ONE-CLASS GENERA OF POSITIVE TERNARY QUADRATIC FORMS

G. L. WATSON

1. *Introduction.* We consider positive-definite ternary quadratic forms with integer coefficients. Such a form, f, can be written in matrix notation as

$$f(\mathbf{x}) = \tfrac{1}{2}\mathbf{x}' A\mathbf{x}, \quad A = A(f) = \begin{pmatrix} 2a_{11} & a_{12} & a_{13} \\ a_{21} & 2a_{22} & a_{23} \\ a_{31} & a_{32} & 2a_{33} \end{pmatrix}. \tag{1.1}$$

Here $\mathbf{x}'$ is the transpose of the column vector $\mathbf{x} = \{x_1, x_2, x_3\}$ and $a_{ij} = a_{ji}$ is the coefficient of $x_i x_j$ in f. Clearly $\det A$ is positive and even and so

$$d = d(f) = -\tfrac{1}{2}\det A(f) \tag{1.2}$$

is a negative integer.

The class of f is the set $\{g : g \sim f\}$ of forms g that are equivalent to f (over the integers, that is, by integral unimodular transformations). The genus of f is the set $\{g : g \simeq f\}$ of forms g that are semi-equivalent to f. Semi-equivalence ($\simeq$) may be defined in various ways. First, we shall define $f \simeq g$, for f as above and g ternary, with integer coefficients, to mean that (i) g is equivalent to f over the real field (that is, g is also positive-definite) and (ii) g is equivalent to f over the ring of p-adic integers, for every prime p.

If however we assume (ii) above then (i) follows [**1**; 72, Theorem 43] (the signatures of f, g cannot differ by a multiple of 8 without being equal), and $d(f) = d(g)$ also follows, trivially. It further follows [**1**; 68, Theorem 41] that there exists a form h which is equivalent to f and congruent to g modulo $d(f)$, identically in the variables. Conversely, if $d(f) = d(g)$ and there exists h as above, then for every prime p we have $f \sim_p g$, $\sim_p$ denoting equivalence over the p-adic integers [**1**; 56, Theorem 33] and $f \simeq g$ follows.

Clearly every genus is a union of classes; and we denote by $c(f)$ the class-number of f, that is, the number of classes in the genus of f. It is well known that $c(f) < \infty$ for all f, so $c(f)$ is a positive integer, invariant under $\simeq$. We shall be interested in the f with $c(f) = 1$. It is known, see Lemma 6 below, that, if $c(f) = 1$, then f represents all positive integers not excluded by congruence considerations. This property, besides being of interest in itself, will be used as a means of finding the one-class genera. As such, it can be made more effective by restricting $d(f)$ to be square-free. After this case has been dealt with the general case, with $\mathrm{d}(f)$ unrestricted, becomes less difficult; and a similar two-part argument can be used to find all the positive n-ary one-class genera with $n \geqslant 4$. This will be explained briefly after we have proved:

THEOREM 1. *Let f be a positive-definite ternary quadratic form with integer coefficients and square-free discriminant. Then the class-number of f is 1 if and only if f is equivalent to one of the forms $f_1, \ldots, f_{20}$ listed in the table below.*

TABLE I

	Coefficients of f_i		
i	a_{11}, a_{12}, a_{13}	a_{13}, a_{23}, a_{33}	$d(f_i)$
1–6	1, 1, 1	0, 1, 1 0, 0, 1 0, 1, 2 0, 0, 2 0, 1, 5 0, 0, 10	−2 −3 −5 −6 −14 −30
7–11	1, 0, 1	1, 1, 2 0, 1, 2 1, 1, 3 0, 1, 4 1, 1, 11	−6 −7 −10 −15 −42
12–14	1, 1, 2	0, 2, 2 0, 1; 2 0, 4, 7	−10 −13 −33
15–17	1, 0, 2	1, 1, 3 1, 0, 3 1, 0, 9	−21 −22 −70
18, 19	1, 1, 3	0, 5, 5 0, 3, 5	−30 −46
20	1, 1, 5	0, 6, 6	−78

The related problem (see Lemma 6 below) of finding ternary positive forms representing all integers not excluded by congruence considerations has been studied in [**4**] and in my Ph.D. thesis (1953). There I obtained results (in which the foregoing forms $f_1, \ldots, f_{20}$ occurred) which were too complicated and incomplete for publication.

