TRANSFORMATIONS OF A QUADRATIC FORM WHICH DO NOT INCREASE THE CLASS-NUMBER

By G. L. WATSON

[Received 20 September 1961]

1. Introduction

THE investigation of the class-number, that is the number of classes in the genus, of a quadratic form with integral coefficients can sometimes be simplified by considering another form with simpler properties. For example, it is well known that reciprocal forms have the same class-number, because equivalent forms have equivalent reciprocals. For another example, see (**1**). Here Jones considered a ternary form $f = f(x_1, x_2, x_3)$ with the property $f \equiv ax_1^2 \pmod{p}$ identically in the variables, where p is prime, $p \nmid 2a$; and showed that the class-number of such an f is not less than that of $g = p^{-1}f(px_1, x_2, x_3)$. This is useful because the discriminant of g is numerically less than that of f. Both these results are included in Theorem 1 of this paper.

Magnus showed in (**3**) that every positive genus of n-ary forms contains at least two classes if $n \geqslant 35$. I shall show, in a paper under preparation, using the results of this paper, that a positive spinor-genus with $n \geqslant 11$ always contains at least two classes. The constant 11 is best possible. The spinor-genus is introduced mainly because it does not seriously complicate the argument; for an account of it see Ch. 7 of (**4**).

The present paper is published separately because the arguments are different from those of the forthcoming one referred to above, and because the results, which seem to be of some interest in themselves, are valid for indefinite as for positive forms. Unfortunately, however, they seem to have no interesting applications as far as indefinite forms are concerned.

The notation is based on that of (**4**), but a somewhat algebraic approach seems desirable, and calls for a number of further definitions and symbols.

2. Definitions and statement of results

For any positive integer n, Λ_n denotes the standard lattice in n-dimensional space; we use the word *lattice* as in the geometry of numbers, not as in abstract algebra. Λ_n will be regarded as consisting of column vectors $\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{t}, \mathbf{x} = \{x_1, \ldots, x_n\}$, with integral elements. Latin capitals will be used to denote n by n nonsingular matrices with integral

Proc. London Math. Soc. (3) 12 (1962) 577–587

elements; the determinants $|T|$, $|U|$ of T, U will be restricted to the values ± 1.

Now let $f = f(x_1, \dots, x_n) = f(\mathbf{x})$ be a quadratic form with integral coefficients (i.e. taking values in Λ_1 for $\mathbf{x}$ in Λ_n). The countable set of all such f will be denoted by $\mathscr{F}(n)$. As in (**4**) we write

$$f(x) = \tfrac{1}{2}\mathbf{x}'A\mathbf{x}, \quad A = A(f) = (\partial^2 f/\partial x_i\, \partial x_j)_{i,j=1,\dots,n}, \tag{2.1}$$

noting that this gives

$$f(\mathbf{x}+\mathbf{y}) = f(\mathbf{x}) + \mathbf{y}'A\mathbf{x} + f(\mathbf{y}), \tag{2.2}$$

and we define the discriminant of f to be

$$d = d(f) = \begin{cases} (-1)^{\frac{1}{2}n}|A| & (n \text{ even}), \\ \tfrac{1}{2}(-1)^{\frac{1}{2}n-\frac{1}{2}}|A| & (n \text{ odd}). \end{cases} \tag{2.3}$$

This makes d a polynomial, with integral coefficients, in the $\frac{1}{2}n(n+1)$ coefficients of f (see (**4**) 3).

The class of f, that is the set of all forms $f^T = f(T\mathbf{x})$ with T as above, will be denoted by (f). We shall denote by $\mathscr{C}(n)$ the set of all (f) with f in $\mathscr{F}(n)$. The genus of f, a definition of which will be given in the proof of Theorem 1, is the union of a finite number, which we shall denote by $\mathscr{N}_{cg}(f)$, of classes. It may also be regarded as the union of $\mathscr{N}_{sg}(f) = 2^\beta$ spinor-genera. Here $\beta = \beta(f)$ is a non-negative integer which is easily calculated by studying the congruence properties of f; see (**4**), loc. cit. The spinor-genus of f, which will be defined in the proof of Theorem 1, is a union of $\mathscr{N}_{cs}(f) \leqslant \mathscr{N}_{cg}(f)$ classes.

