MATHEMATICS OF COMPUTATION
VOLUME 48, NUMBER 177
JANUARY 1987, PAGES 179-182

Special Units in Real Cyclic Sextic Fields

By Marie-Nicole Gras

Dedicated to Daniel Shanks

Abstract. We study the real cyclic sextic fields generated by a root w of $(X-1)^6 - (t^2+108)(X^2+X)^2$, $t \in \mathbf{Z} - \{0, \pm 6, \pm 26\}$. We show that, when t^2+108 is square-free (except for powers of 2 and 3), and $t \neq 0, \pm 10, \pm 54$, then w is a generator of the module of relative units. The details of the proofs are given in [3].

1. Introduction. The "simplest cubic fields" of D. Shanks [7] are generated by a root w_3 of

$$X^3 - tX^2 - (t+3)X - 1, \qquad t \in \mathbf{Z}, \tag{1}$$

and a conjugate of w_3 is $(-w_3 - 1)/w_3$.

We have given in [4] an analog for cyclic quartic fields; these fields are generated by a root w_4 of

$$X^4 - tX^3 - 6X^2 + tX + 1, \qquad t \in \mathbf{Z} - \{0, \pm 3\}, \tag{2}$$

and a conjugate of w_4 is $(w_4 - 1)/(w_4 + 1)$.

The main interest of these fields is that they have an explicit system of fundamental units and a relatively large class number. These class numbers have been computed in [7] for the cubic, and in [4] for the quartic case. A simplest cubic field is used in [6] to compute the first example where the real part of the class number of the pth cyclotomic field is larger than p; similarly, the corresponding quartic fields are used in [1] to prove a general inequality for the real part of the class number of some cyclotomic fields.

Real cyclic sextic fields are studied in [5], where a table of units and class numbers (for conductors less than 2021) is computed. Here we define sextic fields in which we can find θ such that a conjugate of θ is a homographic function of θ (in fact, this conjugate is $(\theta - 1)/(\theta + 2)$), but this element, even if it is a unit, is not a relative unit, as it was in cubic and quartic cases. From this element θ, we construct a relative unit w which is the analog of (1) and (2). First we recall some general results concerning relative units in real cyclic sextic fields, and then apply these results to our special family of units.

Received February 27, 1986.
1980 *Mathematics Subject Classification*. Primary 12A45, 12A35.

2. Relative Units. Let $K/\mathbf{Q}$ be a real cyclic sextic field of conductor f, let σ be a generator of its Galois group, and let k_2 and k_3 be the quartic and cubic subfields of K.

Let E be the group of units of K. We consider the group of relative units of K (i.e., the elements of E whose norm is ± 1 over k_2 and k_3); this group is $\langle \pm 1 \rangle \oplus E_*$, where

$$E_* = \{u \in E, u^{1-\sigma+\sigma^2} = 1\}. \tag{3}$$

Then E_* is a free module over $\mathbf{Z}[\sigma]/(1-\sigma+\sigma^2) \simeq \mathbf{Z}[\exp(2i\pi/6)]$; this implies that there exists a generating relative unit, i.e., a unit ε such that every unit $u \in E_*$ may be written

$$u = \varepsilon^{\lambda+\mu\sigma}, \qquad \lambda, \mu \in \mathbf{Z}; \tag{4}$$

moreover, if $\langle u \rangle$ is the submodule of E_* generated by u, $u \neq 1$, then we have

$$(E_* : \langle u \rangle) = \lambda^2 + \lambda\mu + \mu^2. \tag{5}$$

Using the general formula established in [2], we obtain an upper bound for $(E_* : \langle u \rangle)$ which is of the same kind as the one of [5]:

THEOREM 1. *If the conductor f of K is $\geqslant 28$, then for any unit $u \in E_* - \{1\}$ we have*

$$(E_* : \langle u \rangle) \leqslant M_* = \frac{16}{3} \frac{R_*(u)}{(\operatorname{Log}((f-20)/4))^2}, \tag{6}$$

where

$$R_*(u) = (\operatorname{Log}|u|)^2 + (\operatorname{Log}|u^\sigma|)^2 - (\operatorname{Log}|u|)(\operatorname{Log}|u^\sigma|). \tag{7}$$

3. A Family of Real Sextic Fields. Let $t \in \mathbf{Z}$; we consider the fields $K_t = \mathbf{Q}(\theta)$, where θ is a root of

$$P = X^6 - \frac{t-6}{2}X^5 - 5\frac{t+6}{4}X^4 - 20X^3 + 5\frac{t-6}{4}X^2 + \frac{t+6}{2}X + 1. \tag{8}$$

We show in [3] the following properties (P_1) to (P_5):

(P_1) If $t \in \mathbf{Z} - \{0, \pm 6, \pm 26\}$, then P is irreducible in $\mathbf{Q}[X]$, and $K_t = \mathbf{Q}(\theta)$ is a real cyclic sextic field; a generator σ of its Galois group is characterized by the relation $\sigma(\theta) = (\theta - 1)/(\theta + 2)$. We have $K_{-t} = K_t$ for all $t \in \mathbf{Z}$, and then we can suppose that $t \in \mathbf{N} - \{0, 6, 26\}$.

