MATHEMATICS OF COMPUTATION
VOLUME 45, NUMBER 172
OCTOBER 1985, PAGES 585–589

On Cyclic Cubic Fields

By Veikko Ennola and Reino Turunen

Abstract. A table of class numbers and units in cyclic cubic fields with conductor < 4000 has been given by Marie-Nicole Gras [6]. The authors have constructed an extended table for conductor < 16000. The article comprises lists of fields with totally positive fundamental units and fields in which the class group has a Sylow p-subgroup which is not elementary abelian. We also give statistics about the distribution of class numbers.

Let K be a cyclic cubic field with conductor f and denote by $\mathcal{O}$ the ring of integers of K. If $\alpha \in K$, its conjugates are denoted by α, α', α'' and the trace and norm by $\mathrm{Tr}(\alpha) = \alpha + \alpha' + \alpha''$ and $\mathrm{N}(\alpha) = \alpha\alpha'\alpha''$. We can write

$$f = (a^2 + 3b^2)/4, \tag{1}$$

where a and b satisfy the conditions

$$\begin{aligned} &a \equiv 2 \bmod 3, \quad b \equiv 0 \bmod 3, \quad b > 0 && \text{for } 3 \nmid f, \\ &a \equiv 6 \bmod 9, \quad b \equiv 3 \text{ or } 6 \bmod 9, \quad b > 0 && \text{for } 3 \mid f, \end{aligned} \tag{2}$$

introduced by Hasse [8, p. 12]. Let θ, θ', θ'' denote the Gaussian periods for a generating cubic character of K taken with a suitable sign. Then $K = \mathbf{Q}(\theta)$ and (see, e.g., [9, pp. 7-9])

$$\mathrm{Irr}(\theta, \mathbf{Q}) = \begin{cases} x^3 + x^2 + ((1-f)/3)x + (f(a-3)+1)/27 & \text{for } 3 \nmid f, \\ x^3 - (f/3)x - fa/27 & \text{for } 3 \mid f. \end{cases}$$

A unit τ of the ring $\mathcal{O}$ is called a *fundamental unit* iff -1, τ and τ' generate the group of units of $\mathcal{O}$. We shall further stipulate that

$$\mathrm{N}(\tau) = 1 \text{ and two of the conjugates of } \tau \text{ have absolute value } > 1. \tag{3}$$

It is easy to see that any fundamental unit satisfying (3) must be a conjugate of τ so that their minimal polynomial

$$\mathrm{Irr}(\tau, \mathbf{Q}) = x^3 - \mathrm{Tr}(\tau)x^2 + \mathrm{Tr}(\tau^{-1})x - 1 \tag{4}$$

is uniquely determined.

We note that (3) implies $|\mathrm{Tr}(\tau^{-1})| > |\mathrm{Tr}(\tau)|$. This can be easily seen as follows. Put $s = \mathrm{Tr}(\tau)$, $q = \mathrm{Tr}(\tau^{-1})$ and let δ denote the sign of that conjugate of τ which has absolute value < 1. Then, $\delta(s - q) < 0$ and $\delta(s + q + 2) > 0$, so that $|s| \geqslant |q|$ implies $s = -q$ or $s = -q - 1$. Under these conditions the discriminant of (4) is a square only for $s = -4$, $q = 3$, but, in this case, τ would not be a fundamental unit.

Received April 19, 1983; revised March 26, 1984.
1980 *Mathematics Subject Classification*. Primary 12–04, 12A30, 12A35, 12A45, 12A50.

0025-5718/85 $1.00 + $.25 per page

Tables containing the coefficients of (4) and the class number h of K have been given by M. N. Gras [6] (i) systematically for $f < 4000$, (ii) in the cases $h \equiv 0 \bmod 9$ and $h \equiv 0 \bmod 4$ for $4000 < f < 10000$, and (iii) for certain particular families of fields with $4000 < f < 20000$. The choice of the parameters a, b in [6] is different from ours, owing to the fact that we have stuck to Hasse's old normalization (2). Thus, our numbers a, b are the same as $-a$, $3b$ in M. N. Gras's notation. In the tables of M. N. Gras there are a number of gaps which have been filled independently by Godwin [2], whose method is entirely different from ours, and by ourselves. The two results agree exactly.