We shall study the structure of the set $\mathscr{C}(n)$ by mapping it onto itself, and onto certain proper subsets; under all the mappings the numbers $\mathscr{N}_{cg}, \mathscr{N}_{sg}, \mathscr{N}_{cs}$ are non-increasing, and the signature is invariant. They all depend on the sub-lattice $\Lambda_m(f)$ of Λ_n which we now define.

Let m be a positive integer; the case $m = 1$ is trivial but need not be excluded. Define $\Lambda_m(f)$, for f in $\mathscr{F}(n)$, to be the set of all $\mathbf{x}$ in Λ_n with

$$f(\mathbf{x}+\mathbf{z}) \equiv f(\mathbf{z}) \pmod{m} \quad \text{for all } \mathbf{z} \text{ in } \Lambda_n. \tag{2.4}$$

Trivially, $m|\mathbf{x}$ implies (2.4), so $\Lambda_m(f)$ is n-dimensional; and if $\mathbf{x}, \mathbf{y}$ are both in $\Lambda_m(f)$ then so too is $\mathbf{x}-\mathbf{y}$; so $\Lambda_m(f)$ is a lattice, included in Λ_n and including $m\Lambda_n$. Hence we can choose M (any n-by-n matrix whose column vectors form a basis of $\Lambda_m(f)$) so that $\mathbf{x}$ is in $\Lambda_m(f)$ if and only if $\mathbf{x} = M\mathbf{y}$, $\mathbf{y}$ in Λ_n. If one possible choice of M is $M = M_0$, then all choices are given by $M = M_0 T$, T as above.

Now write

$$g = g_m(f) = m^{-1}f^M, \tag{2.5}$$

i.e. $g(\mathbf{y}) = m^{-1}f(M\mathbf{y})$, and note that, by (2.4) with $\mathbf{z} = \mathbf{0}$, and the choice of M, $m|f(M\mathbf{y})$ for $\mathbf{y}$ in Λ_n, so g is in $\mathscr{F}(n)$. (g) is uniquely determined by m and f; and g can range over the whole of (g), by the remark above regarding the choice of M. (g) is determined by m and (f), because if we replace f by the equivalent f^T we can obviously replace M by $T^{-1}M$, giving the same g. So if we say that the m-mapping is the mapping $(f) \rightarrow (g)$, it is clearly a well-defined mapping of $\mathscr{C}(n)$ into $\mathscr{C}(n)$.

The mapping is onto because, for every f_0 in $\mathscr{F}(n)$, (mf_0) maps into (f_0). (For $f = mf_0$, (2.4) is trivial and we can take M to be I, the n-by-n identity matrix.) The mapping clearly preserves the signature; and g is non-singular if f is so.

In order to define the subsets of $\mathscr{C}(n)$ mentioned above, it is convenient to introduce 0-ary forms, with the convention that $\mathscr{F}(0)$ consists of a single form, which vanishes identically but has discriminant 1.

Now let p be any prime, and consider forms, in $\mathscr{F}(n)$, of the shape

$$f_1(x_1, \dots, x_r) + p\sum_{i=1}^{r}\sum_{j=r+1}^{n} b_{ij}x_i x_j + pf_2(x_{r+1}, \dots, x_n), \tag{2.6}$$

with f_1 in $\mathscr{F}(r)$, f_2 in $\mathscr{F}(n-r)$, and integral b_{ij}. With the convention regarding $\mathscr{F}(0)$, every f in $\mathscr{F}(n)$ is trivially of the shape (2.6), with $r = n$ and an empty double sum. We may therefore define $r_p(f)$, the *rank modulo p* of f, or of (f), to be the least r for which (f) contains a form of the shape (2.6). We shall say that f, or (f), is *strongly primitive* if f is in $\mathscr{F}(n)$ and

$$r_p(f) \geqslant \tfrac{1}{2}n \quad \text{for every prime } p. \tag{2.7}$$

The strongly primitive subsets of $\mathscr{F}(n)$, $\mathscr{C}(n)$ will be denoted by $\mathscr{F}^+(n)$, $\mathscr{C}^+(n)$.

We shall see (Lemma 5) that $r_p(f)$ could alternatively be defined as the greatest r for which f has an r-ary section with discriminant not divisible by p. With this, (2.7) means that f, if strongly primitive, has a section, in $r \geqslant \frac{1}{2}n$ variables, with discriminant prime to $d(f)$.

