only if* (1.1) *holds.*

(iii) *If* (1.1) *holds then*

$$\left\{\frac{1}{3}\left(1+\left(\frac{-3}{a}\right)(ab^2)^{1/3}+\left(\frac{-3}{b}\right)(a^2b)^{1/3}\right),\right.$$
$$\frac{1}{3}\left(1+\left(\frac{-3}{a}\right)\omega\,(ab^2)^{1/3}+\left(\frac{-3}{b}\right)\omega^2\,(a^2b)^{1/3}\right),$$
$$\left.\frac{1}{3}\left(1+\left(\frac{-3}{a}\right)\omega^2\,(ab^2)^{1/3}+\left(\frac{-3}{b}\right)\omega\,(a^2b)^{1/3}\right)\right\}$$

is a NRIB for L/k, where $\omega=\frac{1}{2}\left(-1+\sqrt{-3}\right)$, and for $m\in\mathbb{Z}$ the Legendre-Jacobi-Kronecker symbol $\left(\frac{-3}{m}\right)$ is given by

$$\left(\frac{-3}{m}\right)=\begin{cases} +1, & \text{if } m\equiv 1 \pmod 3,\\ -1, & \text{if } m\equiv 2 \pmod 3,\\ 0, & \text{if } m\equiv 0 \pmod 3.\end{cases}$$

(iv) *The NRIB given in* (iii) *is unique up to permutation and units.*

2 Proof of Theorem 1.1

We begin with a simple lemma.

Lemma 2.1. *Let $Q\subseteq E\subseteq F$ be a tower of fields with F/E normal. Suppose that $\{\theta_1,\theta_2,\ldots,\theta_n\}$ is a normal relative integral basis for F/E. Then $\theta_1+\theta_2+\cdots+\theta_n$ is a unit in O_E, the ring of integers of E.*

Proof. Let $t=\theta_1+\theta_2+\cdots+\theta_n\,(\in O_F)$. As $\theta_1,\theta_2,\ldots,\theta_n$ are conjugates over E, we have $t\in O_E$. Then

$$1=\frac{1}{t}\theta_1+\frac{1}{t}\theta_2+\cdots+\frac{1}{t}\theta_n.$$

But $\{\theta_1, \theta_2, \ldots, \theta_n\}$ is a relative integral basis for F/E so $\dfrac{1}{t} \in O_E$. Hence t is a unit of O_E. $\square$

We are now ready to prove Theorem 1.1.

Proof of Theorem 1.1. (i) By [2, eq. (2.6), p. 1624] we have

$$d(L/k) = \begin{cases} a^2b^2, & \text{if } 3 \nmid a,\ 3 \nmid b,\ 9 \mid a^2 - b^2, \\ 9a^2b^2, & \text{otherwise.} \end{cases}$$

If $3 \nmid a$, $3 \nmid b$, $9 \mid a^2 - b^2$, $\sqrt{-3}$ is not ramified in L/k so that L/k is a tamely ramified extension. Otherwise, as $\sqrt{-3} = P^3$ for some prime ideal P, L/k is wildly ramified.

(ii), (iii) We begin with the case $3 \mid a$, $3 \nmid b$. In this case the integers of L are of the form [2, Table 3.1(i), p. 1624]

$$\alpha + \beta(ab^2)^{1/3} + \gamma\frac{(a^2b)^{1/3}}{\sqrt{-3}}, \tag{2.1}$$

where $\alpha, \beta, \gamma \in O_k$. Suppose that $\{\theta_1, \theta_2, \theta_3\}$ is a NRIB for L/k. Then we see from (2.1) that

$$\theta_1 + \theta_2 + \theta_3 = 3\alpha.$$

By Lemma 2.1, 3α is a unit of O_k. This is impossible. Hence L/k does not possess a NRIB.

The cases $3 \nmid a$, $3 \mid b$ and $3 \nmid a$, $3 \nmid b$, $9 \nmid a^2 - b^2$ follow in exactly the same way using [2, Table 3.1(ii)(iii), p. 1624]. Again L/k does not possess a NRIB in both cases. In the remaining case $3 \nmid a$, $3 \nmid b$, $9 \mid a^2 - b^2$, we claim that $\{r_1, r_2, r_3\}$ is a NRIB for L/k, where

$$\begin{aligned} r_1 &= \frac{1}{3}\left(1 + \left(\frac{-3}{a}\right)(ab^2)^{1/3} + \left(\frac{-3}{b}\right)(a^2b)^{1/3}\right), \\ r_2 &= \frac{1}{3}\left(1 + \left(\frac{-3}{a}\right)\omega(ab^2)^{1/3} + \left(\frac{-3}{b}\right)\omega^2(a^2b)^{1/3}\right), \\ r_3 &= \frac{1}{3}\left(1 + \left(\frac{-3}{a}\right)\omega^2(ab^2)^{1/3} + \left(\frac{-3}{b}\right)\omega(a^2b)^{1/3}\right). \end{aligned}$$

It is clear from [2, Table 3.1, p. 1624] that each r_i ($i \in \{1, 2, 3\}$) is an integer of L. Further a simple calculation shows that

$$(\det R)^2 = a^2b^2 = d(L/k),$$

by [2, eq. (2.6), p. 1624], where

$$R = \begin{pmatrix} r_1 & r_2 & r_3 \\ r_2 & r_3 & r_1 \\ r_3 & r_1 & r_2 \end{pmatrix}.$$

Hence $\{r_1, r_2, r_3\}$ is a NRIB for L/k.