We have constructed an extended table of the 1906 fields with $4000 < f < 16000$. (The total number of cyclic cubic fields with $f < 16000$ is $630 + 1906 = 2536$.) The table is deposited in the Mathematics of Computation's UMT-depository. It consists of three parts, the kth part containing the fields with $4000k < f < 4000(k + 1)$. For each field K the following data are given:

- running number r
- conductor f
- parameters a, b
- class number h
- coefficients $\mathrm{Tr}(\tau)$, $\mathrm{Tr}(\tau^{-1})$ of the polynomial (4).

The number $\mathrm{Tr}(\tau^{-1})$ is written underneath $\mathrm{Tr}(\tau)$ in case there is not enough space for both of them on the same line. The fields are arranged lexicographically according to increasing values of f and b.

The method employed in the computation is essentially the same adaptation of the Voronoi algorithm that we used in [1] to construct a table of totally real cubic fields. In the cyclic case, the unit lattice in the logarithmic space is hexagonal and, therefore, the reduced units determined by our algorithm are conjugates and thus both fundamental units. In fact, one of our reliability tests is based on calculating both units separately and on checking the equality of the minimal polynomials. A disadvantage of the Voronoi algorithm is the fact that the units produced by it

TABLE 1

f	a	b	h	f	a	b	h	f	a	b	h
703	−25	27	12	711	−12	30	12	1009	−43	27	4
1699	−64	30	4	3193	−55	57	12	4291	−64	66	12
4357	119	33	4	4561	−37	75	4	4639	41	75	4
5257	−115	51	12	6037	−154	12	4	6289	−91	75	12
6381	−93	75	12	6553	155	27	4	7027	161	27	4
7639	−172	18	4	8029	−178	12	36	8191	92	90	4
8557	179	27	12	8659	−169	45	12	8797	14	108	84
9109	38	108	4	9217	146	72	12	9283	−13	111	4
9667	191	27	12	9667	−160	66	12	10147	−121	93	12
10399	23	117	4	10771	−64	114	4	11241	−201	39	12
11257	125	99	4	12127	185	69	12	12757	221	27	4
13297	194	72	4	13459	113	117	12	13531	−193	75	12
13921	197	75	4	14209	−217	57	12	14287	−4	138	36
14449	239	15	4	14521	122	120	36	14689	−133	117	12
14917	86	132	12	15139	209	75	4	15237	−246	12	12

