On Voronoi's method for finding an integral basis of a cubic field

Şaban Alaca and Kenneth S. Williams [1]

ABSTRACT. We give a new proof of Voronoi's determination of an integral basis for a cubic field.

Let K be a cubic field. Without loss of generality we may take the cubic field K in the form $K = Q(\theta)$, where θ is a root of the irreducible polynomial

$$f(x) = x^3 - ax + b \ , \ a, b \in Z.$$

For each prime p and each nonzero integer m, $\nu_p(m)$ denotes the greatest exponent l such that $p^l \mid m$. We can also assume that for every prime p

$$\nu_p(a) < 2 \text{ or } \nu_p(b) < 3 \ ,$$

see [4, p. 579]. The discriminant of θ is $\triangle = 4a^3 - 27b^2$ and $\triangle = i(\theta)^2 d(K)$, where $i(\theta)$ denotes the index of θ and $d(K)$ denotes the discriminant of K. For each prime p, set $s_p = \nu_p(\triangle)$ and $\triangle_p = \triangle / p^{s_p}$. The value of $d(K)$ has been given by Llorente and Nart [4, Theorem 2] (also by Alaca [1]).

Theorem 1.

$$d(K) = sgn(\triangle) 2^\alpha 3^\beta \prod_{\substack{p>3 \\ s_p \ odd}} p \prod_{\substack{p>3 \\ 1 \leq \nu_p(b) \leq \nu_p(a)}} p^2,$$

where α and β are given by

$$\alpha = \begin{cases} 3, & if \ s_2 \equiv 1 \pmod 2 \ , \\ 2, & if \ 1 \leq \nu_2(b) \leq \nu_2(a), \ or \ s_2 \ even \ and \ \triangle_2 \equiv 3 \pmod 4 \ , \\ 0, & otherwise \ , \end{cases}$$

and

[1] Research supported by Natural Sciences and Engineering Research Council of Canada Grant A-7233.
Date: May 16, 2002 1991 *Mathematics Subject Clasification:* 11R16,11R29
Key words and phrases: cubic field, discriminant, integral basis.

Utilitas Mathematica **65**(2004), pp. 163-166

$$\beta = \begin{cases} 5, & \textit{if } 1 \le \nu_3(b) < \nu_3(a)\ , \\ 4, & \textit{if } \nu_3(a) = \nu_3(b) = 2,\ \textit{or} \\ & a \equiv 3 \pmod 9\ ,\ 3 \nmid b \textit{ and } b^2 \not\equiv 4 \pmod 9\ , \\ 3, & \textit{if } \nu_3(a) = \nu_3(b) = 1,\ \textit{or} \\ & 3 \mid a\ ,\ 3 \nmid b\ ,\ a \not\equiv 3 \pmod 9) \textit{ and } b^2 \not\equiv a+1 \pmod 9,\ \textit{or} \\ & a \equiv 3 \pmod 9\ ,\ b^2 \equiv 4 \pmod 9 \textit{ and } b^2 \not\equiv a+1 \pmod{27}\ , \\ 1, & \textit{if } 1 = \nu_3(a) < \nu_3(b),\ \textit{or} \\ & 3 \mid a\ ,\ a \not\equiv 3 \pmod 9 \textit{ and } b^2 \equiv a+1 \pmod 9,\ \textit{or} \\ & a \equiv 3 \pmod 9\ ,\ b^2 \equiv a+1 \pmod{27} \textit{ and } s_3 \textit{ odd}\ , \\ 0, & 3 \nmid a,\ \textit{or} \\ & a \equiv 3 \pmod 9\ ,\ b^2 \equiv a+1 \pmod{27} \textit{ and } s_3 \textit{ even}\ . \end{cases}$$

Voronoi [5] (see also [3, pp. 108–112]) has shown how an integral basis of K can be found in terms of a and b. We show how Voronoi's determination of an integral basis for K follows easily from Llorente and Nart's evaluation of $d(K)$ (also from the work of Alaca [1]), thereby giving a new proof of Voronoi's results (Theorems 2 and 3 below).

An integral basis for K comprises 1, a minimal integer of degree 1 in θ, and a minimal integer of degree 2 in θ. A minimal integer of degree 1 in θ is either of the form $u + \theta$ or $(u + \theta)/3$, where u is an integer. The latter happens precisely when

$$a \equiv 3 \pmod 9 \text{ and } b^2 \equiv a + 1 \pmod{27}. \tag{1}$$

It is therefore convenient to consider two cases. We first treat those a and b for which (1) does not hold. For all primes p, we define the integer r_p by

$$r_p = (s_p - \nu_p(d(K)))/2. \tag{2}$$

Lemma 1. *Suppose (1) does not hold. Then, for each prime p, the pair of congruences*

$$\begin{cases} t^3 - at + b \equiv 0 \pmod{p^{2k}}, \\ 3t^2 - a \equiv 0 \pmod{p^k}, \end{cases} \tag{3}$$

is solvable for $k = r_p$ but not for $k = r_p + 1$.