2. *Reduction.* It will be convenient to write

$$F = F(x_1, x_2) = f(x_1, x_2, 0) = a_{11}x_1{}^2 + a_{12}x_1x_2 + a_{22}x_2{}^2, \tag{2.1}$$

$$D = D(f) = d(F) = a_{12}{}^2 - 4a_{11}a_{22}, \tag{2.2}$$

whence obviously $D < 0$, $D \equiv 0$ or $1 \pmod 4$. For any positive integer a, $f \supset a$ (f represents a properly) means that there exist integers x_i satisfying

$$f(x_1, x_2, x_3) = a, \qquad \text{g.c.d.}(x_1, x_2, x_3) = 1. \tag{2.3}$$

As usual, $\min f$ means $\inf\{a : f \supset a\}$. $F \supset a$ is defined in the same way as $f \supset a$, and clearly $\min F \geqslant \min f$. We prove:

LEMMA 1. *By a suitable integral unimodular substitution, the f of Theorem 1 may be supposed to satisfy*

$$a_{11} = \min f = \min F, \qquad 0 \leqslant a_{12} \leqslant a_{11}, \tag{2.4}$$

and

$$|D(f)| = \inf\{|D(g)| : g \sim f,\ \min g = a_{11}\}. \tag{2.5}$$

These conditions imply

$$2a_{11}{}^3 \leqslant |d|, \quad 3a_{11}{}^2 \leqslant |D|, \quad \textit{and} \quad 3D^2 \leqslant 16a_{11}|d|. \tag{2.6}$$

Proof. It is trivial that we may assume (2.4), (2.5). For the first two of (2.6), we use well known inequalities [**1**; 28–9, Theorem 17 and 14; Theorem 7] for the minima of f, F. Now we write f as

$$a_{11}(x_1 + r_2 x_2 + r_3 x_3)^2 + \psi(x_2, x_3),$$

where r_2, r_3 and the coefficients of ψ are rational, and we may clearly suppose $\min\psi = \psi(1, 0)$, giving $D = -4a_{11}\psi(1, 0) = -4a_{11}\min\psi$; and clearly

$$d(f) = a_{11}d(\psi), \quad 3(\min\psi)^2 \leqslant |d(\psi)|,$$

giving the last of (2.6), and completing the proof.

By expressing f as

$$F(x_1 + u_1 x_3,\ x_2 + u_2 x_3) + D^{-1}dx_3^2,$$

with rational u_1, u_2, we see that

$$f \supset a \quad \text{and} \quad F \not\supset a \quad \text{imply} \quad |d| \leqslant a|D|. \tag{2.7}$$

For the hypotheses of (2.7) imply that (2.3) has a solution with $|x_3| \geqslant 1$, which cannot be unless $D^{-1}d \leqslant a$.

Further normalization of f is needed only in special cases:

LEMMA 2. *Suppose $a_{11} = 1$, $a_{12} = 0$ or 1, and $D = -4, -8$, or $-p$, p a prime $\equiv 3 \pmod 4$. Then we must have*

$$d \not\equiv -1 \pmod 4),\ d \not\equiv -1, -3 \pmod 8, \quad \text{or} \quad (d\,|\,p) \neq -1 \tag{2.8}$$

(Legendre symbol). Conversely, if a_{11}, a_{12}, D as above are given, and also d satisfying (2.8), then there is just one possibility for f up to equivalence.

Proof. For suitable integers h, k we use the substitution

$$x_1 \to x_1 + hx_3, \quad x_2 \to x_2 + kx_3. \tag{2.9}$$

We may also, if necessary, put $-x_3$ for x_3; and if $D = -4$, $F = x_1^2 + x_2^2$, we may interchange x_1, x_2, and a_{13}, a_{23}.

Now if $D = -4$ we may suppose $0 \leqslant a_{13} \leqslant a_{23} \leqslant 1$, whence both assertions follow from (1.2), which reduces to $d = a_{13}^2 + a_{23}^2 - 4a_{33}$. If $D = -8$, we suppose $0 \leqslant a_{13} \leqslant 1$, $0 \leqslant a_{23} \leqslant 2$, and (1.2) reduces to $d = 2a_{13}^2 + a_{23}^2 - 8a_{33}$. This is easily seen to be impossible if $d \equiv -1$ or $-3 \pmod 8$, and otherwise to determine a_{13}, a_{23}, a_{33} uniquely when d is given.

In the remaining case $D = -p$, $a_{12} = 1$, $a_{22} = \frac{1}{4}(p+1)$, (2.9) replaces a_{13} by $a_{13} + 2h + k$, whence we may clearly suppose $a_{13} = 0$. Then, putting $k = -2h$, we may replace $a_{13} = 0$, a_{23} by 0, $a_{23} - ph$. So we may suppose $0 \leqslant a_{23} < \frac{1}{2}p$. Then (1.2) reduces to $d = a_{23}^2 - pa_{33}$, whence $(d\,|\,p) = -1$ is impossible and in other cases d determines a_{23}, a_{33}.

