Simplest Cubic Fields

Franz Lemmermeyer, Attila Pethö[1]

Franz Lemmermeyer
Bilkent University
Department of Mathematics
06800 Bilkent, Ankara
Turkey
franz@fen.bilkent.edu.tr

Attila Pethő
Laboratory of Informatics
University of Medicine
Nagyerdei Krt. 98
H–4032 Debrecen
Hungary
pethoe@peugeot.dote.hu

1. Introduction

In this paper we intend to show that certain integers do not occur as the norms of principal ideals in a family of cubic fields studied by Cohn [C], Shanks [Sh], and Ennola [E]. These results will simplify the construction of certain unramified quadratic extensions of such fields (cf. [Wa], [W] etc.).

For a natural number a, let $f_a = x^3 - ax^2 - (a+3)x - 1$, and let $K = K_a$ be the cyclic cubic number field generated by a root α of f_a. Let N denote the Norm $N_{K/\mathbb{Q}}$. Elements in K are said to be *associated* if their quotient is a unit in $\mathbb{Z}[\alpha]$. The polynomial $f = f_a$ has discriminant disc $f = m^2$, where $m = a^2 + 3a + 9$; if we assume m to be squarefree, then we have disc K = disc $f = m^2$ and $\mathcal{O}_K = \mathbb{Z}[\alpha]$ (there exist infinitely many such m, cf. Cusick [Cu]). Moreover it is easy to see that $\{1, \alpha, \alpha'\}$ also is an integral basis of $\mathcal{O}_K$: in fact, this follows from $(\alpha+1)(\alpha^2 - (a+1)\alpha - 2) = -1$. For this family of cyclic cubic fields, we will prove the following result:

Theorem 1. *For all $\gamma \in \mathbb{Z}[\alpha]$ either $|N\gamma| \ge 2a+3$, or γ is associated to an integer. Moreover, if $|N\gamma| = 2a+3$, then γ is associated to one of the conjugates of $\alpha - 1$.*

2. The Proof

We start the proof with the observation that the assertion is correct for $a < 7$ ("proof by inspection" using the decomposition law for cyclic cubic fields or by using the method described below, but with the actual values of α, α' and α''). Moreover, we remark that α, $\alpha' = -\frac{\alpha+1}{\alpha}$ and $\alpha'' = -\frac{1}{\alpha+1}$ are the roots of f. Choosing α as the smallest of the three roots and applying Newton's method, we find that

$$-1 - \frac{1}{a} < \alpha < -1 - \frac{1}{2a}, \quad -\frac{1}{a+2} < \alpha' < -\frac{1}{a+3}, \quad a+1 < \alpha'' < a+1+\frac{2}{a}.$$

These inequalities imply (for $a \ge 7$)

$$|\alpha - \alpha'| < 1 + \frac{1}{a}, \quad |\alpha' - \alpha''| < a+1+\frac{3}{a}, \quad \text{and } |\alpha'' - \alpha| < a+2+\frac{3}{a}.$$

In particular, we have

$$|\alpha - \alpha'| + |\alpha' - \alpha''| + |\alpha'' - \alpha| < 2a+4+\frac{7}{a} \le 2a+5.$$

[1]Research supported in part by Grant 1641 from the Hungarian National Foundation for Scientific Research

Moreover, we will need the relation

$$m = \alpha^2 + \alpha'^2 + \alpha''^2 - \alpha\alpha' - \alpha'\alpha'' - \alpha''\alpha = \det \begin{pmatrix} 1 & 1 & 1 \\ \alpha & \alpha' & \alpha'' \\ \alpha' & \alpha'' & \alpha \end{pmatrix},$$

which can be deduced easily from the well known fact that the square of this determinant equals disc $(1, \alpha, \alpha') = m^2$, making use of the formulae

$$\alpha\alpha' = -\alpha - 1, \quad \alpha^2 = a + 2 + a\alpha - \alpha'.$$

The units α'^{-1} and α'' satisfy the inequalities

$$a + 2 < |\alpha'^{-1}| < a + 3, \quad a + 1 < |\alpha''| < a + 2,$$

and this implies that, given two positive real numbers c_1 and c_2 and an element $\gamma \in Z[\alpha]$, we can find a unit η such that

$$c_1 \le |\gamma\eta| < (a+3)c_1, \quad c_2 \le |\gamma'\eta'| < (a+4)c_2. \tag{1}$$

