ACTA ARITHMETICA
XXVII (1975)

Transformations of a quadratic form which do not increase the class-number (II)

by

G. L. WATSON (London)

In memory of Yu. V. Linnik

1. Introduction and notation. Let f be a quadratic form with integer coefficients, in any number n of variables. Then by $c(f)$, the class-number of f, is meant the number of classes in the genus of f. I showed in [1] that under certain transformations the class-number does not increase. The results of [1], which were used in [2] to show that $c(f) > 1$ for every positive-definite f with $n \geqslant 11$, will here be improved, so as to make possible some further applications explained in §§ 8, 11 below.

The transformations will be defined in a slightly different way, so that we shall have two alternative ways of dealing with the prime number 2. The effect of the transformations on the arithmetic properties of the form, and the cases in which they leave the class-number unaltered, will be investigated more fully than in [1]. The present paper is independent of [1].

Italic letters, with or without accents and subscripts, denote integers, p always prime, except f, g, h, used for quadratic forms (always with integer coefficients). Latin capitals, except F, G, also used for quadratic forms, denote square matrices, I being an identity matrix. Small Latin letter in bold type denote column vectors, with integer elements. An accent is used to denote transposition of a matrix or vector. Λ_n is the standard lattice in n-space, and its points are regarded as column vectors; its origin is $\mathbf{0} = \mathrm{col}\{0, \ldots, 0\}$. $M\Lambda_n$ is the sub-lattice $\{M\boldsymbol{x}: \boldsymbol{x} \in \Lambda_n\}$ and $m\Lambda_n$ $(m \neq 0)$ means $(mI)\Lambda_n$.

The matrix $A(f)$, $= A'(f)$, of the quadratic form f is defined so that we have the identities

$$f(\boldsymbol{x}+\boldsymbol{y}) = f(\boldsymbol{x}) + \boldsymbol{x}'A(f)\boldsymbol{y} + f(\boldsymbol{y}), \quad f(\boldsymbol{x}) = \tfrac{1}{2}\boldsymbol{x}'A(f)\boldsymbol{x}. \tag{1.1}$$

The discriminant $d = d(f)$ is defined by

$$d(f) = \begin{cases} (-1)^{\frac{1}{2}n}\det A(f) & \text{if} \quad 2 \mid n, \\ \frac{1}{2}(-1)^{\frac{1}{2}n-\frac{1}{2}}\det A(f) & \text{if} \quad 2 \nmid n. \end{cases} \tag{1.2}$$

It is easily seen that $A'(f) \equiv -A(f) \pmod 2$, giving $\det A(f) \equiv 0 \pmod 2$ if $2 \nmid n$, so d is always an integer. We suppose always $d(f) \neq 0$; that is, f non-singular.

The symbols $\sim, \underset{\infty}{\sim}, \underset{p}{\sim}$ denote equivalence over the rational integers, the real field, and the p-adic integers respectively; and $f \simeq f'$ means $f \underset{\infty}{\sim} f'$ and $f \underset{p}{\sim} f'$ for every prime p. So the class and genus of f are the sets $\{f' : f \sim f'\}$ and $\{f' : f \simeq f'\}$, respectively.

All quadratic equations occurring in the paper are identities.

Now let $\mathscr{R}$ be a binary relation between quadratic forms. We notice first that if

$$(1.3) \qquad f \mathscr{R} g \quad \text{and} \quad \left.\begin{matrix} f \sim f' \\ g \sim g' \\ f \mathscr{R} g' \end{matrix}\right\} \Rightarrow \text{resp.} \left.\begin{matrix} f' \mathscr{R} g \\ f \mathscr{R} g' \\ g \sim g' \end{matrix}\right.$$

then $\mathscr{R}$ defines, in an obvious way, a mapping from classes to classes. This mapping may or may not be 1-1. We shall express it loosely by writing $f \mathscr{R} g$ with the understanding that f, g are any representatives of their classes.

We shall say that f is *normalized under* $\mathscr{R}$ if $f \mathscr{R} g \mathscr{R} f$ implies $|d(g)| \geqslant |d(f)|$, *minimal under* $\mathscr{R}$ if $f \mathscr{R} g$ implies $g \mathscr{R} f$, and *almost minimal under* $\mathscr{R}$ if $f \mathscr{R} g \mathscr{R} h$ implies either $g \mathscr{R} f$ or $h \mathscr{R} g$.

2. Transformations of quadratic forms. For $m > 0$, $\varepsilon = 0$ or 1, and n-ary f we consider the $x \in \Lambda_n$ satisfying the two congruences

$$(2.1) \qquad A(f)x \equiv \mathbf{0} \pmod m,$$

$$(2.2) \qquad 2^{\varepsilon} f(x) \equiv 0 \pmod m.$$

It is clear from (1.1) that

$$(2.3) \qquad (2.1) \Rightarrow (2.2) \quad \text{in case } \varepsilon = 1 \text{ or } 2 \nmid m.$$

In case $\varepsilon = 0$, (1.1) shows that (2.1) and (2.2) are together equivalent to $f(x+z) \equiv f(z) \pmod m$ for every $z \in \Lambda_n$. From this remark and (2.3),

$$(2.4) \qquad \Lambda(m, \varepsilon, f) = \{x : x \in \Lambda_n, (2.1), (2.2)\}$$

is a sub-lattice of Λ_n. Clearly $\Lambda(m, \varepsilon, f') = \Lambda(m, \varepsilon, f)$ if f' is identically congruent to f modulo m. And if $\det T = \pm 1$ and $f'(x) = f(Tx)$, then $\Lambda(m, \varepsilon, f') = T^{-1}\Lambda(m, \varepsilon, f)$. We choose M so that

$$(2.5) \qquad M\Lambda_n = \Lambda(m, \varepsilon, f),$$

and note that this remains valid with M_1 in place of M if and only if $M_1 = MT$ for some T with $\det T = \pm 1$. Moreover, since each column of M satisfies (2.1), we have $m \mid A(f)M$, whence by transposition $m \mid M'A(f)$.

Now we define a form g by

$$(2.6) \qquad g(y) = 2^{\varepsilon} m^{-1} f(My), \quad A(g) = 2^{\varepsilon} m^{-1} M' A(f) M.$$

It is clear that g has integer coefficients; and $d(g) \neq 0$ since the obvious $\Lambda(m, \varepsilon, f) \supset m\Lambda_n$ implies $\det M \neq 0$. We define $f \to (m, \varepsilon) g$ to mean that there exists M such that (2.5) and (2.6) hold. From the remarks following (2.5) and (2.6), (1.3) holds with $\to(m, \varepsilon)$ for $\mathscr{R}$. So we may regard $\to(m, \varepsilon)$ as a class-to-class mapping; it is the m-mapping of [1] if $\varepsilon = 0$.

Again using the obvious $M\Lambda_n \supset m\Lambda_n$, we see that $N = mM^{-1}$ has integer elements and so we may write (2.5), (2.6) as

$$(2.7) \qquad \Lambda(m, \varepsilon, f) = \{x : x \in \Lambda_n, \ Nx \equiv \mathbf{0} \pmod m\},$$

$$(2.8) \qquad f(x) = 2^{-\varepsilon} m^{-1} g(Nx), \quad MN = mI.$$

In the foregoing, we have worked in the ring Z of rational integers, but the whole argument goes through in the ring Z_p of p-adic integers (p any prime), with Z embedded in the natural way. Suppose we do so, with forms f, g having coefficients in Z_p, matrices and vectors having elements in Z_p, and $\det T$ a p-adic unit. We obtain a mapping of classes under $\underset{p}{\sim}$, satisfying (1.3) with $\underset{p}{\sim}$ for $\sim$. Back to Z by specializing, and we have (for all p, m, ε)

$$(2.9) \qquad f \underset{p}{\sim} f', \quad f \to (m, \varepsilon) g, \quad \text{and} \quad f' \to (m, \varepsilon) g' \Rightarrow g \underset{p}{\sim} g'.$$

