Far East J. Math. Sci. (FJMS) **12**(1) (2004), 1-7

ON REAL CUBIC FIELDS WITH A UNIQUE FUNDAMENTAL UNIT

KENNETH S. WILLIAMS

(Received July 31, 2003)

Submitted by K. K. Azad

Abstract

Simple conditions are given which ensure that the cubic equation

$$x^3 + tx^2 + ux - 1 = 0 \quad (t, u \in \mathbb{Z})$$

has a unique real root $\theta > 1$ which is the unique fundamental unit (> 1) of the cubic field $K = Q(\theta)$.

1. Introduction

Let t and u be integers. Set

$$D = 4t^3 + u^2t^2 - 18ut - (4u^3 + 27). \tag{1.1}$$

We suppose that

$$t + u < 0, \tag{1.2}$$

$$t - u \neq 2, \tag{1.3}$$

$$D < 0. \tag{1.4}$$

2000 Mathematics Subject Classification: Primary 11R16, 11R27.

Key words and phrases: cubic field, fundamental unit.

The author was supported by Natural Sciences and Engineering Research Council of Canada grant A-7233.

Conditions (1.2) and (1.3) ensure that the cubic polynomial

$$f(x) = x^3 + tx^2 + ux - 1 \tag{1.5}$$

satisfies

$$f(1) < 0, \quad f(-1) \neq 0. \tag{1.6}$$

Thus $f(x)$ does not have ± 1 as roots and thus is irreducible in $\mathbb{Z}[x]$. The integer D is the discriminant of $f(x)$ [4, p. 83]. In view of (1.4), $f(x)$ has exactly one real root θ. Moreover, by the first inequality in (1.6) we have

$$\theta > 1. \tag{1.7}$$

Let $r + is$ and $r - is$ ($r \in \mathbb{R}$, $s \in \mathbb{R}\backslash\{0\}$) be the two nonreal roots of $f(x)$. Then

$$\begin{aligned} x^3 + tx^2 + ux - 1 &= (x - \theta)(x - (r + is))(x - (r - is)) \\ &= x^3 - (\theta + 2r)x^2 + (2r\theta + (r^2 + s^2))x - \theta(r^2 + s^2). \end{aligned}$$

Thus

$$t = -(\theta + 2r), \quad u = 2r\theta + (r^2 + s^2), \quad 1 = \theta(r^2 + s^2).$$

By (1.7) we have

$$r^2 + s^2 = \frac{1}{\theta} < 1$$

so that $|r| < 1$. Hence

$$t = -\theta - 2r < -1 - 2r \leq -1 + 2|r| < -1 + 2 = 1.$$

As $t \in \mathbb{Z}$ we deduce that

$$t \leq 0. \tag{1.8}$$

Further we have

$$\begin{aligned} t^2 - 2u &= (\theta + 2r)^2 - 2(2r\theta + (r^2 + s^2)) = \theta^2 + 2r^2 - 2s^2 \\ &> 1 - 2(r^2 + s^2) > 1 - 2 = -1 \end{aligned}$$

so that as $t^2 - 2u \in \mathbb{Z}$ we deduce

$$t^2 \geq 2u. \tag{1.9}$$

Set $K = Q(\theta)$. The field K is a real cubic field whose two conjugate fields are nonreal. Thus, by Dirichlet's unit theorem [2, Theorem 3.6, p. 101], the ring O_K of integers of K has a unique fundamental unit $\eta > 1$ such that every unit of O_K is of the form $\pm\eta^k$ for some $k \in \mathbb{Z}$. As $\theta \in K$ and θ is a root of a monic integral polynomial (namely $f(x)$), we have $\theta \in O_K$. As $\theta(\theta^2 + t\theta + u) = 1$, we see that $\theta | 1$ in O_K. Thus θ is a unit of O_K. Hence $\theta = \pm\eta^k$ for some $k \in \mathbb{Z}$. As $\theta > 1$ and $\eta > 1$ we must have

$$\theta = \eta^k, \quad k \in \mathbb{N}. \tag{1.10}$$

In this note we give a simple criterion on t and u which ensures that $\theta = \eta$.

2. Criterion for Fundamental Unit η of O_K to be θ

With the notation of Section 1, we prove the following theorem.

Theorem. *Let $M = M(t, u)$ be the largest positive integer such that*

$$M^2 | D, \ \frac{D}{M^2} \equiv 0 \text{ or } 1 \pmod 4, \ \frac{|D|}{M^2} \geq 23. \tag{2.1}$$

Let $m = m(t, u)$ be a real number such that

$$f(m) > 0, \ m \geq \left(\frac{3}{2}\right)^{\frac{2}{3}} (= 1.31 \text{ approx}). \tag{2.2}$$

If

$$M \leq \frac{|D|^{1/2}}{(27 + 4m^{3/2})^{1/2}} \tag{2.3}$$

then

$$\theta = \eta. \tag{2.4}$$

Proof. We denote the discriminant of K by $d(K)$ and the index of θ by $\operatorname{ind}\theta$ so that

$$D = (\operatorname{ind}\theta)^2 d(K). \tag{2.5}$$

Thus $(\operatorname{ind}\theta)^2 \mid D$. By Stickelberger's theorem [2, Theorem 2.6, p. 59] we have $d(K) \equiv 0$ or $1 \pmod 4$ so that

$$\frac{D}{(\operatorname{ind}\theta)^2} \equiv 0 \text{ or } 1 \pmod 4. \tag{2.6}$$