This is a special case of a more general result which is valid for all number fields with unit rank ≥ 1; we will, however, give the proof only for totally real cubic fields K because the notation simplifies considerably. Let u_1 and u_2 be two independent units in K; their images in $\mathbb{R}^2$ upon their logarithmic embedding are $\operatorname{Log}(u_1) = v_1 = (\log|u_1|, \log|u_1'|)$ and $\operatorname{Log}(u_2) = v_2 = (\log|u_2|, \log|u_2'|)$. Dirichlet's unit theory shows that v_1 and v_2 are linear independent vectors. This implies that, for any $\xi \in K$, its image $\operatorname{Log}(\xi)$ can be moved into the fundamental domain spanned by v_1 and v_2 by adding and subtracting suitable multiples of v_1 and v_2, i.e. we can find a translate η of $Log(\xi)$ such that

$$\begin{aligned} c_1 &< |\eta| \le c_1 + \Big|\log|u_1|\Big| + \Big|\log|u_2|\Big|, \\ c_2 &< |\eta'| \le c_2 + \Big|\log|u_1'|\Big| + \Big|\log|u_2'|\Big| \end{aligned}$$

Translating this back to the field K and using the units α and α'', we see that we can find a unit η such that

$$c_1 \le |\gamma\eta| < |\alpha\alpha''|c_1, \quad c_2 \le |\gamma'\eta'| < |\alpha'^{-1}\alpha|c_2,$$

where we have chosen the exponents of α, α', α'' in such a way that their absolute value is > 1 (this comes from the absolute values on the log's). Inserting the bounds on $|\alpha|$, $|\alpha'|$, $|\alpha''|$ we get equation (1).

Writing $\xi = \gamma\eta = r + s\alpha + t\alpha'$ and $n = |N_{K/\mathbb{Q}}\xi|$, we find ($T = T_{K/\mathbb{Q}}$ denotes the trace):

$$mt = T\big(\xi(\alpha' - \alpha'')\big), \quad ms = T\big(\xi(\alpha'' - \alpha)\big), \quad mr = T\big(\xi(\alpha\alpha' - \alpha''^2)\big).$$

Letting $c_1 = c_2 = \sqrt[3]{n/(a+3)}$ we get $|\xi|$, $|\xi'|$, $|\xi''| < \sqrt[3]{n} \cdot (a+3)^{2/3}$, and this implies the bounds

$$\begin{aligned} |mt| &\le |\xi||\alpha' - \alpha''| + |\xi'||\alpha'' - \alpha| + |\xi''||\alpha - \alpha'| \\ &< \sqrt[3]{n}(a+3)^{2/3}(2a+5); \\ |ms| &\le |\xi||\alpha'' - \alpha| + |\xi'||\alpha - \alpha'| + |\xi''||\alpha' - \alpha''| \\ &< \sqrt[3]{n}(a+3)^{2/3}(2a+5). \end{aligned}$$

Using $n \le 2a + 3$ and $a \ge 7$ we find that $|t| \le 2, |s| \le 2$. Computing the actual values of α, α' and α'' for $1 \le a \le 6$ and carrying out the above procedure we get the same result.

Now we will look at the $\xi = r + s\alpha + t\alpha'$ that satisfy the following system of inequalities:

$$|s| \le 2, \ |t| \le 2, \quad |\xi\xi'\xi''| \le n \le 2a + 3,$$

$$|\xi|, \ |\xi'|, \ |\xi''| < \sqrt[3]{n}(a+3)^{2/3}.$$

A somewhat tedious computation yields $N_{K/\mathbb{Q}}(r + s\alpha + t\alpha') = r^3 + s^3 + t^3 + ar^2s + ar^2t + 3st^2 - (a^2 + 3a + 6)s^2t - (a+3)rt^2 - (a+3)rs^2 + (a^2 + a + 3)rst$, so for fixed s, t the norm of $r + s\alpha + t\alpha'$ is a cubic polynomial in r. This polynomial will be minimal for values of r in the neighborhood of its roots. We will distinguish the following cases:

(1) $s = t = 0$: then $\xi \in \mathbb{Z}$, and ξ (as well as γ) is associated to a natural number;

(2) $s = \pm 1$, $t = 0$: then $\xi = \alpha - r$ for some $r \in \mathbb{Z}$, and we find
$N_{K/\mathbb{Q}}\xi = -f(r) = -r^3 + ar^2 + (a+3)r + 1$.
The roots of this polynomial are $r \approx 0, r \approx -1$, and $r \approx a+1$, and now
$N\alpha = -N(\alpha+1) = 1$,
$N(\alpha-1) = N(\alpha+2) = 2a+3, \quad N(\alpha-a-1) = 2a+3$,
$N(\alpha-a) = -N(\alpha-a-2) = a^2+3a+1 > 2a+3$, if $a \geq 2$
show that either ξ is associated to 1, or $|N\xi| \geq 2a+3$.