The case $p \nmid m$ of (2.9) follows also from the first of

$$(2.10) \qquad f \to (m, \varepsilon) g \Rightarrow g \underset{p}{\sim} 2^{\varepsilon} mf \quad \text{for} \quad p \nmid m, \text{ and } g \underset{\infty}{\sim} f;$$

these are clear from (2.6), (2.8). Using (2.9) and the second half of (2.10), we see that

$$(2.11) \qquad f \simeq f', \quad f \to (m, \varepsilon) g, \quad \text{and} \quad f' \to (m, \varepsilon) g' \Rightarrow g \simeq g'.$$

3. Repeated transformation, easy cases. For m, ε as in § 2 and q, η satisfying the same conditions, that is, $q > 0$, $\eta = 0$ or 1, we investigate the product of $\to(m, \varepsilon)$ and $\to(q, \eta)$. That is, we seek to eliminate g from

$$(3.1) \qquad f \to (m, \varepsilon) g, \quad g \to (q, \eta) h.$$

Choosing M so that (2.5) and (2.6) hold, we substitute q, η, g, y for m, ε, f, x in (2.1), (2.2), and then substitute for g, $A(g)$ from (2.6). So we see that $\Lambda(q, \eta, g)$ is the set of $y \in \Lambda_n$ satisfying the congruences

$$(3.2) \qquad 2^{\varepsilon} m^{-1} M' A(f) My \equiv \mathbf{0}, \quad 2^{\varepsilon+\eta} m^{-1} f(My) \equiv 0 \pmod q.$$

Now $h(z) = 2^\eta q^{-1} g(Rz)$, where $R\Lambda_n = \Lambda(q, \eta, g)$, which with (2.6) gives

$$h(z) = 2^{\varepsilon+\eta} m^{-1} q^{-1} f(Pz), \tag{3.3}$$

where $P, = MR$, satisfies

$$P\Lambda_n = \{My:\ y \in \Lambda_n, (3.2)\}. \tag{3.4}$$

In the easy case $\varepsilon, q, \eta = 1, 2, 0$, we use $m \mid M'A(f)$, and (3.2) reduces to $m \mid f(My)$. So, by (2.6) and (3.4), $P\Lambda_n$ is the intersection of $\Lambda(m, 1, f)$ and the set of x with $m \mid f(x)$. This gives $P\Lambda_n = \Lambda(m, 0, f)$, which with (3.3) gives $f \to (m, 0)h$. So we have

$$\to(m, 0) = \to(m, 1).\to(2, 0). \tag{3.5}$$

Next, take $q = m, \eta = \varepsilon$. Then (3.2) is easily seen to be satisfied by $y = Nz$, where $N = m^{-1}M$, for every $z \in \Lambda_n$. So if we define

$$\Lambda^{(2)}(m, \varepsilon, f) = \{My:\ y \in \Lambda(m, \varepsilon, g)\} \tag{3.6}$$

we have $\Lambda^{(2)}(m, \varepsilon, f) \supset m\Lambda_n$. (In (3.6), g is defined by (2.6) for M chosen — the choice is clearly immaterial — to satisfy (2.5).) So we see that

$$f \to (m, \varepsilon) g \to (m, \varepsilon) h \Rightarrow h(z) = 4^\varepsilon m^{-2} f(Pz), \tag{3.7}$$

$$f(x) = 4^{-\varepsilon} h(Qx), \quad PQ = mI, \quad P\Lambda_n = \Lambda^{(2)}(m, \varepsilon, f).$$

Now we take m and q to be coprime, and note that $\det M$ is prime to q, because $M\Lambda_n \supset m\Lambda_n$ implies $(\det M) \mid m^n$. So we may simplify (3.2) by omitting the factors m^{-1}, M'. If we then put x for My, (3.2) reduces to

$$2^\varepsilon A(f)x \equiv 0, \quad 2^{\varepsilon+\eta} f(x) \equiv 0 \pmod q; \tag{3.8}$$

and we see that $P\Lambda_n = M\Lambda_n \cap (3.8) = \Lambda(m, \varepsilon, f) \cap (3.8)$. From (2.1), (2.2), and g.c.d.$(m, q) = 1$ it follows easily that

$$\Lambda(m, \varepsilon, f) \cap \Lambda(q, \varepsilon, f) = \Lambda(mq, \varepsilon, f) \tag{3.9}$$

for either value of ε; and by (2.3) we see that (3.9) remains valid with $\Lambda(m, 1-\varepsilon, f)$ for $\Lambda(m, \varepsilon, f)$ if $2 \nmid m$, and similarly if $2 \nmid q$. We may moreover omit the factors 2^ε in (3.8) if $2 \nmid q$; and then we have $(3.8) = \Lambda(q, \eta, f)$. From these remarks we see that $P\Lambda_n = \Lambda(mq, \zeta, f)$, $\zeta = \max(\varepsilon, \eta)$. Now, by (3.3) and (2.6), we find

$$\to(m, \varepsilon).\ \to(q, 0) = \to(q, 0).\to(m, \varepsilon) = \to(mq, \varepsilon) \tag{3.10}$$

if g.c.d.$(2^\varepsilon m, q) = 1$.

4. Monotonicity of the class-number. The case $\varepsilon = 0$ of the following theorem is included in [1] (Theorem 1), but the following proof, valid also for $\varepsilon = 1$, is simpler.

THEOREM 1. *The class-number does not increase under any of the transformations of* § 2; *that is,* $f \to (m, \varepsilon)g$ *implies* $c(g) \leqslant c(f)$.

Proof. We shall first show that

$$f \to (m, \varepsilon)g \quad \text{and} \quad g \simeq g' \Rightarrow f' \to (m, \varepsilon)g' \quad \text{for some } f' \simeq f. \tag{4.1}$$

From $g \simeq g'$ it follows, see, e.g. [3] (p. 68, Theorem 41), for any $q > 0$, that some $g'' \sim g$ is identically congruent to g' modulo q. Using this result, with $2m^2q$ for q, we may suppose without loss of generality that $g \equiv g' \pmod{2m^2q}$ (identically). Now we choose M so that (2.5) and (2.6) hold, and define f' by

$$f'(x) = 2^{-\varepsilon} m^{-1} g'(Nx), \tag{4.2}$$

with $N = mM^{-1}$ as in (2.8); whence clearly f' is identically congruent to f modulo mq. Now by the remark following (2.4) we have

$$\Lambda(m, \varepsilon, f') = \Lambda(m, \varepsilon, f) = M\Lambda_n.$$

It follows that

$$f' \to (m, \varepsilon) 2^\varepsilon m^{-1} 2^{-\varepsilon} m^{-1} g'(NMy) = m^{-2} g'(my) = g'.$$

We notice that f, f', g, g' are all equivalent over the real field, by (4.2), (2.8) and $g \simeq g'$. So $f \underset{\infty}{\sim} f'$; and it is easily seen that $d(f) = d(f')$. Now there is a $q > 0$ (which we could take to be $|d(f)|$) so that these conditions and $f \equiv f' \pmod q$ (identically) imply $f \simeq f'$. For this see [3], loc. cit. So by choosing q suitably we have (4.1).

We now restrict the mapping $\to(m, \varepsilon)$ to the set of classes constituting the genus of f. The image set of classes is included in the genus of g, by (2.11); (4.1) gives the converse inclusion, and the theorem follows.

The next theorem is almost a corollary of Theorem 1.