3. *p-adic properties of f.* With the notation of (2.1), (2.2), define $(D\,|\,2)$ to be 0 if $2\,|\,D$ and otherwise 1, -1 for $D \equiv 1, -3 \pmod 8$; whence (even for $p = 2$), $(D\,|\,p)$ is unaltered by reducing the coefficients of F modulo p. For any prime p, and any integer a, $f \supset_p a$ (in words, f represents a properly over the p-adic integers) may be defined to mean that, for every positive integer t, there exist integers x_i such that

$$f(x_1, x_2, x_3) \equiv a \pmod{p^t} \quad \text{and} \quad p \nmid \text{g.c.d.}(x_1, x_2, x_3). \tag{3.1}$$

$F \supset_p a$ is defined in the same way; and we also define

$$\varepsilon_p(f) = 1 \quad \text{if} \quad f \underset{p}{\supset} 0, \quad -1 \text{ if not.} \tag{3.2}$$

We prove first:

LEMMA 3. *If $p \nmid aD$, or if $(D\,|\,p) = 1$, then $F \supset_p a$. If $(D\,|\,p) = -1$, then (for integers x_1, x_2), $F(x_1, x_2) \equiv 0 \pmod p$ implies $x_1, x_2 \equiv 0, 0 \pmod p$.*

Proof. With $p \nmid D$, the partial derivatives of F are $\equiv 0, 0 \pmod p$ if and only if $x_1, x_2 \equiv 0, 0 \pmod p$. So the first assertion is easily deduced from Hensel's Lemma, since it is elementary that $F \equiv a \pmod p$ is soluble, and that $x_1, x_2 \equiv 0, 0 \pmod p$ is not the only solution, for $p\,|\,a$, if $(D\,|\,p) = 1$. The second assertion is trivial.

We next prove:

LEMMA 4. *For ternary f with integer coefficients and $p^2 \nmid d(f)$, p any prime, we may suppose without loss of generality that (identically in the x_i)*

$$f(x_1, x_2, x_3) \equiv F(x_1, x_2) + a_{33}x_3^2 \pmod{p^4} \tag{3.3}$$

and

$$p \nmid D, \quad d \equiv Da_{33} \pmod{p^4}. \tag{3.4}$$

Then $f \supset_p a$ holds for all a unless

$$(D\,|\,p) = -1 \quad \text{and} \quad p\,|\,a_{33}. \tag{3.5}$$

In case (3.5), $f \supset_p a$ is false if and only if $p\,|\,a$ and either $p^2\,|\,a$ or

$$(p^{-1}a\,|\,p) = (p^{-1}d\,|\,p), \tag{3.6}$$

the latter condition meaning $a \equiv d \pmod{16}$ if $p = 2$.

Proof. It is clear from $p^2 \nmid d$ that the assumption $p \nmid D$ involves no loss of generality. With it, we have (3.3), and so the second of (3.4), by a substitution of the shape (2.9).

Now by using Lemma 3, as it stands and with $a - a_{33}$ for a, after putting $x_3 = 0$ or 1, we see at once that $f \supset_p a$ fails only if (3.5) holds and $p\,|\,a$. Assuming (3.5) and $p\,|\,a$, the last part of Lemma 3, with $p\,|\,a_{33}$ but $p^2 \nmid a_{33}$ by (3.4) and $p^2 \nmid d$, shows that $f \equiv 0 \pmod{p^2}$ implies $x_1, x_2, x_3 \equiv 0, 0, 0 \pmod p$; so $f \supset_p a$ is false if $p^2\,|\,a$.

Supposing therefore, further, that $p^2 \nmid a$, it is trivially sufficient to take $t = 4$ in (3.1). With $x_1, x_2 \equiv 0, 0 \pmod p$ by the second part of Lemma 3, (3.1) may now be written (with integers $y_1, y_2 = p^{-1}x_1, p^{-1}x_2$) as

$$pF(y_1, y_2) + p^{-1}a_{33}x_3^2 \equiv p^{-1}a \pmod{p^3}, \quad p \nmid x_3. \tag{3.7}$$

If $p > 2$, then (3.7) is insoluble if and only if

$$\begin{aligned}(p^{-1}a\,|\,p) &= -(p^{-1}a_{33}\,|\,p),\\ &= (p^{-1}d\,|\,p)\end{aligned}$$

by (3.4). If $p = 2$, then F in (3.7) can be 0 or ± 1, but not 2, modulo 4, by Lemma 3. So (3.7) is insoluble if and only if

$$\tfrac{1}{2}a \equiv \tfrac{1}{2}a_{33} + 2 \equiv \tfrac{1}{2}Dd + 2 \equiv -\tfrac{1}{2}d + 2 \equiv \tfrac{1}{2}d \pmod 8,$$

which completes the proof. Obvious corollaries are:

$$p \nmid d \quad \text{implies} \quad \varepsilon_p(f) = 1, \tag{3.8}$$

$$f \underset{p}{\supset} a \quad \text{and} \quad p^2 \mid a \quad \text{imply} \quad \varepsilon_p(f) = 1, \tag{3.9}$$

and

$$p \mid d \quad \text{and} \quad p \nmid D \quad \text{imply} \quad \varepsilon_p(f) = (D \mid p). \tag{3.10}$$