(3) $s = \pm 2$, $t = 0$: proceeding as in case 2 and keeping in mind that we need examine only those $\xi = 2\alpha - r$ with r odd, we find that
$N(2\alpha+1) = -(2a+3), \quad N(2\alpha-1) = 6a+19$,
$N(2\alpha+3) = 6a-1, \quad N(2\alpha-2a-1) = 4a^2+24a+19$,
$N(2\alpha-2a-3) = -4a^2+17$.

(4) $s = 0, t = \pm 1$ and $s = 0, t = \pm 2$: this yields nothing new, because $\xi' = r + s\alpha'$ has already been examined.

(5) $s = t = \pm 1$: then $\xi = \alpha + \alpha' - r = -\alpha'' + a - r$, and therefore $\xi' = -\alpha + a - r$ is of the type studied in 2; since $N\xi = N\xi'$ we are done.

(6) $s = -t = \pm 1$: then $\xi = r + \alpha - \alpha'$, and

$$f(r) = N(\xi) = r^3 - (a^2+3a+9)r + (a^2+3a+9),$$

$$\begin{array}{lcrlcr}
f(1) & = & 1, & f(2) & = & -a^2-3a-1, \\
f(a+1) & = & -6a+1, & f(a+2) & = & 2a^2-1, \\
f(-a-2) & = & 6a+19, & f(-a-3) & = & -2a^2-6a+9
\end{array}$$

(7) $s = \pm 2, t = \mp 1$: then $\xi = r + 2\alpha - \alpha'$, and

$$f(r) = N(\xi) = r^3 + ar^2 - (2a^2+7a+21)r + (4a^2+12a+37),$$

$$\begin{array}{lcrlcr}
f(2) & = & 2a+3, & f(3) & = & -2a^2+1, \\
f(a+1) & = & -12a+17, & f(a+2) & = & 3a^2-7a+3, \\
f(-2a-3) & = & 30a+37, & f(-2a-4) & = & -6a^2+2a+57
\end{array}$$

(8) $s = \pm 2, t = \pm 1$: then $\xi = r + 2\alpha + \alpha' = r + a + \alpha - \alpha''$, and we can proceed as in 5, refering to case 6 instead of 2.

(9) $s = -t = \pm 2$: then $\xi = r + 2\alpha - 2\alpha'$, and according to 6 we have to consider only the case r odd, thus

$$f(r) = N(\xi) = r^3 - (12a+36+4a^2)r + 8a^2 + 24a + 72,$$

$$\begin{array}{llll}
f(1) & = 4a^2+12a+37, & f(3) & = -4a^2-12a-9, \\
f(2a+1) & = -8a^2-54a+37, & f(2a+3) & = 8a^2-30a-9, \\
f(-2a-3) & = 8a^2+78a+153, & f(-2a-5) & = -8a^2+6a+127.
\end{array}$$

(10) $s = t = \pm 2$: then $\xi = r + 2\alpha + 2\alpha' = r + 2(-\alpha'' + a) = r + 2a - 2\alpha''$ and we can proceed as in 5.

Assume now that $|N\gamma| = 2a+3$. Then the proof of the first assertion shows that γ is associated to one of the elements given in the second column Table 1.

In the third column we have given the factorization of the corresponding element as $\alpha - 1$ or $(\alpha-1)'$ or $(\alpha-1)''$ times a unit. The table consists of four subtables: in the first we collected those numbers whose norms are $2a+3$ for any a. In the remaining subtables you find the exceptional elements which appear only for $a = 1, 2$ or 3. The subtables are indicated with the values of a. The proof of the identities is straightforward and therefore omitted.

This completes the proof of Theorem 1. We acknowledge the help of Maple V (version 4.4) and PARI (version 1.38.3) in checking the computations.

3. Applications

From Theorem 1 we deduce the following

Corollary 2. *Assume that m is squarefree and that $2a+3 = b^2$ for some $b \in \mathbb{Z}$. Then, $L = K(\sqrt{\alpha+2}, \sqrt{\alpha'+2})$ is a quartic unramified extension of K with $Gal(L/K) \cong C_2 \times C_2$. In particular, $Cl(L)$ contains a subgroup of type $C_2 \times C_2$.*

Table 1.