As K is a real cubic field with two nonreal conjugate fields, we have $|d(K)| \geq 23$ so that

$$\frac{|D|}{(\operatorname{ind}\theta)^2} \geq 23, \tag{2.7}$$

[3, Table 3.2, p. 437]. By the maximality of M we deduce that

$$\operatorname{ind}\theta \leq M. \tag{2.8}$$

Hence by (2.3) we have

$$|d(K)| = \frac{|D|}{(\operatorname{ind}\theta)^2} \geq \frac{|D|}{M^2} \geq 27 + 4m^{3/2}. \tag{2.9}$$

Thus, as $m \geq \left(\frac{3}{2}\right)^{\frac{2}{3}}$, we have

$$|d(K)| \geq 27 + 4 \cdot \frac{3}{2} = 33. \tag{2.10}$$

Then, by [1, Question 35, pp. 152-153], we deduce that

$$\eta^3 > \frac{|d(K)| - 27}{4}. \tag{2.11}$$

From (2.9) and (2.11), we obtain

$$\eta^3 > m^{3/2} \tag{2.12}$$

and so

$$\eta^2 > m. \tag{2.13}$$

Since f has a unique real root $\theta > 1$ and $f(m) > 0$, we must have

$$m > \theta. \tag{2.14}$$

From (1.7), (2.13) and (2.14), we deduce that

$$1 < \theta < \eta^2. \tag{2.15}$$

Then, from (1.10) and (2.15), we obtain $\theta = \eta$.

We emphasize that it is not necessary to know the discriminant $d(K)$ of the cubic field K in order to apply the theorem.

3. Polynomials having Fundamental Unit η as a Root

Running through those integers t between -39 and 0 (recall (1.8)) and those integers u between -39 and 39, which satisfy (1.2), (1.3) and $-1000 < D < 0$, we obtain the following table of polynomials $f(x) = x^3 + tx^2 + ux - 1$ of discriminant D having the fundamental unit η as a root.

It should be noted that the theorem does not always find the fundamental unit of a real cubic field with two nonreal embeddings although it does so in a great many cases. For example if $K = Q(\theta)$, where $\theta \in \mathbb{R}$ satisfies $\theta^3 - \theta^2 - 1 = 0$, then it can be deduced from [3, Table 3.2, p. 437] that the fundamental unit (> 1) of O_K is θ. However in this case

$$D = -31,\ M = 1,\ m = 1.466 \text{ (approx)},\ \frac{|D|^{\frac{1}{2}}}{(27 + 4m^{\frac{3}{2}})^{\frac{1}{2}}} = 0.953 \text{ (approx)} < 1.$$

$f(x)$	D	M	m	$\dfrac{\lvert D\rvert^{\frac{1}{2}}}{(27+4m^{\frac{3}{2}})^{\frac{1}{2}}}$
x^3-1x^2-1x-1	–44	1	1.840	1.091
x^3-2x^2+0x-1	–59	1	2.206	1.213
x^3-3x^2+1x-1	–76	1	2.770	1.293
x^3-2x^2-2x-1	–83	1	2.832	1.342
x^3-2x^2-1x-1	–87	1	2.547	1.418
x^3-4x^2+2x-1	–107	1	3.512	1.417
x^3-3x^2+0x-1	–135	1	3.104	1.662
x^3-6x^2+4x-1	–139	1	5.279	1.357
x^3-3x^2-2x-1	–175	1	3.628	1.790
x^3-4x^2+1x-1	–199	1	3.807	1.873
x^3-10x^2+6x-1	–211	1	9.372	1.220
x^3-5x^2-4x-1	–231	1	5.729	1.680
x^3-4x^2-3x-1	–247	1	4.686	1.912
x^3-8x^2+5x-1	–255	1	7.338	1.547
x^3-4x^2+0x-1	–283	1	4.061	2.177
x^3-4x^2-2x-1	–331	1	4.495	2.255
x^3-4x^2-1x-1	–335	1	4.288	2.315
x^3-7x^2+4x-1	–367	1	6.400	2.000
x^3-5x^2+1x-1	–416	2	4.836	2.446
x^3-5x^2-3x-1	–464	2	5.571	2.414
x^3-6x^2-4x-1	–491	1	6.627	2.271
x^3-5x^2+0x-1	–527	1	5.040	2.701
x^3-6x^2+2x-1	–563	1	5.679	2.634
x^3-5x^2-1x-1	–588	2	5.228	2.803
x^3-9x^2+5x-1	–608	2	8.421	2.208

$x^3 - 10x^2 - 6x - 1$	−643	1	10.577	1.977
$x^3 - 11x^2 + 6x - 1$	−671	1	10.435	2.036
$x^3 - 8x^2 - 5x - 1$	−695	1	8.596	2.332
$x^3 - 8x^2 + 4x - 1$	−731	1	7.484	2.591
$x^3 - 6x^2 + 1x - 1$	−751	1	5.859	2.995
$x^3 - 7x^2 - 4x - 1$	−863	1	7.548	2.802
$x^3 - 6x^2 + 0x - 1$	−891	3	6.028	3.215
$x^3 - 6x^2 - 2x - 1$	−931	1	6.341	3.201
$x^3 - 6x^2 - 1x - 1$	−959	1	6.188	3.290
$x^3 - 7x^2 + 2x - 1$	−983	1	6.725	3.187

Acknowledgement

The author would like to thank Mathieu Lemire for computing extensive tables of the fundamental unit in connection with this work.

References

[1] Daniel A. Marcus, Number Fields, Springer-Verlag, New York, Heidelberg, Berlin, 1977.

[2] Wladyslaw Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, Springer-Verlag, Berlin, Heidelberg, New York, 1990.

[3] M. Pohst and H. Zassenhaus, Algorithmic Algebraic Number Theory, Cambridge University Press, Cambridge, 1989.

[4] B. L. van der Waerden, Modern Algebra Vol. I, Frederick Ungar Publ. Co., New York, 1953.

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