We next prove:

LEMMA 5. *For f as in Theorem* 1 *and g satisfying the same conditions we have $f \simeq g$ if and only if $d(f) = d(g)$ and $\varepsilon_p(f) = \varepsilon_p(g)$ for every $p \mid d(f)$.*

Proof. Suppose first that $f \simeq g$. Then as noted in §1 we must have $d(f) = d(g)$, $= d$, say, and we may suppose without loss of generality that $g \equiv f \pmod d$. Then (3.8), (3.10) give $\varepsilon_p(f) = \varepsilon_p(g)$ for all p (each 1 if $p \nmid d$).

To prove the "if", we note first that if $p \nmid d$ we necessarily have

$$f \underset{p}{\sim} g \underset{p}{\sim} x_1 x_2 + d x_3^2$$

[1; 51, Theorem 29]. For $p \mid d$, it suffices to show that there are just two possibilities for f under $\sim_p$, and that these have different $\varepsilon_p(f)$, whence $\varepsilon_p(f) = \varepsilon_p(g)$ gives $f \sim_p g$. One of these possibilities is $f \sim_p x_1 x_2 + d x_3^2$ (which follows easily from (3.5) if $(D \mid p) = 1$). To see that there is only one other is straightforward, but see [1; 54, Theorem 32 and 59, Theorem 35].

4. *Theorem* 1, *proof of sufficiency.* We have to prove that if $f \simeq f_i$, for one of the twenty f_i of the theorem, then $f \sim f_i$, giving $c(f_i) = 1$. Assuming $f \simeq f_i$, Lemma 5 gives

$$d = d(f) = d(f_i) \quad \text{and} \quad \varepsilon_p(f) = \varepsilon_p(f_i) \quad \text{for every } p \mid d. \tag{4.1}$$

By Lemma 1, we may also assume (2.4)–(2.6).

Since the table shows that $\min f_i = 1$ in all twenty cases, the first step is to show that $\min f = a_{11} = 1$. The second step is to show that $D(f) = -3, -4, -7, -8, -11$, or -19, in the cases $i = 1$–6, 7–11, 12–14, 15–17, 18–19, 20 respectively; whence trivially $F = f_i(x_1, x_2, 0)$. Then the third step, $f \sim f_i$, is trivial by Lemma 2.

We use (2.6) to find a finite number of possibilities for the pair a_{11}, D; and then use Lemma 4 and (3.9), (3.10) to show that all but one of these contradict (4.1), or possibly (2.5). For example, if we assume $a_{11} > 2$ we have $a_{11} = 3$ in cases $i = 17, 20$, $d = -70, -78$, and a contradiction otherwise. Then if $d = -78$ we have $\varepsilon_3(f) = -1$ by (4.1), $d \equiv 3 \pmod 9$, and $f \supset_3 3$ false by Lemma 4; contradiction. If $d = -70$, we find by (2.6) that $D = -27, -28, -31$, or -32. But $a_{11} = 3$ is clearly inconsistent with $D = -28$ or $-31 \equiv -1 \pmod 3$. $D = -32$ gives $F = 3x_1^2 + 2x_1 x_2 + 3x_2^2 \supset 4$, whence $f \supset 4$. Then (3.9) gives

$$\varepsilon_2(f) = 1 \neq \varepsilon_2(f_{17}).$$

So $D = -27$, but this by (3.1) gives $\varepsilon_7(f) = 1 \neq \varepsilon_7(f_{17})$. So $a_{11} \leqslant 2$; and equality can be excluded by similar arguments. Then with $a_{11} = 1$ we exclude all possibilities but one for D; I leave the details to the reader.

5. *Theorem* 1, *proof of necessity; possibilities for F.* We need:

LEMMA 6. *Let f be as in Theorem* 1, *with $c(f) = 1$, and let a be any positive integer. Then, see* (2.3), (3.1), *$f \supset a$ if and only if $f \supset_p a$ for every prime p.*

Proof. Since any solution of (2.3) necessarily satisfies (3.1) for all p, t, the "only if" is trivial. Suppose therefore that (3.1) is soluble for all p, t. Then $g \supset a$ for some g in the genus of f, as is well known, see [1; 80, Theorem 51]. That is, for some $g \simeq f$ (2.3) is soluble with g in place of f. But now using $c(f) = 1$, $g \simeq f$ implies $g \sim f$; whence clearly (2.3) is soluble as it is, and the lemma is proved.

