ON THE ORDER INVARIANTS OF INTEGRAL QUADRATIC FORMS

By GORDON PALL (*Montreal*)

[Received 27 March 1934]

SMITH† and Minkowski† laid the foundations of an arithmetical theory of quadratic forms in their definitions of orders and genera of quadratic forms. In this paper we are concerned with those invariants of a quadratic form which characterize its order. We shall see that of Minkowski's invariants $(o_1,\ldots, o_{n-1};\ \sigma_1,\ldots, \sigma_{n-1})$ the latter $n-1$ are quite superfluous, after a modification in the definition of the former. In Smith's terminology, it is no longer necessary to distinguish specifically between properly and improperly primitive forms.

For purposes of arithmetical theory the use of Kronecker's binary forms $ax^2+bxy+cy^2$ and discriminants b^2-4ac has conduced to greater simplicity than the restriction to Gauss's forms $ax^2+2bxy+cy^2$ and determinants $ac-b^2$ or b^2-ac. The following developments seem to lead to a corresponding advancement in the theory of quadratic forms in several variables.

1. The matrix and discriminant of a quadratic form. Any quadratic form f in s variables with integral coefficients may be written as

$$f(x_1,\ldots,x_s)=\sum_{i,j=1}^{s} a_{ij}x_ix_j \qquad (a_{ij}=a_{ji}), \tag{1}$$

where the *coefficients* a_{ii} and $2a_{ij}$ $(i\neq j)$ are integers. The matrix of f is the matrix (a_{ij}); the determinant $|a_{ij}|$ of f will be assumed (throughout this paper) to be not zero. The *discriminant* d of f is, by definition, the determinant multiplied by

$$(-)^{s/2}2^s \quad \text{if } s \text{ is even}, \qquad (-)^{(s-1)/2}2^{s-1} \quad \text{if } s \text{ is odd}. \tag{2}$$

That a discriminant is an integer if s is odd, and is an integer congruent to 0 or 1 (mod 4) if s is even, is a corollary of the following lemma.

† The contents of this paper are cognate with the following: H. J. S. Smith, *Collected Mathematical Papers*, i. 412–15, 510–12, and ii. 623–36; H. Minkowski, *Gesammelte Abhandlungen*, i. 4–6, 8–33, 72, 76–9.

LEMMA 1. *Let $k \geqslant 1$; let e_{ij} $(i,j = 1,\ldots,k)$ be integers such that e_{ii} is even and $e_{ij} = e_{ji}$ for all values of i and j. Then the determinant $|e_{ij}|$ is always even if k is odd, and is congruent to 0 or $(-1)^{k/2}$ (mod 4) if k is even.*

For consider the expansion of $|e_{ij}| = \sum (\pm)e_{1q}\ldots e_{kr}$. With each term $\tau = (\pm)e_{1q}\ldots e_{kr}$ let us associate the transpose term $\tau^* = (\pm)e_{q1}\ldots e_{rk}$ which is equal to τ. Now τ may be its own transpose; but, if k is odd, this happens only if τ contains some factor e_{ii} whence τ is even; and, if k is even, τ will contain an even number of such factors. Hence, if k is even,

$$|e_{ij}| \equiv (-)^{k/2}\{e_{12}e_{34}\ldots e_{k-1,k} + \ldots\}^2 \pmod 4, \tag{3}$$

where the expression in braces is the sum of all algebraically distinct terms $e_{pq}\ldots e_{tr}$ such that all the indices $p, q,\ldots, t, r$ are unequal.

2. Notation. With certain exceptions small Latin letters will connote integers. The exceptions are: f, g represent forms; a_{ij}, b_{ij} denote halves of integers if $i \neq j$. Otherwise the role of the various letters will be defined.