THEOREM 2. *Suppose that either* $\varepsilon = 1$ *or* $2 \nmid m$, *and that* $f \to (m, \varepsilon)g$. *Then* $c'(g) \leqslant c'(f)$, *where* $c'(f)$ *is the number of classes, in the genus of* f, *that do not contain disjoint forms.*

Proof. Suppose first that f is disjoint, and by renumbering the variables that f is of the shape

$$f_1(x_1, \ldots, x_k) + f_2(x_{k+1}, \ldots, x_n), \quad 0 < k < n. \tag{4.3}$$

Define g_1, g_2, up to equivalence, by $f_i \to (m, \varepsilon)g_i$, $i = 1, 2$; and let g be the form

$$g_1(y_1, \ldots, y_k) + g_2(y_{k+1}, \ldots, y_n).$$

Because of the conditions on ε, m, we may appeal to (2.3), disregard (2.2), and break up (2.1) into two congruences, one involving $x_1, \ldots, x_k$, the other $x_{k+1}, \ldots, x_n$. $f \to (m, \varepsilon)g$ follows easily, on satisfying (2.5) with M of the shape $\operatorname{diag}[M_1, M_2]$, M_1 k by k, M_2 $n-k$ by $n-k$.

The foregoing argument works also for every $f' \simeq f$ that is equiva-

lent to a disjoint form. So we may exclude classes of such f' from the mapping of Theorem 1; and with this further restriction the image set still contains all classes that do not contain disjoint forms. The theorem follows.

5. The case of equality in Theorem 1. We shall prove:

THEOREM 3. *Suppose that $f\to(m,\varepsilon)g$ and $f'\to(m,\varepsilon)g$. Choose h so that $g\to(m,\varepsilon)h$ and $M, M_1, N, N_1, P, P_1, Q, Q_1$ so that (2.5)–(2.8), (3.7) hold as they stand and also with f', M_1, N_1, P_1, Q_1, for f, M, N, P, Q. Then each of the following is a necessary and sufficient condition for $f\sim f'$:*

(i) *g has an automorph S such that*

$$MSy\equiv\mathbf{0}(\mathrm{mod}\,m)\Leftrightarrow M_1y\equiv\mathbf{0}(\mathrm{mod}\,m); \tag{5.1}$$

(ii) *h has an automorph U such that*

$$PUx\equiv\mathbf{0}(\mathrm{mod}\,m)\Leftrightarrow P_1x\equiv\mathbf{0}(\mathrm{mod}\,m); \tag{5.2}$$

and these conditions are equivalent respectively to

$$S^{-1}NA_n=N_1A_n,\qquad U^{-1}QA_n=Q_1A_n.$$

Proof. The S of (i) has to have $\det S=\pm1$, since $g(Sy)=g(y)$ gives $(\det S)^2d(g)=d(g)\neq0$. Similarly, $\det U=\pm1$. With this we see that

$$MSy\equiv\mathbf{0}(\mathrm{mod}\,m)\Leftrightarrow MSy\in mA_n=(MS)(S^{-1}NA_n)\Leftrightarrow y\in S^{-1}NA_n.$$

Treating the other three congruences in (5.1), (5.2) similarly, the last assertion follows.

Now assume (i) satisfied; $S^{-1}NA_n=N_1A_n$ implies $S^{-1}N=N_1T$, for some T with $\det T=\pm1$. Now (2.8) and $g(y)=g(Sy)$ give $f(x)=2^{\varepsilon}m^{-1}g(N_1Tx)$, $f'(x)=2^{\varepsilon}m^{-1}g(N_1x)$. These give $f'(Tx)=f(x)$, $f\sim f'$. If we assume (ii) we can argue similarly; so each of (i), (ii) is sufficient.

We may now assume $f\sim f'$ and choose T so that $f'(x)=f(Tx)$, $\det T=\pm1$. As remarked in § 2, after (2.4), this gives $A(m,\varepsilon,f')=T^{-1}A(m,\varepsilon,f)$, that is, $M_1A_n=T^{-1}MA_n$. So for some S with $\det S=\pm1$ we have $M_1=T^{-1}MS$, whence we have (5.1). Similarly, we find U with $\det U=\pm1$ satisfying (5.2). From (2.6), $f'(x)=f(Tx)$, and $M_1=T^{-1}MS$ we have $2^{-\varepsilon}mg(y)=f(MSy)=f(My)$, from which $g(y)=g(Sy)$ follows and so (i) is necessary, as is (ii), by a similar argument.

As an example of the application of Theorem 3, take $m=3$, $\varepsilon=0$, and f congruent (identically) to $-9x_1^2+x_2^2+3(x_3^2+\ldots+x_n^2)(\mathrm{mod}\,27)$. Then we have $f\to(3,0)g\to(3,0)h$, with $g\equiv-3y_1^2+3y_2^2+y_3^2+\ldots+y_n^2(\mathrm{mod}\,9)$ and $h\equiv-z_1^2+z_2^2+3(z_3^2+\ldots+z_n^2)(\mathrm{mod}\,3)$. It is easily seen that $h\to(3,0)g$, and so three applications of Theorem 1 give $c(f)\geqslant c(g)=c(h)$. We examine the possibilities for f' with $f'\to(3,0)g$ and $f'\simeq f$.

We appeal to Theorem 3; and it is simpler to work with (ii) rather than (i) and to regard $f(x)=h(Qx)$ as $h(z)$ with the condition $Pz\equiv0$ (mod 3) on z. Here $Q=\mathrm{diag}[3,1,\ldots,1]$, $P=3Q^{-1}$, so $Pz\equiv\mathbf{0}$ is equivalent to $z_1\equiv0(\mathrm{mod}\,3)$. We see that $P_1z\equiv0(\mathrm{mod}\,3)$ must be consistent with $h(z)\equiv1$ but not with $h(z)\equiv-1(\mathrm{mod}\,3)$, else $f'\simeq f$ is obviously false. This gives us $P_1z\equiv\mathbf{0}\Leftrightarrow z_1\equiv0\Leftrightarrow Pz\equiv\mathbf{0}(\mathrm{mod}\,3)$. So (ii) holds with $U=I$ and Theorem 3 gives $f'\sim f$.

The argument above depends entirely on the generic properties of f, g, h. So it gives us that if $f_1\simeq f_1'\simeq f$, and $f_1, f_1'\to(3,0)g_1$ ($\simeq g$), then $f_1\sim f_1'$. From this we see that $c(f)=c(g)=c(h)$. And this would still hold for the same g- and h-genera but with f in a different genus, $\equiv-x_1^2+9x_2^2+\ldots(\mathrm{mod}\,27)$.

Now suppose we begin with $f\equiv9x_1^2+x_2^2+3(x_3^2+\ldots)(\mathrm{mod}\,27)$. Proceeding in the same way, we find that $P_1z\equiv\mathbf{0}(\mathrm{mod}\,3)$ is equivalent to one of $z_1\equiv0$, $z_2\equiv0(\mathrm{mod}\,3)$. So $f\sim f'$ if h has an automorph U that interchanges these two congruences; $c(f)=c(g)=c(h)$ only if every $h'\simeq h$ has such an automorph.

6. Repeated transformation, the general case. We consider chains

$$f_{i-1}\to(m_i,\varepsilon_i)f_i,\quad i=1,\ldots,k. \tag{6.1}$$

We define $f\to F$ to mean that for some $k\geqslant0$ there exists a chain (6.1) with $f_0\sim f$ and $f_k\sim F$; and $f\leftrightarrow F$ to mean $f\to F\to f$. Repeated application of Theorem 1 shows that $f\to F$ and $f\leftrightarrow F$ imply $c(F)\leqslant c(f)$, $=c(f)$, respectively. Next, $f\underset{\mathscr{G}}{\to}F$ ($\mathscr{G}$ for Gaussian) means the same as $f\to F$ except for the restriction

$$\varepsilon_i=1\quad\text{for every even } m_i; \tag{6.2}$$

and $f\underset{\mathscr{G}}{\leftrightarrow}F$ means $f\underset{\mathscr{G}}{\to}F\underset{\mathscr{G}}{\to}f$. These two relations are of interest in connection with Theorem 2.

It follows at once from (3.10), lengthening the chain (6.1) by factorizing the mappings, that we can impose the restriction

$$\text{each } 2^{\varepsilon_i}m_i \text{ is a power of some prime } p_i, \tag{6.3}$$

whence $\varepsilon_i=0$ if m_i is odd, without affecting any of the foregoing definitions. Further, we define $\underset{p}{\to}$ and $\underset{p}{\leftrightarrow}$, for each prime p, like $\to$ and $\leftrightarrow$, but with the condition (6.3) and each $p_i=p$. Finally, $\underset{2\mathscr{G}}{\to}$ and $\underset{2\mathscr{G}}{\leftrightarrow}$ are defined like $\underset{2}{\to}$ and $\underset{2}{\leftrightarrow}$, but with every $\varepsilon_i=1$.