	$\alpha - 1$	
	$\alpha + 2$	$-(\alpha-1)''(\alpha+1)$
	$\alpha - (a+1)$	$-(\alpha-1)'/(\alpha+1)$
	$2\alpha + 1$	$-(\alpha-1)'\alpha$
	$\alpha + \alpha' - a + 1$	$-(\alpha-1)''$
	$\alpha + \alpha' - a - 2$	$(\alpha-1)'\alpha/(\alpha+1)$
	$\alpha + \alpha' + 1$	$(\alpha-1)(\alpha+1)/\alpha$
	$2\alpha - \alpha' + 2$	$-(\alpha-1)'(\alpha+1)$
	$2\alpha + 2\alpha' - 2a - 1$	$-(\alpha-1)/(\alpha+1)$
$a = 1$	$\alpha - 3$	$(\alpha-1)''/(\alpha+1)$
	$2\alpha + 3$	$(\alpha-1)(\alpha+1)^2/\alpha$
	$\alpha + \alpha' + 2$	$-(\alpha-1)'(\alpha+1)/\alpha$
	$\alpha - \alpha' + 2$	$(\alpha-1)(\alpha+1)$
	$2\alpha + \alpha' - 3$	$-(\alpha-1)''\alpha/(\alpha+1)$
	$2\alpha + 2\alpha' - 5$	$(\alpha-1)''\alpha^2/(\alpha+1)$
$a = 2$	$\alpha - \alpha' + 4$	$(\alpha-1)\alpha$
	$2\alpha - \alpha' + 3$	$(\alpha-1)(\alpha+1)$
	$2\alpha + \alpha' - 6$	$(\alpha-1)''/(\alpha+1)$
$a = 3$	$2\alpha - \alpha' + 5$	$(\alpha-1)\alpha$
	$2\alpha - \alpha' - 10$	$-(\alpha-1)''/\alpha(\alpha+1)$

Proof. Suppose that $\alpha + 2$ is a square in $\mathcal{O}_K$; since $N(\alpha+2) = 2a+3 = b^2$, this implies that there is an element γ of norm $b < 2a+3$. Theorem 3.1. implies that γ is associated to an integer $r \in \mathbb{Z}$, hence $\alpha + 2 = r^2\varepsilon$ for some unit $\varepsilon \in \mathcal{O}_K^\times$. But $\{1, \alpha, \alpha'\}$ is an integral basis of $\mathcal{O}_K$, hence $r \mid (\alpha+2)$ implies that $r = \pm 1$.

The rest of the proof is the same as in [Wa], [W] or [L].

Similarly, we can show (cf. [Wa]):

Corollary 3. *Assume that $m > 13$ is squarefree and that $6a + 19 = b^2$ for some $b \in \mathbb{Z}$. Then, $L = K(\sqrt{\alpha(2\alpha-1)}, \sqrt{\alpha'(2\alpha'-1)})$ is a quartic unramified extension of K with $Gal(L/K) \cong C_2 \times C_2$. In particular, $Cl(L)$ contains a subgroup of type $C_2 \times C_2$.*

Remark: If $a = 1$, $m = 13$, we have $6a + 19 = (2a+3)^2$, i.e. b is a norm.

References

[C] H. Cohn, *A device for generating fields of even class number*, Proc. Amer. Math. Soc. **7** (1956), 595–598 1

[Cu] T.W. Cusick, *Lower bounds for regulators*, in.: Number Theory Noordwijkerhout, 1983, pp. 63–73, Ed.: H. Jager, LNM Vol. 1068, Springer Verlag, 1984 1

[E] V. Ennola, *Cubic fields with exceptional units*, Computational Number Theory Debrecen, Hungary 1989, pp. 103–128, Eds.: A. Pethő, M.E. Pohst, H.C. Williams and H.G. Zimmer, Walter deGruyter Verlag, 1991. 1

[L] Y.-Z. Lan, *Arithmetic properties of a class of cyclic cubic fields*, Sci. China **32** (1989), 922–928 4

[Sh] D. Shanks, *The simplest cubic number fields*, Math. Comp. **28** (1974), 1137–1152 1

[Wa] L. Washington, *Class numbers of the simplest cubic fields*, Math. Comp. **48** (1987), 371–384 1, 4

[W] M. Watabe, *On certain cubic fields IV*, Proc. Japan Acad. **59A** (1983), 387–389 1, 4