Now assuming $d(f)$ square-free and $c(f) = 1$, we may also, by Lemma 1, assume (2.4)–(2.6), and we have to prove f equivalent to one of the f_i. The first step is to show that $a_{11} = 1$. Since Lemma 4 gives $f \supset_p 1$ for every p, $f \supset 1$ follows by Lemma 6, so $a_{11} = 1$ by (2.4), and $a_{12} = 0$ or 1, $\equiv D \pmod 2$.

The second step is to show that $D = -3, -4, -7, -8, -11$, or -19. We note that (2.5), with a_{11}, a_{12} as above, gives

$$a_{22} \leqslant \inf\{a : a > 1, \ f \supset a\} \tag{5.1}$$

(with equality unless $a_{22} = 1$). We have also

$$f \supset 2, \ 3, \text{ or } 6. \tag{5.2}$$

For if $f \not\supset 2$, then Lemma 6 gives $f \not\supset_p 2$ for some p, and Lemma 4 gives $p = 2$ and $d \equiv 2 \pmod{16}$. Similarly, if $f \supset 3$, then $d \equiv 3 \pmod 9$; and if $f \supset 6$, then either $f \supset_2 6$ is false, giving the contradiction $d \equiv 6 \pmod{16}$, or $f \supset_3 6$ is false, giving $d \equiv 6 \pmod 9$. So (5.2) is proved.

From (5.1), (5.2) we have $a_{22} \leqslant 6$, and $D = -4a_{22}$ or $1 - 4a_{22}$ satisfies $|D| \leqslant 24$. This gives twelve possibilities for D, F, six of which we have to exclude.

If $D = -24$, then $\varepsilon_5(f) = 1$ by (3.8), (3.10), and the argument used for (5.2) gives $f \supset_5 5$ by Lemma 4, $f \supset 5$, $a_{22} \leqslant 5$, giving the contradiction $|D| \leqslant 20$. Similarly, if $D = -20$, $a_{22} = 5$, we find $f \supset 3$, contradicting (5.1).

If $D = -15$ or -23, then $\varepsilon_2(f) = 1$ by (3.8), (3.10), $f \supset_2 2$ by Lemma 4 (and $f \supset_p 2$ is trivial for $p > 2$), so Lemma 6 gives $f \supset 2$, contradicting (5.1). In the remaining cases $D = -12, -16$, $F = x_1^2 + 3x_2^2$ or $x_1^2 + 4x_2^2 \supset 4$, $f \supset 4$. Then (3.9) gives $\varepsilon_2(f) = 1$, and we argue as for $D = -15, -23$.

6. *Theorem* 1; *completion of proof.* The third and final step in the proof of the "only if" is to find all the possibilities for f up to equivalence, for each of the six possibilities for D, F found in §5. But in each case, by Lemma 2, it suffices to find the possibilities for d.

For each of the six D, $= -3, -4, -7, -8, -11, -19$, we shall choose primes p, q such that

$$(D \mid p) = -1, \quad (D \mid q) = 1, \quad (q \mid p) = -1, \tag{6.1}$$

the last of these conditions meaning $q \not\equiv 1 \pmod 8$ if $p = 2$. From $(6.1)_1$ and the last part of Lemma 3, it follows that $F \not\supset p$ and $F \not\supset pq$. From Lemma 4 and $(6.1)_2$ we see easily that $f \supset_r p$ and $f \supset_r pq$ are both true for every prime $r \neq p$, and $(6.1)_3$ shows that one of them, at least, holds for $r = p$. So, using Lemma 6, (6.1) implies $f \supset p$ or pq, $f \supset p$ unless $p \mid d$ and $(p^{-1} d \mid p) = 1$. Then (2.7) shows that (6.1) implies

$$|d| \leqslant \begin{cases} pq|D| & \text{always} \\ p|D| & \text{unless} \quad p \mid d \quad \text{and} \quad (p^{-1} d \mid p) = 1, \end{cases} \tag{6.2}$$

the latter condition meaning $d \equiv 2 \pmod{16}$ if $p = 2$.

We note that some values of d below the bound of (6.2) may be excluded by using other cases of (2.7), or by Lemma 2. Further, we note that since $c(f) = 1$ is assumed, $g \simeq f$ implies $g \sim f$ and so (2.5) may be replaced by

$$|D(f)| = \inf\{|D(g)| : g \simeq f,\ g(1, 0, 0) = 1\}. \tag{6.3}$$

Using the foregoing arguments we dispose of the six cases one by one.