By repeated use of (2.6), the end points f_0, f_k of the chain (6.1) are related by an identity of the shape

$$f_k(x)=2^{\varepsilon_1+\ldots+\varepsilon_k}(m_1\ldots m_k)^{-1}f_0(Vx),\qquad \det V|(m_1\ldots m_k)^n. \tag{6.4}$$

If there exists an integer v such that $2^{\varepsilon_1+\ldots+\varepsilon_k}(m_1\ldots m_k)^{-1}=v^2$, and $V=vT$, T having integer elements and $\det T=\pm1$, then we shall say

that the chain (6.1) is *closed*; if so, $f_0 \sim f_k$, and $f_0 \leftrightarrow f_i$ for $i = 1, \ldots, k$. (6.1) may be called a *$\mathscr{G}$-chain* if it satisfies (6.2), a *p-chain* if it satisfies (6.3) with all $p_i = p$. We notice that if we keep the same m_i, ε_i, k but replace f_0 by a form f_0' identically congruent to f_0 modulo $m_1 \ldots m_k$, and the other f_i by suitably chosen forms f_i', then we have a new chain satisfying (6.4) with f_0', f_k' for f_0, f_k and with the same m_i, ε_i, V. So this chain is closed if and only if (6.1) is so.

Now suppose that (6.3) holds and that, for some $i < k$, $p_i \neq p_{i+1}$. Then we may interchange $\to(m_i, \varepsilon_i)$ and $\to(m_{i+1}, \varepsilon_{i+1})$ by (3.10), replacing f_i by some suitable f_i', but, see (3.9), not altering f_0, f_k or V. So again we have a new chain that is closed if and only if the old one is so. Further, suppose that by such interchanges we obtain a chain which is a union of p-chains with distinct p (placed end to end); it is easily seen that the original chain is closed if and only if each of these p-chains is so. For we have for each p-chain an identity of the shape (6.4) with the numerical factor and $|\det V|$ each a power of p; and on eliminating the unwanted f_i from these identities we get (6.4) without any cancellation.

Using the case $k = 1$ of (6.4), see again (2.6), we see that if (6.3) holds then

$$d(f_i)/d(f_{i-1}) \text{ is a power of } p_i. \tag{6.5}$$

Now, see the definitions at the end of § 1, we state and prove:

THEOREM 4. (i) *f is normalized under $\to$ if and only if it is so under $\underset{p}{\to}$ for every p.*

(ii) (i) *above remains valid with 'minimal' in place of 'normalized'.*

(iii) *f is almost minimal under $\to$ if and only if it is almost minimal under $\underset{q}{\to}$ for some prime q, and minimal under $\underset{p}{\to}$ for every $p \neq q$.*

(iv) (i)–(iii) *above all remain valid with $\underset{\mathscr{G}}{\to}$, $\underset{2\mathscr{G}}{\to}$ for $\to$, $\underset{1}{\to}$.*

Proof. Suppose first that f is normalized under $\to$; that is, that every closed chain (6.1) with $f_0 \sim f \sim f_k$ satisfies $|d(f_i)| \geqslant |d(f)|$ for $i = 1, \ldots, k-1$. Because of (6.5), this remains true for any p if we restrict (6.1) to be a p-chain, so f is normalized under $\underset{p}{\to}$, and we have the 'only if' of (i). Proof of the 'if' is similar but simpler; and (ii)–(iv) are proved in the same way.

When the chain (6.1) is a union of p-chains it can be abbreviated, for some $l \leqslant k$, and with $f^{(0)} = f_0$, $f^{(l)} = f_k$, to

$$f^{(i-1)} \underset{p_i}{\to} f^{(i)}, \quad i = 1, \ldots, l, \ p_i \neq p_j \text{ for } i \neq j. \tag{6.6}$$

THEOREM 5. (i) *$f \to F$ if and only if there exists a chain of the shape (6.6), with $f^{(0)} \sim f$ and $f^{(l)} \sim F$; and if so, $F \to f$ if and only if*

$$f^{(i)} \underset{p_i}{\to} f^{(i-1)}, \quad i = 1, \ldots, l. \tag{6.7}$$

(ii) (i) *above remains valid with $\underset{\mathscr{G}}{\to}$ for $\to$ and $\underset{2\mathscr{G}}{\to}$ for $\underset{p_i}{\to}$ when $p_i = 2$.*

Proof. As for Theorem 4.

7. The relation $\underset{p}{\to}$, $p > 2$. In this section p is a fixed odd prime, so, for any f, there are integers a_i, e_i such that

$$f \underset{p}{\sim} \sum_{i=1}^{n} a_i p^{e_i} x_i^2, \quad p \nmid 2a_1 \ldots a_n. \tag{7.1}$$

We define

$$u = u(f, p), \quad v = v(f, p) = \min, \ \max(e_1, \ldots, e_n). \tag{7.2}$$

Then it is well known that u and v are invariant under $\underset{p}{\sim}$. We next write

$$f \to (p^v, 0) F_p; \tag{7.3}$$

the form F_p so defined (up to equivalence) may be called the p-adic reciprocal of f. We note that, for any $w \geqslant 0$,

$$f \to (p^w, 0) g \Rightarrow g \underset{p}{\sim} \sum_{i=1}^{n} a_i p^{|w-e_i|} x_i^2. \tag{7.4}$$

In proving (7.4) we may by (2.9), without loss of generality, suppose f equal to the disjoint form on the right of (7.1). Then by treating this disjoint form as in the proof of Theorem 2 the case $n \geqslant 2$ reduces to the case $n = 1$, which is easy, see (2.1)–(2.6). It follows at once from (7.4) that

$$v(g, p) - u(g, p) \leqslant v(f, p) - u(f, p).$$

So the non-negative p-adic invariant $v - u$ is non-increasing under $\underset{p}{\to}$; that is,

$$f \underset{p}{\to} F \Rightarrow v(F, p) - u(F, p) \leqslant v(f, p) - u(f, p). \tag{7.5}$$

In particular, with the g of (7.4) for F, equality holds in (7.5) if and only if either $w \leqslant u$ or $w \geqslant v$.

In these two cases we can improve (7.4) to

$$f \to (p^w, 0) g \Rightarrow g \sim \begin{cases} p^{-w} f & \text{if} \quad w \leqslant u, \\ p^{w-v} F_p & \text{if} \quad w \geqslant v. \end{cases} \tag{7.6}$$

For the first of these, note that f is identically 0 modulo p^w and so (2.1), with $m = p^w$, is vacuous and we may take $M = I$ in (2.6). For the second, suppose $w > v$ by (7.3), then (2.1) implies $p^{w-v} | x$, as is easily seen from (7.1); and if we put $x = p^{w-v} z$ in (2.1) and cancel p^{w-v}, we see that (2.1) holds if and only if $z \in \Lambda(p^v, 0, f)$. So, looking at (2.6), we have $g \sim p^{v-w} F_p(p^{w-v} z) = p^{w-v} F_p$. We next prove

$$F_p \to (p^v, 0) f, \quad \text{whence by (7.3)} \quad f \underset{p}{\leftrightarrow} F_p. \tag{7.7}$$