3. Classes of forms. Index. If the transformation

$$x_i = \sum_{j=1}^{s} t_{ij}y_j \qquad (i = 1,\ldots,s) \tag{4}$$

with the matrix $T = (t_{ij})$ carries $f(x_1,\ldots,x_s)$ into

$$g(y_1,\ldots,y_s) = \sum b_{ij}y_iy_j \qquad (b_{ij} = b_{ji}; i,j = 1,\ldots,s), \tag{5}$$

then, representing $(2a_{ij})$ and $(2b_{ij})$ by A and B, we have

$$B = T^*AT, \tag{6}$$

where T^* denotes the transpose of matrix T. We can then say that 'f contains g'.

Let T be unitary, i.e. have determinant 1. Then T^{-1} is unitary, and (6) implies $A = (T^{-1})^*BT^{-1}$. Thus g contains f. If f is transformable into g by a transformation of determinant 1, we say that f and g are equivalent, and write $f \sim g$. The relation of equivalence is reflexive, symmetric, and transitive. All forms equivalent to a given one are equivalent to one another, and constitute a *class of forms*.

The discriminant is an invariant of a class. Another invariant is the *index* (to be denoted by I), defined as follows. Since $d \neq 0$, f can be expressed in the form

$$\alpha_1X_1^2 + \ldots + \alpha_sX_s^2,$$

where the α_i are rational non-zero numbers, and the X_i are linear combinations with rational coefficients of the x_i, the determinant of the X_i being not zero. The number I of negative coefficients α_i in every expression of this type for f is the same, and is called the index of f. The *signature* of f, defined to be $s-2I$, is frequently taken to replace I as an invariant of the class.

4. The g.c.d. of order k. We shall conveniently employ the letter σ to connote a subsequence of k $(1 \leqslant k \leqslant s)$ elements of $(1, 2, \ldots, s)$, that is, a sequence of the type $(i_1, i_2, \ldots, i_k)$ $(1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant s)$. The minor determinant of a matrix C formed by the elements at the intersections of rows $i_1, i_2, \ldots, i_k$ and columns $j_1, j_2, \ldots, j_k$ will be denoted by $C[\sigma_1 \sigma_2]$, where $\sigma_1 = (i_1, \ldots, i_k)$ and $\sigma_2 = (j_1, \ldots, j_k)$.

From the equation (6) we have, by a simple property of determinants,

$$B[\sigma_1 \sigma_2] = \sum_{\sigma,\sigma'} A[\sigma\sigma'] T[\sigma\sigma_1] T[\sigma'\sigma_2] \tag{7}$$

summed for all subsequences σ, σ'. Since $C[\sigma\sigma'] = C[\sigma'\sigma]$ ($C = A$ or B), the g.c.d. of all the $A[\sigma\sigma]$ and $2A[\sigma\sigma']$ is a divisor of every

$$B[\sigma\sigma] \quad \text{and} \quad 2B[\sigma\sigma']. \tag{8}$$

The g.c.d. of order k of f is defined as follows, and is denoted by d_k $(k = 1, \ldots, s)$. Let $A = (2a_{ij})$, and, with Lemma 1 in mind, write $\mu_k = 1$ or 2 according as k is even or odd. Then $\mu_k d_k$ is the g.c.d. of all the principal minors and doubles of the secondary minors of order k in A:

$$\mu_k d_k \text{ is the g.c.d. of all the } A[\sigma\sigma] \text{ and } 2A[\sigma\sigma']. \tag{9}$$

For example, d_1 is the g.c.d. of the actual coefficients a_{ii}, $2a_{ij}$ of f. Since $d_s > 0$, the discriminant is equal to

$$d = (-)^{[s/2]-I} d_s. \tag{10}$$

For future expediency we shall define

$$d_{-1} = 0, \qquad d_0 = 1, \qquad d_{s+1} = 0. \tag{11}$$

If $f \sim g$, A and B may be interchanged in (8). *The* g.c.d.'s d_k *are invariants of a class.*

We call d_1 the *divisor* of f or of its class. If $d_1 = 1$, the form and class are called primitive; if d_1 is prime to N, they are *primitive to modulus* N. The form f/d_1 is primitive, and f is said to be *derived* therefrom.