Next we say that f, or (f), is *p-adically square-free* if (f) contains a form of the shape (2.6) with $p \nmid d(f_1)\,d(f_2)$; and *square-free* if this is so for every p. To explain the terminology, note that, for odd p, the diagonal form $a_1x_1^2 + \dots + a_nx_n^2$ is p-adically square-free if and only if p^2 divides none of the a_i; or see (4.1) below. The square-free subset of $\mathscr{C}(n)$ will be denoted by $\mathscr{Q}(n)$, and the strongly primitive subset of $\mathscr{Q}(n)$ by $\mathscr{Q}^+(n)$.

We now state the five theorems to be proved.

THEOREM 1. *The numbers $\mathscr{N}_{cg}, \mathscr{N}_{sg}, \mathscr{N}_{cs}$ do not increase under the m-mapping, and the rank and signature are invariant.*

(The rank is n if $d \neq 0$, or f is non-singular; we might assume this but it is slightly more convenient not to.)

THEOREM 2. *The modulus of the discriminant does not increase under the square of the m-mapping, under which $\mathscr{Q}(n)$ is invariant, and the r_p do not decrease. Moreover, if the square of the m-mapping takes (f) into (ϕ) then $f = \phi^H$ for some H with integral elements, i.e. ϕ represents f.*

THEOREM 3. *The subset of $\mathscr{C}(n)$ consisting of classes of non-singular forms maps onto $\mathscr{Q}(n)$ by a mapping under which $\mathscr{N}_{cg}, \mathscr{N}_{sg}, \mathscr{N}_{cs}$, and $|d|$ do not increase, the signature is invariant, and the r_p do not decrease. The restriction of this mapping to $\mathscr{Q}(n)$ is the identity, and if it maps (f) into (ϕ) then ϕ represents f.*

(Note that (f) in $\mathscr{Q}(n)$ is necessarily non-singular.)

THEOREM 4. *$\mathscr{Q}(n)$ maps onto $\mathscr{Q}^+(n)$ by a mapping whose restriction to $\mathscr{Q}^+(n)$ is the identity, and which has all the invariant and monotonic properties of Theorem 3. If this mapping takes (f) into (g) then there exist m, positive and square-free, and J, K, with integral elements, such that $JK = mI$, $g = m^{-1}f^J$, and $f = m^{-1}g^K$.*

THEOREM 5. *If (f) is in $\mathscr{Q}(n)$ or in $\mathscr{C}^+(n)$, with $d \neq 0$ and $n \neq 2$, then the genus and spinor-genus of f coincide; that is, $\mathscr{N}_{sg}(f) = 1$ and $\mathscr{N}_{cs}(f) = \mathscr{N}_{cg}(f)$.*

It is known, see (**4**), Theorem 63, that $\mathscr{N}_{cs}(f) = 1$ for f in $\mathscr{F}(n)$ if $n \geqslant 3$ and f is indefinite and non-singular; this is why the application of Theorems 1 to 5 is mainly to positive forms.

We here deal briefly with two points mentioned in the introduction. First take $m = \pm 2|A|$. (2.2) and (2.4) imply $m|A\mathbf{x}$, giving $\mathbf{x} = 2(\operatorname{adj} A)\mathbf{y}$, $\mathbf{y}$ in Λ_n. Conversely it is easily verified that this implies (2.4), so we take $M = 2 \operatorname{adj} A$ in (2.5), giving $g(\mathbf{y}) = \pm \mathbf{y}'(\operatorname{adj} A)\mathbf{y}$, a form clearly reciprocal to f. And by a similar argument we see that (g) maps into (f). The property of reciprocal forms mentioned in the introduction thus follows from Theorem 1.

Next, we note that the special case considered by Jones is essentially that in which (2.4) holds for all $\mathbf{z}$ in Λ_n if it holds for $\mathbf{z} = \mathbf{0}$. For general $f, f(\mathbf{x}) \equiv 0 \pmod{m}$ does not define a lattice, and so Jones's method will not work.

3. Properties of the m-mapping

With the notation of § 2 for n-by-n matrices, we define $P \sim Q$ to mean $P = TQU$ for some T, U, and prove a preliminary lemma.

LEMMA 1. (i) *If $|M| \equiv \pm 1 \pmod{m}$ then $M \equiv T \pmod{m}$ for some T.*

(ii) *For every P we have $P \sim D(P)$, for a unique diagonal $D(P)$ whose diagonal elements are positive integers, each dividing the next.*

(iii) *If $|M|, |P|$ are coprime then $D(PM) = D(M)\,D(P) = D(P)\,D(M)$.*

(iv) *With the hypothesis of* (iii), *$MV = PM$ implies $V \sim P$.*

Proof. (i) See (**4**), proof of Theorem 41.