Proof: The proof is straightforward and we give the details only for the case $p = 3$ and $\nu_3(a) = \nu_3(b) = 2$. In this case $s_3 = 6$ and $\nu_3(d(K)) = 4$, so that $r_3 = 1$. The pair of congruences (3) is solvable for $k = r_3 = 1$ with $t = 0$, but is not solvable for $k = r_3 + 1 = 2$. ■

The following lemma is an immediate consequence of Lemma 1.

Lemma 2. *Suppose (1) does not hold. Then the largest positive integer* n *for which the pair of congruences*

$$\left\{ \begin{array}{l} t^3 - at + b \equiv 0 \pmod{n^2}, \\ 3t^2 - a \equiv 0 \pmod{n}, \end{array} \right. \tag{4}$$

is solvable, is $n = \prod p^{r_p}$.

Numerically n can be found as the largest integer such that $n^2 | \triangle$ for which the pair of congruences (4) is solvable.

Now we use Lemma 2 to give Voronoi's method for finding an integral basis for K when (1) does not hold.

Theorem 2. *Suppose (1) does not hold. Let* n^2 *be the largest square dividing* $\triangle$ *for which the pair of congruences (4) is solvable for* t. *Then an integral basis for* K *is*

$$\{1, \theta, (t^2 - a + t\theta + \theta^2)/n\}.$$

Proof: If t is a solution of the pair of congruences (4) then $(t^2 - a + t\theta + \theta^2)/n$ is an algebraic integer as it is a root of the polynomial

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

which has rational integral coefficients. Since $d(1, \theta, (t^2 - a + t\theta + \theta^2)/n) = d(K)$, we deduce that $\{1, \theta, (t^2 - a + t\theta + \theta^2)/n\}$ is an integral basis for K. ∎

Example 1. *Let* $K = Q(\theta)$, *where* $\theta^3 - 6\theta + 32 = 0$. *Then* $a = 6$, $b = 32$, $n = 6$ *and* $t = 4$. *Hence an integral basis for* K *is* $\{1, \theta, (10 + 4\theta + \theta^2)/6\}$.

We can treat the case $a \equiv 3 \pmod{9}$ and $b^2 \equiv a + 1 \pmod{27}$ in a similar manner. In this case $\triangle$ is divisible by 729 and Voronoi's result is the following.

Theorem 3. *Suppose (1) holds. Let* n^2 *be the largest square dividing* $\triangle/729$ *for which the pair of congruences*

$$\left\{ \begin{array}{l} t^3 - at + b \equiv 0 \pmod{27n^2}, \\ 3t^2 - a \equiv 0 \pmod{9n}, \end{array} \right. \tag{5}$$

is solvable for t. *Then an integral basis for* K *is*

$$\{1, (-t + \theta)/3, (t^2 - a + t\theta + \theta^2)/9n\}.$$

Example 2. *Let* $K = Q(\theta)$, *where* $\theta^3 - 3\theta + 56 = 0$. *Then* $a = 3$, $b = 56$, $n = 1$ *and* $t = 1$. *Hence an integral basis for* K *is* $\{1, (-1+\theta)/3, (-2+\theta+\theta^2)/9\}$.

The integral basis for a pure cubic field given in [2, Theorem 6.4.13] and the integral basis for a cyclic cubic field given in [2, Theorem 6.4.11 and Corollary 6.4.12] follow from Theorems 2 and 3.

References

[1] Ş. Alaca, *p-Integral bases of a cubic field,* Proc. Amer. Math. Soc. **126**(1998), No. 7, 1949-1953.

[2] H. Cohen, *A Course in Computational Algebraic Number Theory,* Springer-Verlag, Fourth Printing (2000).

[3] B. N. Delone and D.K. Faddeev, *The Theory of Irrationalities of the Third Degree,* Translations of Mathematical Monographs, Amer. Math. Soc. Vol. 10 (1964).

[4] 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.

[5] G. Voronoi, *Concerning algebraic integers derivable from a root of an equation of the third degree,* Master's Thesis, St. Petersburg, (1894). (Russian)

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