(i) $D = -3$, $F = x_1^2 + x_1 x_2 + x_2^2$.

With $p = 2$, $q = 7$ in (6.1), (6.2) we find $|d| \leqslant 42$ and either $|d| \leqslant 6$ or $d \equiv 2 \pmod{16}$. Lemma 2 gives $(d \mid 3) = 0$ or 1, so $d = -2, -3, -5, -6, -14$ or -30. These six numbers being $d(f_1), \ldots, d(f_6)$, $f \sim$ one of $f_1, \ldots, f_6$ follows as noted at the beginning of this section.

(ii) $D = -4$, $F = x_1^2 + x_2^2$.

With $p = 3, q = 5$, (6.1) holds and (6.2) gives $|d| \leqslant 60$ in all cases, improving to $|d| \leqslant 12$ unless $d \equiv 3 \pmod 9$. Lemma 2 gives $d \equiv 1$ or $2 \pmod 4$, since d is square-free. Obviously, by Lemmas 4, 6, $f \supset 7$ unless $7 \mid d$, so since $F \not\supset 7$ we have either $|d| \leqslant 28$ or $7 \mid d$, by (2.7).

This leaves us eight possibilities for d, five of which are the ones we want, see the table, the other three being -2, -3, -11. In each of these three cases Lemma 2 shows that we can construct g with $g(x_1, x_2, 0) = x_1^2 + x_1 x_2 + x_2^2$; and Lemma 5 shows easily that $g \simeq f$ (we have $g \sim f$ by permuting the variables in the first two cases). So the three unwanted cases are all excluded.

(iii) $D = -7$, $F = x_1^2 + x_1 x_2 + 2x_2^2$.

(6.1) holds with p, $q = 3$, 2, so (6.2) gives $|d| \leqslant 42$ and either $|d| \leqslant 21$ or $d \equiv 3 \pmod 9$. $a = 5$ in (2.7) is easily seen to exclude $d = -42$. Lemma 2 gives $(d \mid 7) = 0$ or 1, and we can use $(2.6)_3$ to give $|d| \geqslant 10$. Using Lemmas 2, 5 as in (ii) we exclude $d = -14$, -17, -21; and similarly, but with $D(g) = -4$, we exclude $d = -19$. The surviving possibilities for d are just the three we want, namely -10, -13, -33.

(iv) $D = -8$, $F = x_1^2 + 2x_2^2$.

We take $p, q = 5$, 3 in (6.1), and (6.2) gives either $|d| \leqslant 40$ or $d = -55$, -70, -95, or -105. We note however that $F \not\supset 4$, whereas $f \supset 4$ is clear from Lemmas 4, 6 if d is odd. So using (2.7) with $a = 4$, we find either $|d| \leqslant 40$ or $d = -70$; and since $-70 = d(f_{17})$ we may suppose $|d| \leqslant 40$, and $2 \mid d$ if $|d| > 32$. We have $|d| \geqslant 12$ by $(2.6)_3$, and $|d| \equiv 2, 5, 6$, or $7 \pmod 8$ by Lemma 2.

It is now easily verified that Lemmas 2, 5 give a contradiction with (6.3) with $D(g) = -3$ in cases $d = -15$, -23, -29, -38, $D(g) = -4$ for $d = -14$, -31, -34, $D(g) = -7$ for $d = -13$, -26. This leaves only the cases $d = -21 = d(f_{15})$, $-22 = d(f_{16})$, and $d = -30$, which must be excluded.

We construct the form

$$g = 2x_1^2 + x_1 x_2 + 3x_2^2 + 2x_1 x_3 + 2x_2 x_3 + 2x_3^2,$$

with $d(g) = -30$ and $D(g) = -23$, whence it is easily seen that with $d(f) = -30$ and $D(f) = -8$ we have $f \simeq g$, and so, with $c(f) = 1$, $f \sim g$. Now (2.7) with 1, g for a, f give the contradiction $|d| \leqslant 23 < 30$.

(v) $D = -11$, $F = x_1^2 + x_1 x_2 + 3x_2^2$.

From (6.1) with p, $q = 2$, 3, and (6.2), we have $|d| \leqslant 66$. (5.1) gives $f \not\supset 2$, $d \equiv 2 \pmod{16}$, and Lemma 2 gives $(d \mid 11) = 0$ or 1, so $d = -30$, -46, or -62. $d = -62$ can be excluded by (6.3), with $D(g) = -3$. So $d = -30$ or $-46 = d(f_{18})$ or $d(f_{19})$.

(vi) $D = -19$, $F = x_1^2 + x_1 x_2 + 5x_2^2$.