(ii) See (**2**), Theorem 26.2.

(iii) An easy corollary of the result just quoted.

(iv) $|V| = |P|$ is also prime to $|M|$, so (iii) gives
$$D(P)\,D(M) = D(PM) = D(MV) = D(V)\,D(M), \quad D(P) = D(V), \quad V \sim P.$$

We use Lemma 1 to prove the properties of the m-mapping that we shall need.

LEMMA 2. *With the notation of* (2.4), (2.5), *and Lemma* 1, *let P be a matrix with $|P|$ prime to m, and let the m-mapping take (f) into (g). Then:*

(i) *For suitable f in (f) a diagonal M can be chosen.*

(ii) *There exists N such that $MN = mI$ and $\mathbf{x}$ in Λ_n is in $\Lambda_m(f)$ if and only if $m|N\mathbf{x}$.*

(iii) *If there exists Q with $Q \equiv P \pmod{m}$ and $QM = MQ$ (implying $QN = NQ$) then $\Lambda_m(f^P) = \Lambda_m(f)$.*

(iv) *(f^P) maps into (g^V) for some $V \sim P$; for suitable choice of g in (g), (f^P) maps into (g^P).*

(v) *(f^W) maps into (g^P) for some $W \sim P$; for suitable choice of f in (f), (f^P) maps into (g^P).*

(vi) *For every prime p, $\Lambda_m(f) \supseteq \Lambda_{mp}(f) \supseteq p\Lambda_m(f)$.*

(vii) *If q is a positive integer prime to m then the m-, q-mappings commute and their product is the mq-mapping.*

Proof. (i) It is clear from the definition of the m-mapping that by replacing f, g by equivalent forms f^T, g^U we can replace M by $T^{-1}MU$, which by Lemma 1(ii) is diagonal for some T, U.

(ii) The choice of M is such that $\mathbf{x}$, in Λ_n, is in $\Lambda_m(f)$ if and only if $M^{-1}\mathbf{x}$ is in Λ_n, that is, if and only if $m|mM^{-1}\mathbf{x}$. This must hold whenever $m|\mathbf{x}$, since then (2.4) is trivial.

(iii) From (ii) it is clear that $\Lambda_m(f^P)$ consists of the $\mathbf{x}$ in Λ_n with $m|NP\mathbf{x} \equiv NQ\mathbf{x} = QN\mathbf{x} \equiv PN\mathbf{x} \pmod{m}$; and with m prime to $|P|$ this is the same as $m|N\mathbf{x}$.

(iv) Using (i), we suppose M diagonal, since it clearly makes no difference if we replace f, g by equivalent forms f^T, g^U, and P by the equivalent $T^{-1}PU$. Now choose a diagonal Q with $|Q| \equiv |P| \pmod{m}$, and we clearly have $QM = MQ$ and $P \equiv QR \pmod{m}$, for an R with $|R| \equiv 1 \pmod{m}$.

Using (i) with R for M, $P \equiv QT \pmod{m}$ for some T. Again replacing P by an equivalent matrix, $P \equiv Q \pmod{m}$, $QM = MQ$. Now using (iii), (f^P) maps into $(m^{-1}f^{PM}) = (g^V)$, $V = M^{-1}PM$. V has integral elements because $mV = NPM \equiv NQM = NMQ = mQ \pmod{m}$. Now $MV = PM$ gives $V \sim P$ by Lemma 1(iv). For the second part of (iv), replace g, g^V, V by the equivalent $g^T, g^{VU}, T^{-1}VU$, and choose T, U so that $T^{-1}VU = P$.

(v) The proof is the same as that of (iv). It is not asserted that (f^{W}) is the only class mapping into (g^P); this in general is not the case.

(vi) The first inclusion is trivial. The second means that if (2.4) holds then also $f(p\mathbf{x}+\mathbf{z}) \equiv f(\mathbf{z}) \pmod{mp}$, for all $\mathbf{z}$ in Λ_m. This becomes obvious on using (2.2).

(vii) This is trivial.