TABLE 2

f	a	b	h	Generators of G	Relations	Invariants of G
1777	14	48	16	$\mathrm{Cl}\,\mathfrak{p}_2, \mathrm{Cl}\,\mathfrak{p}_2'$	$\mathfrak{p}_2^4 \sim \mathfrak{p}_2'^4 \sim 1$	4,4
2817	−66	48	48	$\mathrm{Cl}\,\mathfrak{p}_2, \mathrm{Cl}\,\mathfrak{p}_2'$	$\mathfrak{p}_2^{12} \sim 1, \mathfrak{p}_2'^4 \sim \mathfrak{p}_2^4$	3,4,4
4297	131	3	16	$\mathrm{Cl}\,\mathfrak{p}_{13}, \mathrm{Cl}\,\mathfrak{p}_{13}'$	$\mathfrak{p}_{13}^4 \sim \mathfrak{p}_{13}'^4 \sim 1$	4,4
4711	113	45	27	$\mathrm{Cl}\,\mathfrak{p}_3, \mathrm{Cl}\,\mathfrak{p}_3'$	$\mathfrak{p}_3^9 \sim 1, \mathfrak{p}_3'^3 \sim \mathfrak{p}_3^3$	3,9
4711	−76	66	27	$\mathrm{Cl}\,\mathfrak{p}_2, \mathrm{Cl}\,\mathfrak{p}_2'$	$\mathfrak{p}_2^9 \sim 1, \mathfrak{p}_2'^3 \sim \mathfrak{p}_2^3$	3,9
5383	92	66	27	$\mathrm{Cl}\,\mathfrak{p}_2, \mathrm{Cl}\,\mathfrak{p}_2'$	$\mathfrak{p}_2^9 \sim 1, \mathfrak{p}_2'^3 \sim \mathfrak{p}_2^3$	3,9
5383	−43	81	27	$\mathrm{Cl}\,\mathfrak{p}_3, \mathrm{Cl}\,\mathfrak{p}_3'$	$\mathfrak{p}_3^9 \sim 1, \mathfrak{p}_3'^3 \sim \mathfrak{p}_3^3$	3,9
5409	−147	3	48	$\mathrm{Cl}\,\mathfrak{p}_{11}, \mathrm{Cl}\,\mathfrak{p}_{11}'$	$\mathfrak{p}_{11}^{12} \sim 1, \mathfrak{p}_{11}'^4 \sim \mathfrak{p}_{11}^4$	3,4,4
6139	−16	90	48	$\mathrm{Cl}\,\mathfrak{p}_2, \mathrm{Cl}\,\mathfrak{p}_2'$	$\mathfrak{p}_2^{12} \sim 1, \mathfrak{p}_2'^4 \sim \mathfrak{p}_2^4$	3,4,4
6247	−151	27	16	$\mathrm{Cl}\,\mathfrak{p}_{11}, \mathrm{Cl}\,\mathfrak{p}_{11}'$	$\mathfrak{p}_{11}^4 \sim \mathfrak{p}_{11}'^4 \sim 1$	4,4
7351	−1	99	49	$\mathrm{Cl}\,\mathfrak{p}_3$	$\mathfrak{p}_3^{49} \sim 1$	49
7657	170	24	81	$\mathrm{Cl}\,\mathfrak{p}_2, \mathrm{Cl}\,\mathfrak{p}_2', \mathrm{Cl}\,\mathfrak{p}_5$	$\mathfrak{p}_2^9 \sim 1, \mathfrak{p}_2'^3 \sim \mathfrak{p}_2^3, \mathfrak{p}_5^3 \sim \mathfrak{p}_2^6$	3,3,9
8563	185	3	49	$\mathrm{Cl}\,\mathfrak{p}_5$	$\mathfrak{p}_5^{49} \sim 1$	49
9247	−76	102	48	$\mathrm{Cl}\,\mathfrak{p}_2, \mathrm{Cl}\,\mathfrak{p}_2'$	$\mathfrak{p}_2^{12} \sim 1, \mathfrak{p}_2'^4 \sim \mathfrak{p}_2^4$	3,4,4
10513	−205	3	64	$\mathrm{Cl}\,\mathfrak{p}_{11}, \mathrm{Cl}\,\mathfrak{p}_{11}'$	$\mathfrak{p}_{11}^8 \sim \mathfrak{p}_{11}'^8 \sim 1$	8,8
11167	−181	63	27	$\mathrm{Cl}\,\mathfrak{p}_3, \mathrm{Cl}\,\mathfrak{p}_3'$	$\mathfrak{p}_3^9 \sim 1, \mathfrak{p}_3'^3 \sim \mathfrak{p}_3^3$	3,9
11167	116	102	27	$\mathrm{Cl}\,\mathfrak{p}_2, \mathrm{Cl}\,\mathfrak{p}_2'$	$\mathfrak{p}_2^9 \sim 1, \mathfrak{p}_2'^3 \sim \mathfrak{p}_2^3$	3,9
12403	173	81	27	$\mathrm{Cl}\,\mathfrak{p}_3, \mathrm{Cl}\,\mathfrak{p}_3'$	$\mathfrak{p}_3^9 \sim 1, \mathfrak{p}_3'^3 \sim \mathfrak{p}_3^3$	3,9
12403	65	123	27	$\mathrm{Cl}\,\mathfrak{p}_5, \mathrm{Cl}\,\mathfrak{p}_5'$	$\mathfrak{p}_5^9 \sim 1, \mathfrak{p}_5'^3 \sim \mathfrak{p}_5^3$	3,9
12439	−223	3	27	$\mathrm{Cl}\,\mathfrak{p}_{31}, \mathrm{Cl}\,\mathfrak{p}_{31}'$	$\mathfrak{p}_{31}^9 \sim 1, \mathfrak{p}_{31}'^3 \sim \mathfrak{p}_{31}^3$	3,9
12439	209	45	27	$\mathrm{Cl}\,\mathfrak{p}_3, \mathrm{Cl}\,\mathfrak{p}_3'$	$\mathfrak{p}_3^9 \sim 1, \mathfrak{p}_3'^3 \sim \mathfrak{p}_3^3$	3,9
14527	164	102	147	$\mathrm{Cl}\,\mathfrak{p}_2$	$\mathfrak{p}_2^{147} \sim 1$	3,49
15561	−246	24	243	$\mathrm{Cl}\,\mathfrak{p}_2, \mathrm{Cl}\,\mathfrak{p}_2', \mathrm{Cl}\,\mathfrak{p}_3, \mathrm{Cl}\,\mathfrak{p}_7$	$\mathfrak{p}_2^9 \sim \mathfrak{p}_3^3 \sim \mathfrak{p}_7^3 \sim 1, \mathfrak{p}_2'^3 \sim \mathfrak{p}_2^3$	3,3,3,9
15823	245	33	16	$\mathrm{Cl}\,\mathfrak{p}_7, \mathrm{Cl}\,\mathfrak{p}_7'$	$\mathfrak{p}_7^4 \sim \mathfrak{p}_7'^4 \sim 1$	4,4
15889	−238	48	16	$\mathrm{Cl}\,\mathfrak{p}_2, \mathrm{Cl}\,\mathfrak{p}_2'$	$\mathfrak{p}_2^4 \sim \mathfrak{p}_2'^4 \sim 1$	4,4