5. The o-invariants of f. Definition of order. For odd primes p it is plain that if $p^n|d_{k-1}$ then $p^n|d_k$. This is proved in § 8 for $p = 2$. Hence

$$d_{k-1}|d_k \qquad (1 \leqslant k \leqslant s+1).$$

The following two theorems are also established in § 8.

THEOREM 1. *Each of the numbers o_k defined by*

$$o_k = \frac{4\mu_{k+1}d_{k+1}\mu_{k-1}d_{k-1}}{(\mu_k d_k)^2} = 4^{1+(-1)^k}\frac{d_{k+1}d_{k-1}}{d_k^2} \qquad (k = 0,\ldots,s), \quad (12)$$

is an integer. Further:

$$o_k \not\equiv 2 \pmod 4 \qquad (k = 0,\ldots,s). \quad (13)$$

If any o_k $(1 \leqslant k \leqslant s-1)$ is odd, then $o_{k-1} \equiv o_{k+1} \equiv 0 \pmod{16}$.

Thus $o_0 = 0 = o_s$, $o_1 = d_2/d_1^2$. As here defined, $o_1,\ldots,o_{s-1}$ are positive.

These o_k, together with d_1, will be chosen to replace the d_k as invariants of a class, and may be called the o-invariants. All forms or classes in s variables with the same index I, the same divisor d_1, and the same system of invariants $o_1,\ldots,o_{s-1}$ constitute an *order*.

The g.c.d.'s d_k are given in terms of the o_k by the equations

$$\frac{d_{k+1}}{d_1^{k+1}} = \frac{o_1^k o_2^{k-1}\ldots o_k}{4^{[k^2/2]}} \qquad (k = 1, 2,\ldots, s-1), \quad (14)$$

d_1 being an arbitrary positive integer.

The greatest common divisor of a set of numbers λa_i $(i = 1,\ldots,n)$, where λ is a real number differing from zero and the a_i are integers, may naturally and without ambiguity be defined to be $|\lambda|D$, where D is the g.c.d. of the a_i. Thus the g.c.d. of order k of the form λf is $\pm\lambda^k d_k$. Observing with a view to (12) that

$$(\lambda^{k+1}\lambda^{k-1})/(\lambda^k)^2 = 1,$$

we see that: *the invariants o_k of λf are the same as those of f.*

5a. Definitions of even, odd, and classical forms. An integral quadratic form f is called *even* or *odd*† according as the primitive form f/d_1 from which f is derived has all its cross-product coefficients even or has at least one of them odd. A form is called *classical* if all its cross-product coefficients are even. The determinant of a classical form is an integer.

† It is appropriate virtually to reverse Smith's use of these terms.

6. The comitant forms f_k and F_k. Let f be a form (1). Employ the notations of § 4. The form f_k in the ${}_sC_k$ variables ξ_σ defined by

$$\mu_k f_k(\xi) = \sum_{\sigma,\sigma'} A[\sigma\sigma']\xi_\sigma \xi_{\sigma'} \qquad (k = 1,\ldots,s-1) \tag{15}$$

$$(\mu_k = 1 \quad \text{if } k \text{ is even}, \qquad \mu_k = 2 \quad \text{if } k \text{ is odd})$$

is called the kth comitant of f. The divisor of f_k is d_k: cf. (9). Also $f_1 = f$. By § 8, we have

THEOREM 2. *The form f_k is even or odd according as o_k is even or odd.*

Let us write

$$(-)_\sigma = 1 \text{ or } -1 \text{ according as the sum of the elements in } \sigma \text{ is even or odd.} \tag{16}$$

Replacing every ξ_σ in $f_k(\xi)$ by $(-)_\sigma \xi_\sigma$ yields a new form $\bar{f}_k$ differing from f_k only in the signs of certain secondary coefficients. The forms

$$F_k = \bar{f}_k/d_k \qquad (k = 1,\ldots,s-1) \tag{17}$$

are called the *primitive comitants* of f. The $(s-1)$th primitive comitant F_{s-1} is called the *reciprocal* of f/d_1.

6a. Reciprocal orders. (§ 6a is not used in proving Theorems 1 and 2.)