We now study the square of the m-mapping. Obviously this involves consideration of the lattice $\mu_m(f)$ of all $\mathbf{x}$ with

$$\mathbf{x} = M\mathbf{y}, \quad \mathbf{y} \text{ in } \Lambda_m(g) = \Lambda_m(m^{-1}f^M). \tag{3.1}$$

Using (2.4), with g for f, and Lemma 2(ii), we can replace (3.1) by $\mathbf{x}$ in Λ_n and

$$m \mid N\mathbf{x}, \quad f(\mathbf{x}+M\mathbf{z}) \equiv f(M\mathbf{z}) \pmod{m^2}, \text{ all } \mathbf{z} \text{ in } \Lambda_n. \tag{3.2}$$

The first of these conditions is implied by the second, with $\mathbf{z} = N\mathbf{t}$, which gives $f(\mathbf{x}+m\mathbf{t}) \equiv 0 \pmod{m^2}$ for all $\mathbf{t}$ in Λ_n, whence $m^2 \mid f(\mathbf{x})$, $m \mid A\mathbf{x}$ using (2.2), these giving (2.4), or $\mathbf{x}$ in $\Lambda_m(f)$. Hence $\mu_m(f)$ is the set of $\mathbf{x}$ in Λ_n with

$$f(\mathbf{x}+\mathbf{t}) \equiv f(\mathbf{t}) \pmod{m^2} \quad \text{for all } \mathbf{t} \text{ in } \Lambda_m(f). \tag{3.3}$$

LEMMA 3. *(i) $m \mid \mathbf{x}$ implies $\mathbf{x}$ in $\mu_m(f)$.*

(ii) If, conversely, $\mathbf{x}$ in $\mu_m(f)$ implies $m \mid \mathbf{x}$, and $p \mid m$, then $\mathbf{x}$ in $\mu_{mp}(f)$ implies $mp \mid \mathbf{x}$.

Proof. (i) Using (2.2), it suffices to show that $\mathbf{t}$ in $\Lambda_m(f)$ implies $m \mid A\mathbf{t}$; but (2.4) with $\mathbf{t}$ for $\mathbf{x}$ gives that m divides $f(\mathbf{t}) + \mathbf{z}'A\mathbf{t}$, for all $\mathbf{z}$ in Λ_n.

(ii) It follows easily from Lemma 2(vi) that $\mu_{mp}(f)$ is included in $\mu_m(f)$, so $\mathbf{x}$ in $\mu_{mp}(f)$ implies $m \mid \mathbf{x}$, hence also $p \mid \mathbf{x}$, by hypothesis. Now we see that $\mu_{mp}(f)$ is the set of $\mathbf{x} = p\mathbf{y}$, with $\mathbf{y}$ satisfying

$$f(p\mathbf{y}+\mathbf{t}) \equiv f(\mathbf{t}) \pmod{m^2p^2} \quad \text{for all } \mathbf{t} \text{ in } \Lambda_{mp}(f). \tag{3.4}$$

We have to show that (3.4) implies $m \mid \mathbf{y}$. It is enough to show that (3.4) implies $m \mid \mathbf{y}$ when it is modified by restricting $\mathbf{t}$ to be in $p\Lambda_m(f)$, which makes it weaker by Lemma 2(vi). So modified, (3.4) becomes

$$f(p\mathbf{y}+p\mathbf{z}) \equiv f(p\mathbf{z}) \pmod{m^2p^2} \quad \text{for all } \mathbf{z} \text{ in } \Lambda_m(f).$$

Comparing this with (3.3), assumed to imply $m \mid \mathbf{x}$, the conclusion $m \mid \mathbf{y}$ follows on cancelling p^2.

4. The p-mapping

We examine the case m prime of the m-mapping more closely.

LEMMA 4. *For f in $\mathscr{F}(n)$, each of the following properties implies the other two:* (i) $\mathbf{x}$ *in* $\Lambda_p(f)$ *does not imply* $p \mid \mathbf{x}$; (ii) $r_p(f) < n$; (iii) $p \mid d(f)$.

Proof. First assume (i); then clearly there is an $\mathbf{x}$ in $\Lambda_p(f)$ whose elements have greatest common divisor 1; so replacing f by an equivalent f^T, with suitable T, which does not affect (ii) or (iii), we may assume that $\{0, \ldots, 0, 1\}$ is in $\Lambda_p(f)$. Looking at (2.4) with $m = p$, and denoting by a_{ij} the coefficient of $x_i x_j$ in f, this tells us that p divides all the a_{in}. Hence f is of the shape (2.6) with $r < n$, and (ii) follows by the definition of $r_p(f)$. (iii) also follows by the remark following (2.3) (each term in the expansion of d clearly has some a_{in} as a factor).