(before the reduction) are excessively large in some cases. In the largest case we have encountered, i.e., $(f, a, b) = (15679, -196, 90)$, the coordinates of these units with respect to the integral basis $\{1, \theta, \theta'\}$ have about 1400 digits while $\mathrm{Tr}(\tau^{-1})$ has 110 digits. Therefore, an efficient method is needed to deal with the large cases if one wants to pursue the computations further along these lines. There are 921 prime conductors less than 16000 and it seems that in most of the very large cases the conductor is one of them.

Much work has been done on unit signatures (see, e.g., [4] and [5]). There are 45 cyclic cubic fields with $f < 16000$ such that τ is totally positive, i.e., $\mathrm{Tr}(\tau) > 0$, $\mathrm{Tr}(\tau^{-1}) > 0$. These fields and their class numbers h are listed in Table 1.

Contrary to the general totally real cubic case [1], the Sylow p-subgroups of the class group G are elementary abelian for most fields K. This peculiarity of cyclic fields has been elucidated in [10]. In Table 2 we collect all the fields K with $f < 16000$ such that the ideal class group G of K has a Sylow p-subgroup which is not elementary abelian. For $f = 7351$ and 8563 the structure of G has been determined by Smadja [11], and for $f = 4711$, 5383, 7657 the result follows from [3]. By $\mathfrak{p}_p$ we denote a prime ideal with norm $\mathrm{N}(\mathfrak{p}_p) = p$, $\mathrm{Cl}\,\mathfrak{p}_p$ is the ideal class containing it, and $\mathfrak{p}_p'$ is a conjugate ideal. The symbol $\sim$ indicates equivalence of ideals.

Table 3 gives statistics referring to the class numbers h. The numbers at the top of each column are the bounds on the conductor.

TABLE 3

h	1 4000	4001 8000	8001 12000	12001 16000	Σ
1	230	186	171	170	757
3	249	236	238	227	950
4	24	23	23	27	97
7	10	4	7	2	23
9	64	91	108	101	364
12	27	35	32	29	123
13	2	1	2	1	6
16	1	3	0	2	6
19	5	1	1	1	8
21	8	14	11	9	42
25	0	1	0	1	2
27	2	11	11	18	42
28	0	3	2	0	5
31	0	1	3	0	4
36	5	11	7	18	41
37	0	0	1	1	2
39	1	2	4	10	17
43	0	0	1	1	2
48	1	2	1	0	4
49	0	1	2	0	3
57	0	3	0	2	5
61	0	0	0	2	2
63	1	3	4	3	11
64	0	0	1	0	1
73	0	0	1	0	1
75	0	2	0	0	2
81	0	1	0	0	1
84	0	1	1	0	2
93	0	0	0	1	1
109	0	0	1	1	2
111	0	0	0	1	1
117	0	0	2	1	3
127	0	0	0	1	1
147	0	0	0	1	1
171	0	1	0	0	1
228	0	1	1	0	2
243	0	0	0	1	1
Σ	630	638	636	632	2536

Let t denote the number of ramified primes. It is well-known that the number of ambiguous classes is 3^{t-1}. For $h = 27$, it is not hard to see that the structure of G (even as a $\mathrm{Gal}(K/\mathbf{Q})$-module) is determined by t. For $t = 2$ we have the 10 cases with $G \cong (\mathbf{Z}/3\mathbf{Z}) \oplus (\mathbf{Z}/9\mathbf{Z})$ listed above. For $t = 3$ and 4 there are, respectively, 25 and 7 fields with $G \cong (\mathbf{Z}/3\mathbf{Z})^3$. In the latter case the action of $\mathrm{Gal}(K/\mathbf{Q})$ on G is trivial, all fields having conductor $f = 15561$.