By using (7.4) twice over, and noting that $|v-|v-e_i|| = |e_i|$, we find a chain

$$f \to (p^v, 0)F_p \to (p^v, 0)G, \tag{7.8}$$

with a G for which $G \underset{p}{\sim} f$ is obvious, but $G \sim f$ is needed for (7.7). Now $G \sim f$ is immediate in the special case $f = f_0, f_0$ being the right member of (7.1). So by the arguments following (6.4) it follows from the weaker hypothesis $f \equiv f_0 (\mathrm{mod}\, p^{2v})$ (identically); and this hypothesis is easily seen to involve no loss of generality. Alternatively, (3.7), with $m, \varepsilon = p^v, 0$, gives $f = G(Qx)$ with $|\det Q|$ a power of p, so $= 1$ because of $f \underset{p}{\sim} G$, and again we have (7.7). From (7.6) and (7.7) it is easily seen that

$$f \underset{p}{\leftrightarrow} pf. \tag{7.9}$$

We now state and prove:

THEOREM 6. *For every odd prime p, with the notation above, we have*:

(i) $f \underset{p}{\leftrightarrow} F$ *if and only if either* $F \underset{p}{\sim} p^r f$ *or* $F \underset{p}{\sim} p^r F_p$ *holds for some integer* r;

(ii) f *is normalized under* $\underset{p}{\to}$ *if and only if* $u = 0$ *and* $e_1 + \ldots + e_n \leqslant \frac{1}{2}nv$;

(iii) f *is minimal under* $\underset{p}{\to}$ *if and only if* $v - u = 0$ *or* 1;

(iv) f *is almost minimal under* $\underset{p}{\to}$ *if and only if either* (a) $v - u = 2$ *or* (b) $v - u = 3$ *and none of the* $e_i = u+1$ *or* $u+2$;

(v) *for every* f, $f \underset{p}{\to} F$ *holds for some* F *which is minimal under* $\underset{p}{\to}$;

(vi) *for every pair* f, F *as in* (v) *but with* f *not minimal*, $f \underset{p}{\to} g \underset{p}{\to} F$ *for some almost minimal* g;

(vii) *if* α, β *are the numbers of even, odd* e_i *in* (7.1) *then* $|\alpha - \beta|$ *is invariant under* $\underset{p}{\to}$.

Proof. The 'if' of (i) is clear from (7.7), (7.9) and the transitivity of $\underset{p}{\leftrightarrow}$.

It is easy to see that the p-adic reciprocals of pf, F_p are $F_p, p^{-u}f$ respectively, so the conditions to be proved necessary (for the 'only if' of (i)) are unaltered by replacing f by the g of either case of (7.6). On the other hand we have

$$f \to (p^w, 0)g \underset{p}{\to} h \text{ and } u < w < v \quad \text{imply} \quad h \underset{p}{\nleftrightarrow} f. \tag{7.10}$$

For on going from f to g the exponent difference $v-u$ undergoes a decrease which by (7.5) cannot be made good on further mappings, from g to h and then to f. Constructing a p-chain from f to F and back to f, an easy induction on its length completes the proof of (i).

For (ii) we note that, by definition, f is normalized under $\underset{p}{\to}$ if and only if $|d(f)| \leqslant |d(F)|$ for every $F \underset{p}{\leftrightarrow} f$. Using (i), it evidently suffices to take $F = p^{-u}f$ or F_p; then $d(f)/d(F) = p^{nu}$ or p^s, with $s = v - 2e_1 + \ldots + v - 2e_n$. This gives the result.

For the 'only if' of (iii), supposing $v - u \geqslant 2$, we choose w with $u < w < v$, and then (7.10), with any h, say $h = g$, gives $f \underset{p}{\to} h \underset{p}{\nleftrightarrow} f$ and so f is not minimal. On the other hand, if $v - u = 0$ or 1, (7.6) is always applicable and with (i) gives $f \to (p^w, 0)g \Rightarrow f \underset{p}{\leftrightarrow} g$ for every w. From this the 'if' of (iii) follows.

In the proof of (iv) we may by (iii) assume that $v - u \geqslant 2$, and then from the definition in § 1 it follows easily that f is almost minimal under $\underset{p}{\to}$ if and only if there exists no w for which $f \to (p^w, 0)g$ implies $g \underset{p}{\nleftrightarrow} f$ and g not minimal under $\underset{p}{\to}$. Using (iii) this means that we cannot have $1 < v(g,p) - u(g,p) < v(f,p) - u(f,p)$. Using (7.4), this pair of inequalities can be expressed as

$$1 < \max_i |w - e_i| - \min_i |w - e_i| < v - u. \tag{7.11}$$

Now $w = u+1$ satisfies (7.11) if $v - u \geqslant 4$, so supposing $v - u \leqslant 3$ and noting that (7.11) implies $u < w < v$ the proof of (iv) is easily completed.

(v) is trivial if f is minimal, and nearly so if f is almost minimal; the construction for (iv) gives an induction on $v-u$ in the remaining case. (vi) follows easily from (v). For (vii) we look at (7.4) and note that

$$|w - e_i| - |w - e_j| \equiv e_i - e_j (\mathrm{mod}\, 2).$$

8. The relations $\underset{2g}{\to}$, $\underset{g}{\to}$. For $p = 2$ we have to replace (7.1) by

$$f \underset{2}{\sim} \sum_{i=1}^{v} 2^{a_i} a_i x_i^2 + \sum_{j=1}^{\varrho} 2^{r_j} \theta_j (x_{v+2j-1}, x_{v+2j}), \tag{8.1}$$

where the θ_j are binary forms with odd discriminants, the a_i are odd integers, and v, ϱ are non-negative integers with $v + 2\varrho = n$. If we write

$$e_{v+2j-1} = e_{v+2j} = r_j - 1 \quad \text{for} \quad j = 1, \ldots, \varrho, \tag{8.2}$$

then we can define $u = u(f,2)$ and $v = v(f,2)$ just as in (7.2). We define the 2-adic reciprocal of f, cf. (7.3), by

$$f \to (2^{\varepsilon+1}, 1)F_2. \tag{8.3}$$

Corresponding to (7.4), and proved in the same way, we have

$$f \to (2^{w+1}, 1)g \Rightarrow g \underset{2}{\sim} \sum_{i=1}^{v} 2^{|w-e_i|} a_i x_i^2 + \sum_{j=1}^{\varrho} 2^{|w+1-r_j|+1} \theta_j (x_{v+2j-1}, x_{v+2j}). \tag{8.4}$$

From this and (8.2) we see that we have

$$e_i(g) = |w - e_i(f)|$$

as in § 7.

The form f may be called Gaussian if its product terms all have even coefficients, or equivalently if $2|A(f)$. Clearly, by (8.4),

$$f \to (2^{w+1}, 1)g \Rightarrow 2|A(g). \tag{8.5}$$

This shows that we lose nothing by considering Gaussian forms only, for the rest of this section. For such forms it is easily seen that (7.5)–(7.9) hold good with 2 for p, $\to(2^{w+1}, 1)$ for $\to(p^w, 0)$, $\underset{2\mathscr{G}}{\to}$ for $\underset{p}{\to}$, and $\underset{2\mathscr{G}}{\leftrightarrow}$ for $\underset{p}{\leftrightarrow}$. We also have

THEOREM 7. *For Gaussian forms, Theorem 6 remains valid for $p = 2$, if $\underset{p}{\to}$ and $\underset{p}{\leftrightarrow}$ are replaced by $\underset{2\mathscr{G}}{\to}$, $\underset{2\mathscr{G}}{\leftrightarrow}$.*

Proof. Because of the remark following (8.4), we can argue just as in the proof of Theorem 6. The restriction to Gaussian f ensures $r_j \geqslant 1$, $e_i \geqslant 0$, $u \geqslant 0$.

