MATHEMATICS OF COMPUTATION, VOLUME 27, NUMBER 121, JANUARY, 1973

Quadratic Fields with Four Invariants Divisible by 3

By Daniel Shanks and Richard Serafin

Abstract. Imaginary quadratic fields are developed that have four invariants divisible by 3. Their associated real fields are found to differ in one significant respect: one case has two elementary generators and the other has only one.

1. Series 6. The number of invariants of a quadratic field $Q(d^{1/2})$ that are divisible by 3 equals the number of factors in the 3-Sylow subgroup of its class group. Following Scholz [1], we use r for this number if $d < 0$ and s if $d > 0$. The first case of $r = 1$ is $Q((-23)^{1/2})$. This has $C(3)$ as its class group. The first case [2] of $r = 2$ is $Q((-3299)^{1/2})$ with $C(9) \times C(3)$. The smallest *known* case [3] of $r = 3$ is $Q((-63199139)^{1/2})$ with $C(3) \times C(3) \times C(3) \times C(116)$. These three discriminants are

$$-D_6(1), \quad -D_6(-2), \quad -D_6(28),$$

respectively, where

$$D_6(z) = 108z^4 - 148z^3 + 84z^2 - 24z + 3. \tag{1}$$

It was proven in [3] that $r \geqq 2$ for all square-free discriminants $-D_6(z)$ with $z \equiv 1 \pmod 3$ except for the degenerate $z = 1$. It was also shown that $r = 3$ for

$$z = 28, \quad -29, \quad 34, \quad -41, \quad -44, \quad 46, \tag{2}$$

and while it was not proven that $-D_6(z)$ yields infinitely many cases of $r > 2$, that seemed very probable. If one continues (2), one finds that $r = 3$ also for

$$z = 79, \quad -92, \quad -122, \quad -125, \quad 127, \quad -131, \quad 148, \quad -164. \tag{2a}$$

Empirically, about 1/6 of all square-free $D_6(z)$ have $r > 2$ and it seemed plausible [3] that after a moderate number of such $r > 2$ were located, an example of $r = 4$ would appear. But this was not pursued at the time.

Recently, we learned from Professor D. J. Lewis that a doctoral student of his, Maurice Craig [4], had constructed a $Q((-D)^{1/2})$ with $r = 4$. No details were conveyed except that D is very large, of the order of $400 \cdot 10^{100}$, and so it is not suitable for a detailed numerical examination. To prove the existence of an $r = 4$, only one case is needed, but, analytically speaking, some interest attaches to the size of the smallest such D. Thus, we could ask: How big must D be for the Diophantine equation

$$4a^3 = b^2 + c^2 D \tag{3}$$

to have 81 distinct solutions with $0 < a < (D/3)^{1/2}$, $0 < b$, $(b, c) \leqq 2$? Such solutions

Received May 15, 1972.
AMS (MOS) subject classifications (1970). 12A25, 12A50.

correspond to ideals $\mathfrak{A} = (a, (b + c(-D)^{1/2})/2)$ whose cube is principal:

$$\mathfrak{A}^3 = \left(\frac{b + c(-D)^{1/2}}{2}\right).$$

Since it appeared likely that a much smaller D could be obtained with $D_6(z)$, we therefore continued (2) and found that the next case after (2a) does have $r = 4$. This is

$$\text{(2b)} \qquad D = D_6(169) = 87386945207 = 167 \cdot 12409 \cdot 42169$$

which has the class group

$$\text{(4)} \qquad C(3) \times C(3) \times C(3) \times C(3) \times C(1448) \times C(2).$$

To verify that $[C(3)]^4$ is a subgroup, it suffices to verify the 14 solutions of (3) in Table 1.

TABLE 1

a	b	c	Structure
113738	76715859	1	J
6854	1095693	-1	K
89158	40480625	117	J^2K
11904	2580707	1	J^2K^2
22574	6776883	1	L
106028	65782389	71	J^2L
164511	133418432	10	JL
112456	2509283	255	K^2L^2
73278	18341941	-119	KL^2
96774	20911027	-191	$J^2K^2L^2$
11321	459414	-8	JK^2L^2
31972	8186767	-27	J^2KL^2
131167	38385160	294	JKL^2
2802	24685	1	M

These 14, together with their 14 inverses obtained by changing the sign of c, correspond to 28 ideals of order 3 and minimal norm a within their respective equivalence classes. Since the identity of a class group with $r < 4$ can have at most 27 such cube-roots, we must have $r \geqq 4$.

