EXTRACTA MATHEMATICAE 2, n.2, 53-55 (1987)

RAMIFICATION AND UNITS OF THE CUBIC NUMBER FIELD $Q(\theta)$ GENERATED BY A ROOT OF $X^3 + abX + b = 0$

J.R. Delgado

This paper is the second part of [2] ;the same notation and and terminology are used.Except for our first theorem below we assume that θ is the only real root of the polynomial $X^3+ah^2kX +h^2k = 0$,where h and k are both square-free and relatively prime integers and a and k are negative integers.Hence θ is a positive real number and Dirichlet's Units Theorem tells that $K = Q(\theta)$ has as units group the set $U_K = \{\pm w^n : n = 0,\pm 1,\dots\}$.

THEOREM 1: The only rational primes p which ramify in K are those dividing its discriminant,namely:the prime factors of hkq and (eventually) $p = 3$ .Furthermore:

(1) if $p|hk$,then p is totally ramified in K ,that is,there exists a prime ideal p_1 in the ring R of algebraic integers of K such that $pR = p_1^3$;

(2) if $p|q$,then there are exactly two different prime ideals p_1 and p_2 of R such that $pR = p_1^2p_2$,except for (eventually) the case $3|q$;

(3) assume that 3 is ramified in K (equivalently, $3|\mathrm{disc}(R)$ as calculated in [2]);if this is the case, 3 is totally ramified except for exactly the following cases:(i) $3\nmid hk$ and $9|a$ or (ii) $(ahk,hk^2) \equiv (3,23),(12,14),(21,5),(6,22),(15,13),(24,4)$ mod 27 .

THEOREM 2: K is a pure cubic field if and only if the Delaunay-Nagell-Ljunggren equation $mX^3+nY^3 = c$ $(c = 1,3)$ has a solution in rational integers X and Y ,where m and n are cube-free relatively prime integers such that $cmn = -h^2k$ and $CXY = a$, in case that $C = 3,1$ when $c = 1,3$ .In this situation,one also gets $K = Q((m^2n)^{1/3})$

Remark: The equation quoted above is very well known.It has at most one non-trivial solution in rational integers and,in many cases,is unsolvable.In fact,an algorithm is available to look for solutions.In our case,once we fix h^2k there are at most finitely many values of a for which K is pure.

AMS Subject Classifications (1980):10B10,14G99.

We now deal with units. We shall use the fact that $1+a\theta = -\theta^3/h^2k$ is a unit, since it is an algebraic integer whose norm is equal to 1 .

THEOREM 3: For every d there are at most finitely many values of a , h and k such that $1+a\theta \in R^n$, with $n \geqslant 5$. Furthermore, those values are computable and, as a matter of fact, for $d = 1$ there are not any value of a , h and k with that property.

THEOREM 4: Once we fix h^2k there are at most finitely many values of a such that $1+a\theta \in R^3$. Furthermore, those values are computable, since K appears as pure cubic where the fundamental unit is known.

THEOREM 5: For every d there are at most finitely many values of a , h and k such that $1+a\theta \in R^2$. Furthermore, those values are computable and, as a matter of fact, $1+a\theta \notin R^2$ for $d = 1$.

THEOREM 5: Assume that K is not pure. For every d the unit $1+a\theta$ is the fundamental unit of K such that $0 < 1+a\theta < 1$, except for finitely many values of a , h and k .

COROLLARY: If $4a^3h^2k+27$ is square-free, then $1+a\theta$ is a fundamental unit of K , that is, $U_K = \{\pm(1+a\theta)^n : n = 0, \pm 1, \ldots\}$

Remark: Dirichlet's theorem about primes in arithmetic progression enables us to say that there are an infinitude of fields K for which our corollary holds.

The results in this paper and [2] have a lot of applications to diophantine equations. We shall present one of them. According to the calculus of disc(R) in [2] it is easy to see that R is monogenic (that is, there is an algebraic integer z such that R is a free abelian group with basis 1 , z , z^2) iff the diophantine equation below has solution in rational integers y and z :

$$(*) \qquad kdy^3-3ahky^2z+qhz^3 = 3$$

in case that $\{1,\theta_1,\theta_2/3\}$ is an integral basis of R . Let us choose $m = |n|+1$ with m and n square-free relatively prime integers (there are infinitely many values of m and n with such properties). Dedekind showed that $Q((mn^2)^{1/3})$ is monogenic when, for instance, $mn \equiv 0 \pmod 3$. A simple calculation shows that this pure cubic field appears as one of our fields K , namely, if $k = mn$, $h = 1$ and $a = -3$. When we take n to be negative, it holds $k = n(1-n)$, $h = 1$, $a = -3$, $d = 3(2n-1)$ and $q = 3$. This field K **satisfies** the hypothesis of th.1(1) of [2], hence it has $\{1, \theta_1, \theta_2/3\}$ as integral basis. Since it is monogenic, the above equation (*) must be solvable and we obtain that: if n is negative and prime with $1-n$, both are square-free and $n \equiv 0,1 \pmod 3$, then the diophantine equation

$$n(1-n)(2n-1)y^3+3n(1-n)y^2z+z^3 = 1$$

has a solution in ratinal integers y and z. Thus, if we take n to be $-2.3.5.7...p_k$ (the product of the first k primes), an equation like that has integers solutions. For instance,

$$18654510y^3-132930y^2z+z^3 = 1$$

is solvable (compare with [6];page 208).

REFERENCES

[1] B. Delaunay, On the complete solution of the equation $X^3d+Y^3 = 1$, Publ.Soc.Math.Charkow (1916).

[2] J.R. Delgado, Some questions concerning the cubic number field $Q(\theta)$ ..., Extracta Math. 1(3), 142-44.

[3] H. Cohn, A classical invitation to algebraic numbers and class fields, Springer-Verlag, Berlin-N.York, 1978.

[4] W. Ljunggren, On an improvement of a theorem of T. Nagell, Math. Scand. 1(1953), 297-309.

[5] D.A. Marcus, Number Fields, Springer-Verlag, N.York, 1977.

[6] L.J. Mordell, Diophantine Equations, Academic Press, 1969.

[7] T. Nagell, Solution complète de quelques équations cubiques à deux indéterminées, J.Math.Pur.Appl.,(9)4 (1925), 209-270.

[8] P. Samuel, Théorie algébrique des nombres, Hermann, 1967.

[9] M. Scarowsky, On units of certain cubic fields and the diophantine equation $x^3+y^3+z^3 = 3$, Proc.Amer.Math.Soc. 91(3), 1984, 351-356.

Departamento de Algebra, Universidad Complutense
28040 Madrid (Spain)