(P_2) The quadratic subfield of K_t is $k_2 = \mathbf{Q}(\sqrt{t^2 + 108})$.

(P_3) The cubic subfield of K_t is $k_3 = \mathbf{Q}(\varphi)$, where

$$\varphi = \theta^{-1-\sigma^3} = -\frac{2\theta + 1}{\theta(\theta + 2)}$$

and

$$\operatorname{Irr}(\varphi, \mathbf{Q}) = X^3 - \frac{t-6}{4}X^2 - \frac{t+6}{4}X - 1;$$

the discriminant of this polynomial is $((t^2 + 108)/16)^2$.

(P_4) The conductor f of K_t is given by the following procedure: Let m be the product of primes, different from 2 and 3, dividing $t^2 + 108$ with an exponent not congruent to 0 modulo 6; then $f = 4^k 3^l m$, where

$$k = 0 \quad \text{if } t \equiv 1 \bmod 2 \text{ or } t \equiv \pm 6 \bmod 16, \qquad k = 1 \quad \text{if not,}$$
$$l = 0 \quad \text{if } t \equiv 1 \bmod 3, \qquad l = 1 \quad \text{if } t \equiv 0 \bmod 27, \qquad l = 2 \quad \text{if not.}$$

(P_5) If $t \equiv 2 \bmod 4$, the polynomial P defined in (8) belongs to $\mathbf{Z}[X]$, θ is a unit of K_t, and $k_3 = \mathbf{Q}(\varphi)$, where

$$\operatorname{Irr}(\varphi, \mathbf{Q}) = X^3 - nX^2 - (n+3)X - 1, \quad \text{with } n = (t-6)/4;$$

then the fields k_3 are the "simplest cubic fields" recalled in (1).

4. The Group E_* for the Fields K_t. We consider the following element of K_t:

$$w = \theta^{1-\sigma^3} = -\frac{\theta(2\theta + 1)}{\theta + 2}; \tag{9}$$

then $w^\sigma = -\theta(\theta - 1)/(\theta + 1)(\theta + 2)$, and we verify that ($t \in \mathbf{N} - \{0, 6, 26\}$)

$$\operatorname{Irr}(w, \mathbf{Q}) = (X-1)^6 - (t^2 + 108)(X^2 + X)^2 \tag{10}$$

and, by construction, $w \in E_*$ (see (3)).

First, we study the size of w when $t \to +\infty$; we show that $\theta \sim t/2$, and then $w \sim -t$ and $w^\sigma \sim -1$. We deduce from this, that when $t \to +\infty$, we have

$$R_*(w) \sim (\operatorname{Log} t)^2. \tag{11}$$

Next, we study if w is a generator of E_*. By computing an upper bound for the roots of (10), and using (6), we obtain: If $t \geqslant 26$ and $f \geqslant 28$, then

$$(E_*: \langle w \rangle) \leqslant M_t = \frac{16}{3}\left(\frac{\operatorname{Log}(t+6)}{\operatorname{Log}((f-20)/4)}\right)^2. \tag{12}$$

Finally, using (4) and (5), we test if there exist λ, $\mu \in \mathbf{Z}$ such that $w = \varepsilon^{\lambda + \mu\sigma}$, for all λ, μ such that $\rho = \lambda^2 + \lambda\mu + \mu^2 \leqslant M_t$. The values of ρ which are to be considered are then $\rho = 3$, $\rho = 4$ or $\rho \geqslant 7$ ($\rho = 7, 9, 13, \ldots$):

(i) We have $\rho = 3$ if and only if there exists $v \in E_*$ such that $w = v^{1+\sigma}$, and we verify that this happens if and only if there exists $s \in \mathbf{Z}$ such that

$$t = s(s^2 + 9). \tag{13}$$

(ii) We have $\rho = 4$ if and only if there exists $u \in E_*$ such that $w = u^2$, and this is impossible, since w is not totally positive; then the index ρ is odd.

To apply (12), it is necessary to know the conductor f of K_t and then, using (P_4), the squares dividing $t^2 + 108$. So we obtain two infinite sets of fields K_t where a generator of E_* is known:

Definition 1. *Let T be the infinite set of $t \in \mathbf{N}$, $t \neq 0$, such that $t^2 + 108$ is square-free, except for powers of* 2 *and* 3.