Theorems 4–7 can be used to deduce what we need to know about $\underset{\mathscr{G}}{\to}$. In particular, we have

THEOREM 8. *Let f be an n-ary positive-definite quadratic form with integer coefficients such that every class in the genus of f contains a disjoint form (that is, $c'(f)$, defined in Theorem 2, is zero). Then there exists a square-free integer q and n by n matrices B, C, each with integer elements, such that $C = qB^{-1}$, $\det B|\det C$, and the Gaussian form $x'Bx$ satisfies all the conditions imposed on f.*

Proof. By Theorems 4–7, there exists a form F with $f \underset{\mathscr{G}}{\to} F$ and F normalized and minimal under $\underset{\mathscr{G}}{\to}$. Replacing f by $2f$ if necessary, and using (8.5), F is Gaussian, so $B = \frac{1}{2}A(F)$ has integer elements. $C = qB^{-1}$ also has integer elements if we define q as the least common denominator of the elements of B^{-1}. By Theorem 4, F is normalized and minimal under $\underset{p}{\to}$ for every $p > 2$, and under $\underset{2\mathscr{G}}{\to}$. Using (ii) and (iii) of Theorem 6, and Theorem 7, this gives $u = 0$, $v \leqslant 1$, $e_1 + \ldots + e_n \leqslant \frac{1}{2}n$, for each p. It follows easily that q is square-free and $\det B|\det C$. Repeated application of Theorem 2 shows that $c'(F) \leqslant c'(f)$, so $c'(F) = 0$ and this completes the proof. I hope to use Theorem 8 later to prove the

CONJECTURE. *For given n there exists a form f satisfying the hypotheses of Theorem 8 if and only if $2 \leqslant n \leqslant 13$.*

I have proved this conjecture for large n in an unpublished manuscript, using Siegel's formula for the weight of a genus, and Theorem 8; for $x'Bx$ as in Theorem 8 the weight formula becomes considerably simpler than it is in general.

9. Statement of results on $\underset{2}{\to}$. Clearly, for every f,

$$f \to (1, 1)2f \to (2, 0)f, \quad \text{whence} \quad f \underset{2}{\leftrightarrow} 2^r f, \tag{9.1}$$

for $r \geqslant 0$; and putting in factors 2 to avoid complication with non-Gaussian forms we have trivially

$$2f \underset{2\mathscr{G}}{\to} 2F \Rightarrow f \underset{2}{\to} F. \tag{9.2}$$

We therefore have (using Theorem 7) a necessary and sufficient condition for $f \underset{2}{\leftrightarrow} F$ if we can determine all the cases in which

$$f \underset{2}{\leftrightarrow} F \text{ is true but } 2f \underset{2\mathscr{G}}{\leftrightarrow} 2F \text{ is false.} \tag{9.3}$$

We write $[a, b, c, \ldots]$ for a diagonal form with coefficients a, b, c, $\ldots$, and ψ_r for the sum of the θ_j in (8.1) with $r_j = r$, $r = 0, 1, \ldots$ Then we can abbreviate (8.1) to

$$f \underset{2}{\sim} [2^{e_1}a_1, 2^{e_2}a_2, \ldots] + \psi_0 + 2\psi_1 + 4\psi_2 + \ldots \tag{9.4}$$

It will sometimes be convenient to put in one or two 0's after $2^{e_r}a_r$, or to put $+2^s\psi_s$ after $\ldots$ thereby indicating that ψ_r is identically 0 for all $r > s$, and possibly also for some or all of the $r \leqslant s$.

With this notation we give examples to show that (9.3) is possible. Each of them can, with $m = 2$ or 4, be written in the shape

$$f_0 \to (m, 1)\ f_1 \to (2, 0)\ f_2 \to (m, 1)\ f_3 \to (2, 0)\ f_0, \tag{9.5}$$

$$f_1 \to (2m, 1)\ 2f_0 \to (2m, 1)\ f_1, \qquad f_3 \to (2m, 1)\ 2f_2 \to (2m, 1)\ f_3, \tag{9.6}$$

$$f_i \underset{2}{\leftrightarrow} f_j \text{ always}, \quad 2f_i \underset{2\mathscr{G}}{\leftrightarrow} 2f_j \text{ only if } \{i, j\} = \{0, 1\} \text{ or } \{2, 3\}. \tag{9.7}$$

EXAMPLE 1. Take $m = 2$ and $a = b = a' = b' = \pm 1$ or $a, b = \pm 1, \mp 3$, a', $b' = \mp 1$, ± 3, and let $f_0, \ldots, f_3$ be

$$[a, b] + \psi_0 + 2\psi_1, \quad [a, b] + 4\psi_0 + 2\psi_1,$$
$$[a', b'] + 2\psi_0 + \psi_1, \quad [a', b'] + 2\psi_0 + 4\psi_1.$$

It is easy to verify (9.5) and (9.6), whence the first part of (9.7); and we note that f_1, f_3 are the 2-adic reciprocals of f_0, f_1. Using Theorem 7, if the second half of (9.7) is false then $2^\alpha f_3 \underset{2}{\sim} f_0$ or f_1, for some α which is obviously 0. The first alternative gives $\psi_0 = \psi_1 = 0$. The second can be excluded by choosing ψ_0, ψ_1 not to have the same number of variables.

EXAMPLE 2. $m = 4$, a_3 odd, a_1, a_2 each odd or 0, $f_0, \ldots, f_3 =$

$$[a_1, a_2, 2a_3] + \psi_0 + 2\psi_1 + 4\psi_2, \quad [2a_1, 2a_2, a_3] + 8\psi_0 + 4\psi_1 + 2\psi_2,$$
$$[a_1, a_2, 2a_3] + 4\psi_0 + 2\psi_1 + \psi_2, \quad [2a_1, 2a_2, a_3] + 2\psi_0 + 4\psi_1 + 8\psi_2.$$

It can be shown exactly as in Example 1 that this gives all we require, except possibly the second half of (9.7), which, crudely, can fail only if ψ_0 and ψ_2 have equally many variables.

More generally, with $f_0, \dots, f_3$ as in either of these examples, (9.3) holds if there exist f', F' such that

$$2f \underset{2\mathscr{G}}{\leftrightarrow} 2f', \quad 2F \underset{2\mathscr{G}}{\leftrightarrow} 2F', \quad f', F' \underset{2}{\sim} f_0, f_2. \tag{9.8}$$

THEOREM 9. (9.3) *holds only if there exist* f', F' *satisfying* (9.8), *with* f_0, f_2 *as in Examples* 1 *and* 2.

It may be noticed that the conditions on a, b, a', b' could be weakened to $ab \equiv 1 \pmod 4$ and $a', b' \equiv \pm a, \pm b$, with the + or − sign according as $ab \equiv 1$ or $-3 \pmod 8$; and then by symmetry (interchanging ψ_0 and ψ_1) f_0 and f_2 can be interchanged in (9.8).

THEOREM 10. *To every* f *there corresponds an* F *such that* $f \underset{2}{\to} F$ *and* F *is minimal under* $\underset{2}{\to}$. *A form is minimal under* $\underset{2}{\to}$ *if and only if it is 2-adically equivalent to a multiple of one of the following*:

(i) $\psi_0 + 2\psi_1$;

(ii) *the forms* $f_0, \dots, f_3$ *of Example* 1 *above*;

(iii) *the* $f_0, \dots, f_3$ *of Example* 2, *with* $a_3 = 0$, $a_1 a_3$ *odd, and* $\psi_2 = 0$;

(iv) *the* $f_0, \dots, f_3$ *of Example* 2, *with* $a_1 = a_2 = 0$, a_3 *odd, and* $\psi_2 = 0$.

In case (i), $\psi_0 + 2\psi_1 \to (2,0) 2\psi_0 + \psi_1 \to (2,0) \psi_0 + 2\psi_1$, so $\psi_0 + 2\psi_1$ is normalized only if its discriminant does not exceed that of $2\psi_0 + \psi_1$, that is, only if ψ_0 has at least $\frac{1}{2}n$ variables. Similarly, the normalized forms can be picked out in cases (ii)–(iv).