Here (5.1) gives $f \not\supset 2$, 3 so $d \equiv 2 \pmod{16}$, $3 \pmod 9$, $-78 \pmod{144}$. (5.2) gives $f \supset 6$, so with $F \not\supset 6$ (2.7) gives $|d| \leqslant 114$, so $d = -78 = d(f_{20})$, and this completes the proof of Theorem 1.

7. *Ternary forms with d not square-free.* Let the ternary form f have integer coefficients and $d \neq 0$; and suppose f primitive. For any prime p, there are two possibilities: (i), p does, (ii), does not, divide all the elements of the matrix adj $A(f)$ [in case $p = 2$, this is equivalent to p does, does not, divide all three of a_{12}, a_{13}, a_{23}].

In case (i), we must have $p^2 \mid d$, and may clearly suppose, by an integral unimodular transformation, that (identically in the x_i)

$$f \equiv a_{11} x_1^2 \pmod p, \quad p \nmid a_{11}. \tag{7.1}$$

In case (ii), we may suppose $p \nmid D$, and then, as in Lemma 4, that (3.3) holds, whence if $p^2 \mid d$ we have

$$f \equiv F \pmod{p^2}, \quad p \nmid D. \tag{7.2}$$

In case (7.1), define

$$g = g(x_1, x_2, x_3) = p^{-1} f(px_1, x_2, x_3). \tag{7.3}$$

In case (7.2), define

$$g = g(x_1, x_2, x_3) = p^{-2} f(px_1, px_2, x_3). \tag{7.4}$$

In each of these cases, note that g has integer coefficients and that $d(g) = p^{-1} d(f)$ or $p^{-2} d(f)$ satisfies

$$|d(g)| < |d(f)|. \tag{7.5}$$

Taking $n = 3$ and $m = p$ in [2; 579, Theorem 1], we also have

$$c(g) \leqslant c(f). \tag{7.6}$$

(See also §8, below, for some notation used in [2].)

Looking at (7.5), (7.6), we see that by repeating the argument, with suitable choice of p at each step, we have always

$$c(f) \geqslant c(f_0), \quad \text{with} \quad d(f_0) \quad \text{square-free,} \tag{7.7}$$

and f equivalent over the rationals to a multiple of f_0. Supposing f positive, Theorem 1 and (7.7) give $c(f) > 1$ unless

$$f_0 \sim \text{one of } f_1, \ldots, f_{20}. \tag{7.8}$$

Now I could prove:

THEOREM 2. *There are just 787 possibilities up to equivalence for a positive-definite ternary quadratic form f, primitive and with integer coefficients, which has class-number* 1.

To prove Theorem 2, one has to examine the cases of equality in (7.6); unfortunately these are rather numerous. There are however certain simplifications. First, we need only consider cases in which repetition of the argument leading to (7.6) leads to the case (7.7), (7.8). Further, in going back from f_0 to f, if strict inequality holds in (7.6) at a late step, one need not consider earlier steps. So, for most of the argument, one is concerned with f such that $p^2 \mid d$ for only one prime p, and which does not behave too badly even for that p. Then the arguments used for Theorem 1 need only small modifications. I am still trying to simplify the arguments, and also to present the result more concisely, so as to avoid listing all the 787 possibilities individually.

8. *One-class n-ary, positive-definite, genera with* $n \neq 3$. The case $n = 1$ is trivial, and $n \geqslant 11$ has been dealt with in [3] (the class-number is always $\geqslant 2$). The case $n = 2$ is very difficult, and I have not been able to deal with it. So in what follows $4 \leqslant n \leqslant 10$ is assumed; and $d = d(f)$ is defined as in (1.2), but with the factor $-\frac{1}{2}$ replaced by $(-1)^{\frac{1}{2}n}$ if $2 \mid n$, $\frac{1}{2}(-1)^{\frac{1}{2}n-\frac{1}{2}}$ if $2 \nmid n$. Suppose also f primitive and $p \mid d$. We outline some notation and results of [2].

We transform a given form f into an equivalent form of the shape

$$f^{(0)}(x_1, \ldots, x_r) + p\sum\{b_{ij}x_ix_j : 1 \leqslant i \leqslant r < j \leqslant n\} + pf^{(1)}(x_{r+1}, \ldots, x_n), \qquad (8.1)$$

where $f^{(0)}, f^{(1)}$ are forms with integer coefficients, the b_{ij} are integers, and $r = r_p(f)$ is as small as possible. This last condition is equivalent to $p \nmid d(f^{(0)})$.