For all $t \in T$, we consider the field $K_t = \mathbf{Q}(w)$, where w is defined in (10). The main result concerning this family is the following

THEOREM 2. *For all $t \in T - \{10, 54\}$, the unit w given by* (10) *is a generator of the module E_* of relative units of K_t.*

Proof. We verify, using (13), that $(E_* : \langle w \rangle) = 3$ if and only if $t = 10$ $(s = 1)$ and $t = 54$ $(s = 3)$. After this, we can prove, using (12), that for all $t > 90$, $(E_* : \langle w \rangle) < 7$, and we compute directly $(E_* : \langle w \rangle)$ for all fields K_t, $t \in T$, $t \leqslant 90$ [3].

Definition 2. *Let S be the infinite set of $s \in \mathbf{N}$, $s \neq 0, 2$, such that $s^2 + 3$ and $s^2 + 12$ are square-free, except for powers of* 2.

For all $s \in S$, let $t = s(s^2 + 9)$; we consider the field $L_s = K_t = \mathbf{Q}(w)$, where w is defined in (10). From (13), there exists a unit $v \in E_*$ such that $w = v^{1+\sigma}$, and we compute

$$\text{(14)} \qquad \operatorname{Irr}(v, \mathbf{Q}) = (X - 1)^6 + (s^2 + 12)(X^5 - X^4 - s^2X^3 - X^2 + X).$$

We have $t^2 + 108 = (s^2 + 3)^2(s^2 + 12)$; since $s \in S$, we deduce from (P_4) that the conductor f of L_s is

$$\text{(15)} \qquad f = \frac{(s^2 + 3)(s^2 + 12)}{e}, \quad \text{where } e \text{ divides } 48.$$

Let M_* be the upper bound of $(E_* : \langle v \rangle)$ given in (6). When $s \to +\infty$, from (11) there follows $R_*(v) \sim \frac{1}{3}(\operatorname{Log} s^3)^2$, and if $s \in S$, from (15) there follows $\operatorname{Log}((f - 20)/4) \sim \operatorname{Log} s^4$. Then,

$$\text{(16)} \qquad M_* \to 1 \quad \text{when } s \to +\infty \text{ and } s \in S.$$

This proves that the upper bound established in Theorem 1 cannot be improved for the set of real cyclic sextic fields.

In the same way, we prove in [3] the analog of Theorem 2 for the set S:

THEOREM 3. *For all $s \in S$, the unit v given by* (14) *is a generator of the module E_* of relative units of L_s.*

Remark. If $s \in S$ and if $s = 6r + 3$, then the conductor of k_2 is $f_2 = 36r^2 + 36r + 21$, and the fundamental unit of k_2 is

$$\varepsilon_2 = \left((12r^2 + 12r + 5) + (2r + 1)\sqrt{(36r^2 + 36r + 21)}\right)/2.$$

Since $t = (6r + 3)(36r^2 + 36r + 18) \equiv 2 \mod 4$, the field k_3 is a simplest cubic field. Then, if $s \in S$ and $s \equiv 3 \mod 6$, the three fields k_2, k_3, and K_t have an explicit system of fundamental units.

Université de Besançon et CNRS
Faculté des Sciences
Laboratoire de Mathématiques
U. A. n°040741
F-25030 Besançon Cédex, France

1. G. CORNELL & L. C. WASHINGTON, "Class numbers of cyclotomic fields," *J. Number Theory*, v. 21, 1985, pp. 260–274.

2. G. GRAS & M.-N. GRAS, "Calcul du nombre de classes et des unités des extensions abéliennes réelles de **Q**," *Bull. Sci. Math.* (2), v. 101, 1977, pp. 97–129.

3. M.-N. GRAS, "Familles d'unités dans les extensions cycliques réelles de degré 6 de **Q**," *Publ. Math. Besançon*, 1984/85–1985/86.

4. M.-N. GRAS, "Table numérique du nombre de classes et des unités des extensions cycliques réelles de degré 4 de **Q**," *Publ. Math. Besançon*, 1977/78, fasc. 2, pp. 1–26 & 1–53.

5. S. MÄKI, *The Determination of Units in Real Cyclic Sextic Fields*, Lecture Notes in Math., vol. 797, Springer-Verlag, Berlin and New York, 1980.

6. E. SEAH, L. C. WASHINGTON & H. C. WILLIAMS, "The calculation of a large cubic class number with an application to real cyclotomic fields," *Math. Comp.*, v. 41, 1983, pp. 303–305.

7. D. SHANKS, "The simplest cubic fields," *Math. Comp.*, v. 28, 1974, pp. 1137–1152.