THEOREM 11. f *is almost minimal under* $\underset{2}{\to}$ *if and only if there exist* f', F *such that* $f \underset{2}{\leftrightarrow} f' \underset{2}{\sim} F$ *and* F *is one of*

$$[a] + \psi_0 + 2\psi_1 + 4\psi_2, \quad \psi_0\psi_2 \neq 0, \quad \textit{and either } a = 0 \textit{ or } 4 \nmid a; \tag{9.9}$$

$$[a, b] + \psi_0 + 2\psi_1 + 4\psi_2, \quad \psi_0\psi_2 \neq 0, \quad ab \equiv 1 \textit{ or } 2 \pmod 4; \tag{9.10}$$

$$[a] + \psi_0 + 8\psi_3, \quad \psi_0\psi_3 \neq 0, \quad \textit{and either } a = 0 \textit{ or } 2 \nmid a; \tag{9.11}$$

$$[a, b] + \psi_0 + 8\psi_3, \quad \psi_0\psi_3 \neq 0, \quad ab \equiv 1 \textit{ or } 2 \pmod 4; \tag{9.12}$$

$$[4a] + \psi_0 + 2\psi_1, \quad \psi_0 \neq 0, \quad 4 \nmid a, \quad \psi_1 = 0 \textit{ if } 2 \mid a; \tag{9.13}$$

$$[1, a] + \psi_0 + 2\psi_1, \quad a \equiv -1 \pmod 4; \tag{9.14}$$

$$[2a, 4b] + \psi_0 + 2\psi_1, \quad ab \equiv 1 \textit{ or } 2 \pmod 4; \tag{9.15}$$

$$[a, 4b] + 2\psi_1 + 4\psi_2, \quad ab \equiv 1 \pmod 4; \tag{9.16}$$

$$[1, a, 2b] + 2\psi_1 + 4\psi_2, \quad 2 \nmid ab; \tag{9.17}$$

$$[1, -1, 2a, 2b] + 2\psi_1 + 4\psi_2, \quad ab \equiv 1 \pmod 4; \tag{9.18}$$

$$[a, 8b] + 2\psi_1 + 4\psi_2 + 8\psi_3, \quad 2 \nmid ab, \quad \psi_1\psi_3 = 0; \tag{9.19}$$

$$[1, -1, 4a] + 2\psi_1 + 4\psi_2 + 8\psi_3, \quad 2 \nmid a, \quad \psi_1\psi_3 = 0; \tag{9.20}$$

$$[1, -1, 2a, 4b] + 2\psi_1 + 4\psi_2 + 8\psi_3, \quad 2 \nmid ab, \quad \psi_1\psi_3 = 0. \tag{9.21}$$

If f *is not minimal,* $f \underset{2}{\to} F$, *and* F *is minimal, then* $f \underset{2}{\to} g \underset{2}{\to} F$ *for some* g *which is almost minimal under* $\underset{2}{\to}$.

10. Proof of Theorems 9–11. We need to normalize (8.1), and (9.4), by making ν as small as possible. To do so, note that, for odd a_i,

$$[a_1, a_2, a_3] \underset{2}{\sim} [a_1 + a_2 + a_3] + 2\theta, \tag{10.1}$$

with $d(\theta) = -a_1a_2a_3(a_1 + a_2 + a_3)$. This gives us that we may suppose no three of the e_i equal, or more precisely

$$e_1 \leqslant \dots \leqslant e_\nu, \quad e_i < e_{i+2} \quad \text{if} \quad i \leqslant \nu - 2, r_1 \leqslant \dots \leqslant r_\varrho. \tag{10.2}$$

With this condition it is easily seen that

$$2 \mid A(f) \quad \text{and} \quad f \to (2,0) h \Rightarrow h \underset{2}{\sim} h_1 + h_2, \tag{10.3}$$

where

$$h_1 = 0, \quad 2a_1x_1^2, \quad \text{or} \quad \tfrac{1}{2}a_1(2x_1 + x_2)^2 + \tfrac{1}{2}a_2x_2^2, \tag{10.4}$$

according as the number of zero e_i is 0, 1, or 2; and h_2 is derived from the right member of (8.1), or (9.4), by omitting the terms with odd coefficients and dividing the others by 2. In the third case of (10.4), if $a_1a_2 \equiv -1 \pmod 4$ we have $h_1 = 2\theta$, $d(\theta)$ odd; but if $a_1a_2 \equiv 1 \pmod 4$ then $h_1 \underset{2}{\sim} \pm(a_1x_1^2 + a_2x_2^2)$, with the sign + or − according as $-a_1a_2 \equiv 1$ or $-3 \pmod 8$.

It will be convenient to postpone the proof of Theorem 9.

Deduction of Theorem 10 from Theorem 9. For given f, suppose $f \to (m, \varepsilon) g$, m a power of 2. Then the possibilities for g up to equivalence can be found by using (3.5) and (7.6); there are infinitely many, but if we write $g = 2^r h$, $r \geqslant 0$ and h 2-adically primitive, then there are only finitely many possibilities for h.

In particular, taking f to be 2-adically equivalent to a form of one of the shapes (i)–(iv), we find either $h \sim f$ or F_2, see (7.3), or h equivalent to one of the other two members of the quadruplet of Example 1 or 2 to which f belongs. In each case $h \underset{2}{\to} f$ is clear, so $f \underset{2}{\to} g \underset{2}{\to} h \underset{2}{\to} f$, $f \underset{2}{\leftrightarrow} g$, and f is minimal. So by (9.1) is $2^r f$, $r \geqslant 0$. This proves the 'if' of the theorem.

Now, starting with any f, a sufficiently long chain (6.1) with mappings $\to(2,1)$, $\to(2,0)$ alternately gives $f \underset{2}{\to} g$, for some $g \underset{2}{\sim} g'$, g' one of (i)–(iv). This is easily verified, and using the 'if' it gives the first assertion of the theorem. Specializing by taking f to be minimal, $f \underset{2}{\to} g$ implies $g \underset{2}{\to} f$, and so Theorem 9 gives the 'only if'.

Deduction of Theorem 11 from Theorems 9, 10. Let f be one of the forms that we have to prove almost minimal; whence by Theorem 10 we see that f is not minimal. Proceeding as in the first part of the proof

above, we find that $f \to (m, \varepsilon) g$, m a power of 2, implies either $g \underset{2}{\to} f$ or g minimal. Clearly this is also implied by $f \underset{2}{\to} g$, and so f is almost minimal. This gives the 'if'.

For the 'only if' suppose f not minimal; then $f \underset{2}{\to} g$ for one of the g that have been proved almost minimal. This is more subtle than the corresponding argument for the 'only if' of Theorem 10; but I leave it to the reader with the remark that it suffices to use $\to(2, 0)$ and $\to(2^{w+1}, 1)$, $w \leqslant 3$. Now if f is almost minimal, $g \underset{2}{\to} f$, $f \underset{2}{\leftrightarrow} g$, and Theorem 9 gives us the 'only if'.

The argument just used will not prove the remaining assertion, because F has to depend only on f, not on g. We construct a chain under $\underset{2}{\to}$ with each link irreversible:

$$f_{i-1} \underset{2}{\to} f_i \underset{2}{\not\to} f_{i-1}, \quad i = 1, \ldots, k, \tag{10.5}$$

$$f_0 = f, \quad f_1, \ldots, f_{k-1} \text{ all normalized}, \quad f_k = F;$$

for given f, F satisfying $f \underset{2}{\to} F$, F minimal, f not so, whence $k \geqslant 1$, and the f_i are pairwise inequivalent. If, for fixed f, F, k is bounded we choose the chain (10.5) to make k maximal; then $g = f_{k-1}$ gives $f \underset{2}{\to} g \underset{2}{\to} F$, g almost minimal. So suppose k unbounded. Since there are only finitely many classes with given d, $d(f_i)$ is unbounded. So, with $u_i = u(f_i, 2)$ and $v_i = v(f_i, 2)$ as in (7.2), (8.2), and $u_i = 0$ by (10.5), v_i is unbounded. It is however easily seen from (3.5), (8.4), (10.3) that $\max(2, v-u)$ is non-increasing under $\underset{2}{\to}$. So we have a contradiction which completes the proof.