Now we say that f is strongly primitive (SP) if $r_p(f) \geqslant \frac{1}{2}n$ for every p. f is p-adically square-free if, and only if, f is equivalent to a form of the shape (8.1) with r minimal, i.e. $= r_p(f)$, and also $r_p(f^{(1)}) = n - r$, that is, with $p \nmid d(f^{(1)})$. Finally, f is square-free (SF) if it is p-adically square-free for every p.

Now for each n from 4 to 10 I have proved an analogue of Theorem 1, with the assumption that f is SF and SP in place of d square-free (the two assumptions are easily seen to be equivalent when $n = 3$). These results involve just 67 classes. I have so far worked out the analogue of Theorem 2 only for $n = 9$, 10.

References

1. G. L. Watson, *Integral quadratic forms* (Cambridge Tract No. 51 (Cambridge, 1960).
2. ———, " Transformations of a quadratic form which do not increase the class-number ", *Proc. London Math. Soc.* (3), 12 (1962), 577–587.
3. ———, " The class-number of a positive quadratic form ", *Proc. London Math. Soc.* (3), 13 (1963), 549–576.
4. Gordon Pall and Burton W. Jones, " Regular and semi-regular positive ternary quadratic forms ", *Acta Mathematica*, 70 (1939), 165–191.

University College,
London.

10C05: *Number theory; Quadratic forms.*

(*Received on the* 13*th of April*, 1972)

CLASS GROUPS FOR INTEGRAL REPRESENTATIONS OF METACYCLIC GROUPS

S. GALOVICH, I. REINER AND S. ULLOM

1. *Introduction.* Let R be a Dedekind domain whose quotient field K is an algebraic number field, and let Λ be an R-order in a semisimple K-algebra A with 1. A Λ-*lattice* is a finitely generated R-torsionfree left Λ-module. We shall call a Λ-lattice M *locally free of rank n* if for each maximal ideal $\mathfrak{p}$ of R, $M_\mathfrak{p}$ is $\Lambda_\mathfrak{p}$-free on n generators. (The subscript $\mathfrak{p}$ denotes localization.) The (locally free) *class group* of Λ is the additive group $C(\Lambda)$ generated by symbols

$$x_M = [\Lambda] - [M], \quad M = \text{locally free rank 1 } \Lambda\text{-lattice},$$

where

$$x_{M_1} + x_{M_2} = x_{M_3} \quad \text{whenever } M_1 \dotplus M_2 \cong \Lambda \dotplus M_3,$$

and where $x_M = 0$ if and only if M is stably free (that is, $M \dotplus \Lambda^{(k)} \cong \Lambda \dotplus \Lambda^{(k)}$ for some k).

Let ZG be the integral group ring of a finite group G. A number of recent articles have been devoted to the calculation of the class group $C(ZG)$ for various groups G (see Fröhlich [1], Kervaire and Murthy [3], Martinet [5], Reiner and Ullom [7, 8], and Ullom [11]). For the most part, it is only in rare cases that the order $|C(ZG)|$ can be computed explicitly. In such cases, the formula for $|C(ZG)|$ usually involves the ideal class numbers of certain cyclotomic fields, and makes use of detailed information about units in integral group rings.

The purpose of this note is to compute $C(ZG)$ for the case where G is a metacyclic group of order pq. Let

$$(1.1) \qquad G = \langle x, y : x^p = 1, y^q = 1, yxy^{-1} = x^r\rangle,$$

where p is an odd prime, q is any divisor of $p-1$, and r is a primitive q-th root of 1 mod p. Let ω be a primitive p-th root of 1 over Q, and set $K = Q(\omega)$, $R = Z[\omega]$; thus $R = \text{alg. int.}\{K\}$, the ring of all algebraic integers in K. Let L be the unique subfield of K such that $(K: L) = q$, and put $S = \text{alg. int. }\{L\}$. Denote by $C(S)$ the ideal class group of S. Let $H = \langle y\rangle$, a cyclic group of order q.

Our main result is

(1.2) THEOREM. *There is an epimorphism*

$$C(ZG) \to C(S) \dotplus C(ZH),$$

whose kernel $D_0(ZG)$ *is a finite cyclic group of order* q, q *odd, and of order* $q/2$, q *even.*

The case where $q = 2$ is already known (see Lee [4], Reiner and Ullom [7, 8]). It is rather surprising that such an explicit formula can be obtained, especially since as yet there is no analogous result for the seemingly simpler case of a cyclic group of order pq, with p, q distinct primes. When q is prime, we know from Rim [9] or Reiner [6] that $C(ZH) \cong C(R')$, where $R' = \text{alg. int.}\{K'\}$, and $K' = Q(\sqrt[q]{1})$. For

The last two named authors were partially supported by a contract with the National Science Foundation.

[MATHEMATIKA 19 (1972), 105–111]