(iv) Suppose that $\{s_1, s_2, s_3\}$ is another NRIB for L/k, where $3 \nmid a$, $3 \nmid b$, $9 \mid a^2 - b^2$. Then there exist $A, B, C \in O_k$ such that

$$\begin{array}{rcl} s_1 & = & Ar_1 + Br_2 + Cr_3, \\ s_2 & = & Cr_1 + Ar_2 + Br_3, \\ s_3 & = & Br_1 + Cr_2 + Ar_3. \end{array}$$

Let

$$S = \begin{pmatrix} s_1 & s_2 & s_3 \\ s_2 & s_3 & s_1 \\ s_3 & s_1 & s_2 \end{pmatrix}.$$

Then

$$(\det S)^2 = (A+B+C)^2(A^2+B^2+C^2-AB-BC-CA)^2(\det R)^2.$$

Hence $(A+B+C)^2(A^2+B^2+C^2-AB-BC-CA)^2$ is a unit of O_k. As $A+B+C \in O_k$ and $A^2+B^2+C^2-AB-BC-CA \in O_k$, each of $A+B+C$ and $A^2+B^2+C^2-AB-BC-CA$ is a unit of O_k. But the units of O_k are $\{\pm 1, \pm\omega, \pm\omega^2\}$ so that there exist $m, n \in \mathbb{Z}$ such that

$$A + B + C = \pm\omega^m \tag{2.2}$$

and

$$A^2+B^2+C^2-AB-BC-CA = \pm\omega^n.$$

Then

$$(A+B+C)^2 - 3(AB+BC+CA) = \pm\omega^n$$

so that

$$AB+BC+CA = \frac{1}{3}\left(\omega^{2m} \mp \omega^n\right).$$

As $AB+BC+CA \in O_k$ we must have

$$\frac{1}{3}\omega^{2m} \mp \frac{1}{3}\omega^n \in O_k.$$

But $\{1, \omega\}$ is an integral basis for k so $2m \equiv n \pmod 3$ and the minus sign holds. Hence

$$AB + BC + CA = 0. \tag{2.3}$$

Then

$$AB + (A+B)(\pm\omega^m - (A+B)) = 0$$

so

$$A^2 + (B \mp \omega^m)A + B(B \mp \omega^m) = 0. \tag{2.4}$$

Hence the quadratic polynomial $x^2 + (B \mp \omega^m)x + B(B \mp \omega^m) \in O_k[x]$ has a root A in O_k. Thus its discriminant must be a square in O_k, that is

$$(B \mp \omega^m)^2 - 4B(B \mp \omega^m) = H^2$$

for some $H \in O_k$, that is

$$\left(3B \mp \omega^m + \sqrt{-3}H\right)\left(3B \mp \omega^m - \sqrt{-3}H\right) = 4\omega^{2m}.$$

As O_k is a unique factorization domain and 2 is a prime in O_k, we have

$$\begin{aligned} \left(3B \mp \omega^m + \sqrt{-3}H\right) &= \pm 2\omega^f, \\ \left(3B \mp \omega^m - \sqrt{-3}H\right) &= \pm 2\omega^{2m-f}, \end{aligned}$$

for some $f \in \mathbb{Z}$. Then

$$3B \mp \omega^m = \pm\left(\omega^f + \omega^{2m-f}\right)$$

so

$$3B = \pm\omega^f\left(1 + \omega^{2m-2f} \pm \omega^{m-f}\right).$$

As $1 \pm \omega^r + \omega^{2r} \equiv 0 \pmod 3$ in O_k if and only if the plus sign holds, we see that the plus sign holds in $1 + \omega^{2m-2f} \pm \omega^{m-f}$. Thus

$$3B = \pm 3\omega^f \text{ or } 0,$$

that is B is a unit of O_k or 0. From (2.4) and then (2.3) and (2.2), we deduce that exactly one of A, B, C is a unit and the others are 0. This proves that s_1, s_2, s_3 is a unit multiple of a permutation of r_1, r_2, r_3. □

3 Acknowledgement

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

References

[1] J. E. Carter, "Normal integral bases in quadratic and cyclic cubic extensions of quadratic fields," *Archiv der Mathematik*, vol. 81, pp. 266–271, 2003.

[2] B. K. Spearman and K. S. Williams, "A relative integral basis over $\mathbb{Q}(\sqrt{-3})$ for the normal closure of a pure cubic field," *International Journal of Mathematics and Mathematical Sciences*, vol. 2003, pp. 1623–1626, 2003.

Received: April 10, 2008