For Theorem 9 we need some further preliminaries. We define

$$e(f) = e_\nu - e_1 \quad (= 0 \text{ if } \nu = 0), \tag{10.6}$$

$$e'(f) = \max\{e_i + 1 - r_j : i \leqslant \nu, j \leqslant \varrho\} \quad (= 0 \text{ if } \nu\varrho = 0), \tag{10.7}$$

$$e''(f) = r_\varrho - r_1 \quad (= 0 \text{ if } \varrho = 0). \tag{10.8}$$

From (8.4) we see that

$$f \to (2^{w+1}, 1) g \Rightarrow v(g) \leqslant v(f), \ e(g) \leqslant e(f), \tag{10.9}$$
$$\text{and if } v(g) = v(f), \text{ then also } e'(g) \leqslant e'(f), \ e''(g) \leqslant e''(f).$$

From (10.3), (10.4) we have

$$2 \mid A(f) \text{ and } f \to (2, 0) h \Rightarrow v(h) \leqslant v(f), \ e(h) \leqslant e(f), \tag{10.10}$$
$$\text{and if } v(h) = v(f), \text{ then } e''(h) \leqslant e''(f).$$

Now consider the possibility

$$2 \mid A(f), \ 2 \nmid f, \ f \to (2, 0) h, \ v(h) = v(f), \tag{10.11}$$
$$e(h) = e(f), \ e'(h) \geqslant e(f), \ e''(h) = e''(f).$$

Straightforward calculation shows that (10.11) implies that the invariants of f satisfy

$$\nu > 0, \ e_1 = 0, \ e_\nu \leqslant 1, \ r_\varrho \leqslant 2 (\text{or } \varrho = 0), \tag{10.12}$$
$$\text{and if } \nu \geqslant 2 \text{ and } e_2 = 0, \text{ then } \nu = 2 \text{ and } a_1 a_2 \equiv 1 \pmod 4.$$

Now, supposing $f \underset{2}{\leftrightarrow} F$, we have a closed chain

$$f_{i-1} \to (2^{w_i+1}, \varepsilon_i) f_i, \quad i = 1, \ldots, k, \quad f_k = f_0, \tag{10.13}$$

with two of the $f_i = f, F$ respectively. Factorizing the mappings with $\varepsilon_i = 0$ by (3.5), and noting that $\varepsilon_i = 1$ implies $2 \mid A(f_i)$, see (8.4), we may suppose that

$$\varepsilon_i = 0 \text{ only if } w_i = 0 \text{ and } 2 \mid A(f_i). \tag{10.14}$$

Looking at (10.9), (10.10) we see that the chain (10.13) cannot close unless ν, e and e'' have the same values for all its f_i. From the constancy of ν and Theorem 7, we see easily that $2f_{i-1} \underset{2^\nu}{\leftrightarrow} 2f_i$ whenever $\varepsilon_i = 1$; also, trivially when $f_{i-1} = 2f_i$. Supposing therefore that $2f \underset{2^\nu}{\leftrightarrow} 2F$ is false, one of the mappings of the chain has to be $\to(2, 0)$, with $f_{i-1} \neq 2f_i$. Choose such a mapping with $e'(f_i) - e'(f_{i-1})$ maximal, and so non-negative; and obviously there is no loss of generality in supposing $f_{i-1} = f$. Writing h for f_i, (10.11) holds, and (10.12) follows.

This leaves us just a few simple cases in which it is easy to find all the F with $f \underset{2}{\leftrightarrow} F$ and so complete the proof. It becomes still easier if we assume that f_i is the 2-adic reciprocal of f_{i-1} whenever $\varepsilon_i = 1$; and that assumption is easily justified.

11. Conclusion. For any f, with matrix A, we have

$$f \to (|\det A|, 1) g, \quad \text{where} \quad g(\boldsymbol{y}) = \boldsymbol{y}' (\operatorname{adj} A) \boldsymbol{y},$$

whence using $\operatorname{adj}(\operatorname{adj} A) = (\det A)^{n-2} A$ we see that $f \leftrightarrow g$. Hence the result, mentioned in § 6, that $f \leftrightarrow g \Rightarrow c(f) = c(g)$ may be regarded as a generalization of the classical result that equivalent forms have equivalent adjoints. From a 'family' (union of classes) of forms pairwise related by $\leftrightarrow$ it is easy to pick out the normalized ones, that is, those with smallest $|d|$. And given any representative of the family, normalized or not, it is easy to construct the whole family. Since $f \leftrightarrow af$ for every f and every $a > 0$, it

is convenient to omit the imprimitive members of the family, leaving a finite union of classes. For these remarks see Theorems 4–9.

I now outline an approach to the problem of finding, for given n, all the n-ary positive-definite quadratic forms with class-number 1. Suppose $n \geqslant 2$, since $n = 1$ is trivial. Consider only normalized forms; this shortens the labour and makes it less difficult to present the result in a reasonably concise form. With these preliminaries we may proceed by three steps.

Step 1. Find all the (classes of) positive-definite n-ary forms F with $c(F) = 1$, F minimal and normalized under $\to$.

This seems hopelessly difficult for $n = 2$, but I have done it for $n \geqslant 3$. For $n \geqslant 11$ there are no possibilities; for $n = 3$, 4 see [4], [5]. For $5 \leqslant n \leqslant 10$ see [6].

Step 2. Find all the positive g with $c(g) = 1$, g normalized and almost minimal under $\to$.

Theorem 4 (iii) (with g for f) shows that the arithmetic properties of the g here considered are not much more complicated than those of the F of Step 1, so the methods used for Step 1 are still available. It helps further to note that there must be a minimal F with $g \to F$ (see Theorems 5(i), 6(v), 10) and Theorem 1 gives $c(F) \leqslant c(g)$, so $c(F) = 1$, and the possibilities for F may be supposed known. They may be taken one by one if convenient. For many F with $c(F) = 1$ we find no almost minimal g at all with $g \to F$ and $c(g) = 1$; but in any case we find an upper bound for the 'bad' prime q of Theorem 4(iii), for which g is almost minimal under $\underset{q}{\to}$.

Step 3. Find all the positive f with $c(f) = 1$ that are normalized but neither minimal nor almost minimal under $\to$.

As in Step 2 we choose F, minimal under $\to$, so that $f \to F$. Then, Theorems 5(i), 6(vi), 11, we have $f \to g \to F$, g almost minimal; and we may choose g to be almost minimal under $\underset{q}{\to}$ for any prime q for which f is not minimal under $\underset{q}{\to}$. Theorem 1 shows that $c(f) = 1$ implies $c(g) = c(F) = 1$; so by Step 2 we have finitely many possibilities for g, f, and f minimal under $\underset{p}{\to}$ for every p that is not among the possibilities for q.

In the references quoted above for Step 1 the notation and results of [1] are used, and so should be related to those of this paper. In [1], f is strongly primitive (SP), if, for every p and some $r \geqslant \frac{1}{2}n$, f has an r-ary section f' with $p \nmid d(f')$. Further, f is square-free (SF) if it is p-adically SF for every p; and the definition of a p-adically SF form implies that f is p-adically SF if and only if $f \to (p, 0) g \to (p, 0) h$ implies $h \sim f$. See [1], p. 584, Lemma 6.

Now f is minimal and normalized under $\to$ if and only if it is SF and SP. When f is minimal under $\to$ but not normalized, it is not necessarily SF (because, see Theorem 10, (9.4) may have a non-zero term $4\psi_3$).

References

[1] G. L. Watson, *Transformations of a quadratic form which do not increase the class-number*, Proc. London Math. Soc. (3) 12 (1962), pp. 577–587.

[2] — *The class-number of a positive quadratic form*, Proc. London Math. Soc. (3) 13 (1963), pp. 549–576.

[3] — *Integral quadratic forms* (Cambridge Tract no. 51), Cambridge 1960.

[4] — *One-class genera of positive ternary quadratic forms*, Mathematika 19 (1972), pp. 96–104.

[5] — *One-class genera of positive quaternary quadratic forms*, Acta Arith. 24 (1974), pp. 461–475.

[6] — *One-class genera of positive quadratic forms in $n > 5$ variables*, Acta Arith., to appear.

UNIVERSITY COLLEGE
London

Received on 23. 6. 1973 (427)