The elementary abelian class group of order 16 occurs for $(f, a, b) = (7687, -169, 27)$ and is generated by $\mathrm{Cl}\ \mathfrak{p}_3$, $\mathrm{Cl}\ \mathfrak{p}_3'$, $\mathrm{Cl}\ \mathfrak{p}_{13}$, $\mathrm{Cl}\ \mathfrak{p}_{13}'$.

For $(f, a, b) = (10267, -1, 117)$ we have $G \cong (\mathbf{Z}/7\mathbf{Z})^2$, as has been first shown in [11].

It is obvious that a 5-class group of order 25 must be noncyclic. This occurs for $(f, a, b) = (6901, -154, 36), (7441, -46, 96)$ when $h = 75$, and for $(f, a, b) = (7753, -58, 96), (15937, -190, 96)$ when $h = 25$. All these groups are generated by $\mathrm{Cl}\ \mathfrak{p}_2$, $\mathrm{Cl}\ \mathfrak{p}_2'$ with relations $\mathfrak{p}_2^{h/5} \sim 1$, $\mathfrak{p}_2'^5 \sim \mathfrak{p}_2^5$.

All of the computations were done on the DEC-20 computer at the University of Turku, Finland, and we would like to express our gratitude to the members of the staff of the Computer Center for their cooperation. The work has been supported financially by the Academy of Finland.

Department of Mathematics
University of Turku
SF-20500 Turku 50
Finland

1. VEIKKO ENNOLA & REINO TURUNEN, "On totally real cubic fields," *Math. Comp.*, v. 44, 1985, pp. 495–518.

2. H. J. GODWIN, "The calculation of large units in cyclic cubic fields," *J. Reine Angew. Math.*, v. 338, 1983, pp. 216–220.

3. GEORGES GRAS, "Sur les l-classes d'ideaux dans les extensions cycliques relatives de degré premier l," I, II, *Ann. Inst. Fourier (Grenoble)*, v. 23, no. 3, 1973, pp. 1–48; *ibid.*, v. 23, no. 4, 1973, pp. 1–44. MR **50** #12967.

4. GEORGES GRAS & MARIE-NICOLE GRAS, "Signature des unités cyclotomiques et parité du nombre de classes des extensions cycliques de $\mathbf{Q}$ de degré premier impair," *Ann. Inst. Fourier (Grenoble)*, v. 25, no. 1, 1975, pp. 1–22. MR **52** #13728.

5. MARIE-NICOLE GRAS, "Sur le nombre de classes du sous-corps cubique de $\mathbf{Q}^{(p)}$, $p \equiv 1$ (3)," *Séminaire de Théorie des Nombres*, 1971-1972 (Univ. Bordeaux I, Talence), Exp. No. 2 bis, 1972, 9pp. MR **53** #346.

6. MARIE-NICOLE GRAS, "Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de $\mathbf{Q}$," *J. Reine Angew. Math.*, v. 277, 1975, pp. 89–116. MR **52** #10675.

7. M. N. GRAS, N. MOSER & J. J. PAYAN, "Approximation algorithmique du groupe des classes de certains corps cubiques cycliques," *Acta Arith.*, v. 23, 1973, pp. 295–300. MR **48** #8437.

8. H. HASSE, "Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern," *Abh. Deutsch. Akad. Wiss. Berlin, Math.-Naturw. Kl.*, **1948**, No. 2, 1950. MR **11**, 503.

9. SIRPA MÄKI, *The Determination of Units in Real Cyclic Sextic Fields*, Lecture Notes in Math., vol. 797, Springer-Verlag, Berlin and New York, 1980. MR **82a**: 12004.

10. DANIEL SHANKS, "The simplest cubic fields," *Math. Comp.*, v. 28, 1974, pp. 1137–1152. MR **50** #4537.

11. RENÉ SMADJA, "Sur le groupe des classes des corps de nombres," *C. R. Acad. Sci. Paris Sér. A-B*, v. 276, 1973, pp. A1639-A1641. MR **49** #10661.