Now we assume (iii) and prove (ii). Using Theorem 35 of (**4**) if $p = 2$, or simply transforming f into an equivalent form congruent modulo p to a diagonal one if $p \neq 2$, we see that for some P with $p \nmid |P|$ we have f^P independent of x_n modulo p, or $r_p(f^P) < n$; $r_p(f) < n$ clearly follows.

We deduce:

LEMMA 5. *For each prime p, every (f) in $\mathscr{C}(n)$ contains an f of the shape*

$$f_1(x_1, \ldots, x_r) + p \sum_{r=1}^{r} \sum_{j=r+1}^{k} b_{ij} x_i x_j + pf_2(x_{r+1}, \ldots, x_k)$$
$$+ p^2 \sum_{i=r+1}^{k} \sum_{j=k+1}^{n} c_{ij} x_i x_j + p^2 f_3(x_{k+1}, \ldots, x_n), \tag{4.1}$$

with integral b_{ij} and c_{ij}, f_1, f_2, f_3 in $\mathscr{F}(r), \mathscr{F}(k-r), \mathscr{F}(n-k)$, and

$$r = r_p(f), \quad p \nmid d(f_1)\, d(f_2). \tag{4.2}$$

Proof. Choose f in (f) of the shape (2.6), with least possible r, that is, with $r = r_p(f)$. Then Lemma 4 shows that there is an f in (f) of the shape (2.6) with smaller r if $p \mid d(f_1)$; so we have $p \nmid d(f_1)$. Apply the same argument to the f_2 of (2.6) and the lemma follows. But to justify the remark following (2.7), regarding an alternative definition of $r_p(f)$, we shall show that $p \nmid d(f_1)$ in (4.1), or in (2.6), implies $r = r_p(f)$.

To see this, note that in (2.4) with $m = p$ we may replace f by $f_1 \equiv f \pmod{p}$. Now Lemma 4 shows that $\mathbf{x}$ in $\Lambda_p(f)$ implies r independent congruence conditions on the x_i, if $p \nmid d(f_1)$. On the other hand, (2.6) or (4.1) with the smallest $r = r_p(f)$ shows trivially that $\mathbf{x}$ in $\Lambda_p(f)$ is implied by $r_p(f)$ such conditions ($p \mid x_i$ for $i = 1, \ldots, r$). Clearly therefore $p \nmid d(f_1)$ implies $r_p(f) \geqslant r$; the converse inequality is trivial by the definition of $r_p(f)$ as the minimal r in (2.6).

From Lemma 5 we deduce:

Lemma 6. *If f is the form (4.1) satisfying (4.2) then the p-mapping takes (f) into (g) and (g) into (ϕ), where*

$$g = p^{-1}f(px_1, \ldots, px_r, x_{r+1}, \ldots, x_n), \tag{4.3}$$

$$r_p(g) = k-r = n-r \text{ if } f \text{ is } p\text{-adically square-free}, \tag{4.4}$$

and

$$\phi = p^{-2}f(px_1, \ldots, px_k, x_{k+1}, \ldots, x_n), \tag{4.5}$$

giving

$$f = \phi(x_1, \ldots, x_k, px_{k+1}, \ldots, px_n), \tag{4.6}$$

and $f \sim \phi$ if f is p-adically square-free.

Proof. Looking at (4.1), with $p \nmid d(f_1)$, and using Lemma 4, we see that $\mathbf{x}$ is in $\Lambda_p(f)$ if and only if $p \mid x_i$ for $i = 1, \ldots, r$; (4.3) follows on putting $m = p, M = [p, \ldots, p, 1, \ldots, 1]$ (a diagonal matrix with r elements p) in (2.5).

(4.1) and (4.3) show that g is of the shape (2.6), with $k-r, f_2$, for r, f_1, $p \nmid d(f_2)$, and with the variables permuted. (4.4) follows. The argument for (4.3) gives

$$\phi = p^{-1}g(x_1, \ldots, x_r, px_{r+1}, \ldots, px_k, x_{k+1}, \ldots, x_n),$$

which with (4.3) gives (4.5), whence (4.6).

5. Proof of Theorem 1

We show first that if (f) is taken into (g) by the m-mapping then $\mathscr{N}_{cg}(f) \geqslant \mathscr{N}_{cg}(g)$, that is that the genus of f contains at least as many classes as that of g. This follows if we prove (i) that to every class (f') in the genus of f there corresponds a unique class (g') in the genus of g, into which the m-mapping takes (f'), and (ii) that conversely, given a class (g') in the genus of g, there exists a class (f') in the genus of f, not necessarily unique, which maps into (g'). We ignore the uniqueness in (i) because it follows from the definition of the m-mapping; thus the proofs of (i), (ii) become similar.