The entries J, K, L, M constitute four generators and the products of the first three make up the other rows in Table 1 and their inverses: J^2, K^2, JK^2, etc. J is the "elementary explicit cube-root" [3] given by

$$a = 4z^2 - 3z + 1, \qquad b = 16z^3 - 18z^2 + 6z - 1, \qquad c = 1.$$

The remaining 26 values of a are obtained by taking all ideal products with M. They are, in order of size, 3378, 4208, $\cdots$, 156228. All 40 values of a are distinct. The four generators could have been selected in 24261120 ways; e.g., in place of the K and L shown we could have taken the smaller 3378 and 4208, both of which also have $c = 1$.

By Scholz's theorem [1] and Theorem 3 of [3], the real field $Q(\sqrt{3D_6(169)})$ will have $s = 3$. Its group is

$$C(9) \times C(3) \times C(3) \times C(16) \times C(2).$$

Since its class number $h = 2592$ is relatively large for a real field, its fundamental unit $\epsilon = (T + U(3D)^{1/2})/2$ is correspondingly not too large to be given exactly:

$$T = 9\ 6179600759\ 7355406365\ 7316493191\ 5352034585, \tag{5}$$
$$U = 187844\ 7508730142\ 6405065469\ 7450227699.$$

It is desirable to explain how the $r = 4$ here comes about. In [3], it is proven that $r = s + 1$ for $-D_6(z)$ and $3D_6(z)$, $z \equiv 1 \pmod 3$, and of the two solutions of

$$4a^3 = b^2 - c^2 3D$$

given by

$$a = 3z, \qquad b = 54z^2 - 36z + 9, \qquad c = 3, \tag{6a}$$

$$a = 3z - 2, \qquad b = 54z^2 - 36z + 7, \qquad c = 3, \tag{6b}$$

at least one corresponds to an ideal of order 3 in $Q((3D)^{1/2})$. Then $s = 2$ and $r = 3$ will occur if

(1) both ideals (6a, b) are of order 3 and independent, or

(2) a third ideal, independent of (6a) and (6b), is of order 3.

Both possibilities happen. Then, as predicted in [5, p. 86], if *both* (1) and (2) occur we will have $s = 3$ and $r = 4$. This happens for $z = 169$ with the fourth power of a prime ideal of norm 5. The prime ideal is of order 12, and its fourth power is a third, independent generator. Owing to the size of ϵ, its b and c are large:

$$a = 625,$$
$$b = 1228199422\ 5220152913, \tag{6c}$$
$$c = 2398\ 7499711333.$$

Continuing $D_6(z)$ for a few more values of z (to comprise exactly 100 discriminants) yields two more examples of $r = 3$ at $z = -170$ and $z = 175$.

2. Series 3. Series 3 are [3] the square-free

$$D_3(y) = 27y^4 - 74y^3 + 84y^2 - 48y + 12 \tag{7}$$

with $y \equiv -1 \pmod 6$. We did not similarly extend the earlier table of $D_3(y)$ by examining each successive case; we confined ourselves to selected $D_3(y)$ that are either prime or, on the contrary, have many factors. Thus,

$$D = D_3(-235) = 83309629817 \equiv 1 \pmod 4) \tag{8}$$

is prime and the class group of $Q((-D)^{1/2})$ is

$$C(9) \times C(3) \times C(3) \times C(3) \times C(724) \tag{9}$$

with $r = 4$. The 40 inequivalent ideals $(a, b + c(-D)^{1/2})$ satisfying $a^3 = b^2 + c^2D$ are listed in Table 2.

TABLE 2

$a^3 = b^2 + c^2$ 83309629817

a	b	c	a	b	c
6957	58985	2	140317	50197121	54
7629	332839	2	150421	6140438	201
7898	399282	2	176538	72976990	46
9218	670842	2	181157	48022254	209
11714	1128774	2	193773	28935833	278
16258	1139390	6	194338	84241810	54
45482	9682530	2	204369	2215897	320
47381	7368846	25	222314	104819874	2
47441	9243687	16	226409	101197899	128
63029	15813261	2	232261	37007227	366
78282	21894850	2	234981	6486427	394
84033	20787385	44	237546	90539594	250
86074	11438686	78	238474	9940366	402
95317	27189566	39	249026	101174274	250
100938	21638642	82	265301	51162438	439
101194	29820986	42	265554	135345358	70
107241	34813963	16	277818	49070002	478
120889	41889061	12	293458	145485622	222
137058	42877690	94	297309	155648414	157
137673	35277317	128	302241	150498103	244

Both (4) and (9) contain $C(181)$. Presumably, this is a coincidence; if it had some causal significance that would certainly be of interest! Also puzzling are the pairs with $c = c_1$ or $c = 2c_1$. See $c = 78, 16, 12, 54, 128, 402, 250$ in Table 2.