The necessary and sufficient condition for f, f' to be in the same genus, or to be semi-equivalent, in symbols $f \simeq f'$, can be expressed as $f'(\mathbf{x}) = f(h^{-1}P\mathbf{x})$, for some positive integer h and some matrix P (with integral elements) such that $|h^{-1}P| = \pm 1$ and h is prime to $d(f)$ (assumed $\neq 0$; the case $d(f) = 0$ is unimportant and easily dealt with). But if these conditions can be satisfied, then they can still be satisfied if we strengthen the last of them to h prime to $md(f)$, m any positive integer, or to h prime to $md(f)d(g)$. With this (for which see, e.g. Theorem 50 of (**4**)), the conditions for $g \simeq g'$ are of the same shape: we take the m to be the m of the mapping.

Now to prove (i), note that Lemma 2(iv) tells us that by suitable choice of g in (g) we may suppose (f) and $(h^2f')(f', \simeq f, = f(h^{-1}P\mathbf{x})$, with P as above) to map into (g) and (g'') respectively. It follows that (f') maps into (g'), $g' = g(h^{-1}P\mathbf{x}) \simeq g$.

Using Lemma 2(v), (ii) above is proved in the same way. Thus $\mathscr{N}_{cg}$ has been proved not to increase under the mapping.

To prove that $\mathscr{N}_{cs}$ does not increase, we need suitable necessary and sufficient conditions for f, f' (or g, g') to be spinor-related, or in the same spinor-genus. These are just as above (see (184) and (185) of (**4**)) except that one more condition has to be imposed on the rational matrix $h^{-1}P$. The exact nature of this further condition is not important, since it is the same for f as for g; it can be expressed as $h^{-1}D(P) = (h^{-1}Q)^2$, for some Q with integral elements. This disposes of $\mathscr{N}_{cs}$.

To see that $\mathscr{N}_{sg}$ does not increase, we apply the argument above for $\mathscr{N}_{cg}$ to a set of classes in the genus of g containing one representative of each spinor-genus in the genus of g.

The assertions regarding the rank and signature being trivial, the theorem is proved.

6. Proofs of Theorems 2 to 5

Proof of Theorem 2. Suppose that the m-mapping takes (f) into (g), and (g) into (ϕ). Then Lemma 3 shows that $\phi = m^{-2}f^K$, for any K whose column vectors form a basis of the lattice $\mu_m(f)$ of that lemma. From Lemma 3(i) it follows, cf. Lemma 2(ii), that $H = mK^{-1}$ has integral elements and so $f = \phi^H$. This shows that $|d|$ is non-increasing, and gives the last part of the theorem. Trivially, $r_p(f) = r_p(\phi^H)$ cannot exceed $r_p(\phi)$. It remains therefore only to prove the invariance of $\mathscr{Q}(n)$.

Now the foregoing argument shows that we have $|H| = \pm 1$ and $f \sim \phi$ if and only if the lattice $\mu_m(f)$ is $m\Lambda_n$. We have therefore to prove that this is always the case if (f) is square-free, i.e. in $\mathscr{Q}(n)$. We assume that, for some m, the lattice $\mu_m(f)$ strictly includes $m\Lambda_n$, and deduce that f is not square-free. From Lemma 3(ii) it follows that if $\mu_m(f)$ strictly includes $m\Lambda_n$ for some m, say $m'p^2$, which is not square-free then $\mu_m(f)$ also includes $m\Lambda_n$ strictly for $m = p^{-1}m = m'p$. It follows therefore that there is a square-free m such that $\mu_m(f)$ includes $m\Lambda_n$ strictly. Clearly therefore, see Lemma 2(vii), there is a prime p such that $\mu_p(f)$ strictly includes $p\Lambda_n$. By Lemma 6 this shows that f is not p-adically square-free, hence not square-free.

Proof of Theorem 3. We construct the mapping of this theorem by applying the m_1-mapping twice, then the m_2-mapping twice, ..., for suitably chosen $m_1, m_2, \ldots$, all square-free. We choose m_1 so that the first two operations give (f_1) with $|d(f_1)| = |H|^{-2}|d(f)| < |d(f)|$, if possible. The proof of

Theorem 2 shows that this is possible unless f is square-free; in that case (f) maps into itself, and the set $(m_1, m_2, \ldots)$ may be taken to be empty. We choose m_2 similarly; the construction terminates since the strictly decreasing sequence $|d(f)|$, $|d(f_1)|$, ... of positive integers cannot be infinite. All the assertions of Theorem 3 now follow from Theorem 2 if only we show that the image class is independent of the choice of $m_1, m_2, \ldots$ (it might not be if we used non-square-free m's).

Now Lemma 2(vii) shows that we have used in effect a finite number of p-mappings, with various values of p each an even number of times; and that the order of these mappings does not matter. The total number does not matter either, because once we have arrived at a square-free class we can add two more mappings, for any m. This completes the proof.

Proof of Theorem 4. The mapping of this theorem is just the m-mapping, but with

$$m = \prod_{r_p(f) < \frac{1}{2}n} p. \tag{6.1}$$

It is of course the identity mapping if the product is empty, that is if (2.7) holds. We break it up into p-mappings, by Lemma 2(vii). We appeal to Lemma 6, with $k = n$ since f is square-free. (4.4) tells us that the p-mapping replaces $r_p(f) < \frac{1}{2}n$ by $n - r_p(f) > \frac{1}{2}n$; trivially, r_q is unaltered for any prime $q \neq p$. Hence the mapping maps $\mathscr{Q}(n)$ onto $\mathscr{Q}^{+}(n)$. To see that $|d|$ does not increase, note that (4.3) gives $|d(g)|/|d(f)| = p^{2r-n} < 1$, for $r = r_p(f) < \frac{1}{2}n$.

All the assertions of Theorem 4 are now clear from Theorem 2.

Proof of Theorem 5. The case $n = 1$ is trivial, so using the hypothesis $n \neq 2$ we may suppose $n \geqslant 3$. The case (f) in $\mathscr{Q}(n)$ follows from the other by Theorem 4. So we suppose (f) to be in $\mathscr{C}^{+}(n)$, with $d \neq 0$.

Suppose now that there are two or more spinor-genera in the genus of f. Then by Theorem 69 of (**4**) there are two possibilities. One is that f has 'bad' congruence properties in relation to some odd prime p; by Theorem 66 of (**4**), the properties in question are certainly not bad enough unless $f(\mathbf{z})f(\mathbf{t})$ ($\mathbf{z}, \mathbf{t}$ in Λ_n) is never a quadratic non-residue modulo p. This, however, cannot be the case if f has a binary section with discriminant not divisible by p; but if it has no such section, then $r_p(f) \leqslant 1 < \frac{1}{2}n$, contradicting (2.7) and showing that (f) is not in $\mathscr{C}^{+}(n)$. The other possibility is that one of $f(\mathbf{z})f(\mathbf{t}) \equiv -3 \pmod 8$, $-1 \pmod 4$ is insoluble. This also leads to a contradiction; the theorem follows.

7. Conclusion

The application of the present results depends on investigating the properties of a genus in $\mathscr{Q}^{+}(n)$. One of these is that the genus contains a

disjoint form which is a sum of forms, each in at most eight variables, no two of which have a variable in common. Another is that the genus of f, (f) in $\mathscr{Q}^{+}(n)$, or in $\mathscr{Q}(n)$, contains a form which represents a given ν-ary form ϕ, in $\mathscr{F}(\nu)$, $\nu \leqslant n-3$, $\nu < \min\limits_{p} r_p(f)$, provided only that the signatures of f, ϕ are such that f represents ϕ over the real field. These are two properties which, in certain cases, could not be possessed by the same class in the genus; whence my improvement on Magnus's result mentioned in the Introduction. It simplifies the proofs of these results to consider only the positive case for which they are of most interest. Accordingly I include them in the forthcoming paper referred to above.

REFERENCES

1. BURTON W. JONES, 'An extension of Meyer's theorem on indefinite ternary quadratic forms', *Canadian J. Math.* 4 (1952) 120–8.
2. C. C. MACDUFFEE, *The theory of matrices* (Ergebnisse der Mathematik, New York, 1946).
3. W. MAGNUS, 'Über die Anzahl derin einem Geschlecht enthaltenen Klassen von positiv-definiten quadratischen Formen', *Math. Ann.* 114 (1937) 465–75.
4. G. L. WATSON, *Integral quadratic forms* (Cambridge Tract no. 51, Cambridge, 1960).

University College
London