The class group of $Q((3D)^{1/2})$ is now $C(3) \times C(3) \times C(3) \times C(2)$. The elementary solutions of

$$a^3 = b^2 - c^2 3D$$

are

(10a) $\quad a = 6y, \qquad b = 54y^2 - 72y + 36, \qquad c = 6,$

(10b) $\quad a = 6y - 8, \qquad b = 54y^2 - 72y + 28, \qquad c = 6,$

for Series 3 but for $y = -235$ the ideal corresponding to (10a) is now principal. So for $D_3(-235)$ there are *two* additional ideals of order 3 that are independent of (10a, b) and each other. The ideal for (10b) is equivalent to a prime ideal of norm 37 and the two other generators can be taken as prime ideals of norm 23 and 71. We may therefore escalate our expectations and now expect cases with $s = 4$ and $r = 5$.

On a point of terminology that frequently causes confusion: When we wrote that the first case of $r = 2$ is $Q((-3299)^{1/2})$, we meant that 3299 is the minimal absolute value of the discriminant. As is known, $Q((-D)^{1/2})$ also has $r = 2$ for $D = 974$ and 2437, but here the discriminant is $-4D$, not $-D$. Of course, "first case" and "smallest" can equally well be defined to mean the smallest D, and some well-known books assert that $Q((-5)^{1/2})$ is the first case of nonunique factorization while others say that $Q((-15)^{1/2})$ is. By our choice, $Q((-D_6(169))^{1/2})$ is the "smaller" of our two cases of $r = 4$ even though (8) is smaller than (2b). That seems the preferred convention in this context; e.g., compare the values of a in Tables 1 and 2.

Finally, since it may be of interest, we record

$$D = D_3(449) = 1090678524545 = 5 \cdot 23 \cdot 83 \cdot 193 \cdot 592057. \tag{11}$$

Here, $Q((-D)^{1/2})$ has (only) $r = 3$ but the 2-Sylow subgroup has five factors in addition:

$$C(9) \times C(3) \times C(3) \times C(8) \times C(2) \times C(2) \times C(2) \times C(2) \times C(73).$$

3. The Class Field Towers. Golod and Šafarevič proved [6] that the class field tower of an algebraic field k is infinite if its class group requires sufficiently many generators. Such k therefore cannot be imbedded in a larger algebraic field, of finite degree, having unique factorization. Specifically, from Roquette's formula [7, Eq. (1), p. 233], it follows that an imaginary quadratic field does have an infinite tower if its 3-rank (our r above) exceeds 3. So $Q((-D)^{1/2})$ has such a tower for the D in (2b) and (8), the second case being especially noteworthy since its D is prime. The $Q((-D)^{1/2})$ for (11) has an infinite tower because of its 2-rank $= 5$ (see Roquette, p. 234), but whether its 3-rank $= 3$ would also suffice is apparently not now known.

Computation & Mathematics Department
Naval Ship Research & Development Center
Bethesda, Maryland 20034

1. A. Scholz, "Über die Beziehung der Klassenzahlen quadratischer Körper zueinander," *Crelle's J.*, v. 166, 1932, pp. 201–203.

2. A. Scholz & Olga Taussky, "Die Hauptideale der kubischen Klassenkörper imaginär quadratischer Zahlkörper: ihre rechnerische Bestimmung und ihr Einfluss auf den Klassenkörperturm," *Crelle's J.*, v. 171, 1934, pp. 19–41.

3. Daniel Shanks, "New types of quadratic fields having three invariants divisible by 3," *J. Number Theory*. (To appear.)

4. Maurice Craig, *Irregular Discriminants*, Dissertation, University of Michigan, Ann Arbor, Mich., 1972.

5. Daniel Shanks & Peter Weinberger, "A quadratic field of prime discriminant requiring three generators for its class group, and related theory," *Sierpiński Memorial Volume, Acta Arith.*, 1972, pp. 71–87.

6. E. S. Golod & I. R. Šafarevič, "On class field towers," *Izv. Akad. Nauk SSSR*, v. 28, 1964, pp. 261–272. (Russian)

7. Peter Roquette, "On class field towers," in *Algebraic Number Theory*, Thompson, Washington, D.C., 1967.