The form $\phi = \bar{f}_{s-1} = d_{s-1}F_{s-1}$ is the contravariant of f. We have

$$\mu_{s-1}\phi(x_1,\ldots,x_s) = \sum_1^s A_{ij}x_i x_j,$$

where A_{ij} denotes the cofactor of $2a_{ij}$ in $(2a_{ij})$. Write $E = (A_{ij})$. Let τ and τ' denote subsequences of $s-k$ elements of $(1, 2,\ldots, s)$, and σ and σ' the conjugate subsequences consisting of the remaining k elements $(k = 1,\ldots,s-1)$. Then by a simple property of determinants

$$E[\sigma\sigma'] = |2a_{ij}|^{k-1}(-)_\tau(-)_{\tau'}A[\tau\tau'].$$

Hence, if s is even, the kth comitant of ϕ is seen to be

$$\phi_k = (-)^{s(k-1)/2}d^{k-1}\bar{f}_{s-k}, \tag{A}$$

where d is the discriminant of f, i.e. $d = (-)^{s/2}|2a_{ij}|$. If s is odd, the kth comitant of $\frac{1}{4}\phi$ reduces similarly to

$$(\tfrac{1}{4}\phi)_k = \mu_k^{-2}(-)^{(s-1)(k-1)/2}d^{k-1}\bar{f}_{s-k}. \tag{B}$$

From (A) and (B) we can easily write down the divisors of ϕ_k and $(\frac{1}{4}\phi)_k$. Let o_k' (temporarily) have the same significance for ϕ (and hence, by the end of § 5, for $\frac{1}{4}\phi$) as o_k has for f. Substituting for the various g.c.d.'s in (12) we immediately find that

$$o_k' = o_{s-k} \qquad (k = 1,\ldots,s-1). \tag{18}$$

If a form f has index I its reciprocal has index I', where

$$I' = I \quad \text{if } s \text{ is even}, \qquad I' = s-I \quad \text{if } s \text{ is odd}. \tag{18'}$$

If f belongs to the order $(d_1 = 1;\ I;\ o_1,\dots,o_{s-1})$, its reciprocal belongs to the order $(1;\ I';\ o_{s-1},\dots,o_1)$. By (A) and (B) with $k = s-1$, f/d_1 is the reciprocal of F_{s-1}. The primitive orders $(1;\ I;\ o_1,\dots,o_{s-1})$ and $(1;\ I';\ o_{s-1},\dots,o_1)$ are called *reciprocal orders*. The kth primitive comitant of F_{s-1} is f_{s-k}/d_{s-k} $(k = 1,\dots,s-1)$.

7. Canonical forms of f to modulus p^t. In studying the properties of the minors of A, to modulus N, it is expedient to transform f into a simple equivalent form, to modulus N. Two forms f and g of type (1) are said to be *equivalent, to modulus N*, if there exists in the class of f a form whose coefficients are congruent, to modulus N, to the corresponding coefficients of g. Equivalence, to modulus N, is reflexive, symmetric, and transitive.

LEMMA 2. *Let $s \geqslant 2$, f being a form (1). Let t be positive, p an odd prime. Then f is equivalent, to modulus p^t, to a form g of the type*

$$g(y_1,\dots,y_s) = p^{\alpha_1}m_1y_1^2+p^{\alpha_2}m_2y_2^2+\dots+p^{\alpha_s}m_sy_s^2 \qquad (0 \leqslant \alpha_1 \leqslant \alpha_2 \leqslant \dots \leqslant \alpha_s), \tag{19}$$

the α_i being integers, and the m_i prime to p.

LEMMA 3. *Let $s \geqslant 2$, $t > 0$. Then f is equivalent, to modulus 2^t, to a form g of the type*

$$\begin{aligned} g(y_1,\dots,y_s) = {} & 2^{\beta_1}m_1y_1^2+\dots+2^{\beta_u}m_uy_u^2+ \\ & +2^{\gamma_1}(n_1y_{u+1}^2+m^{(1)}y_{u+1}y_{u+2}+n_2y_{u+2}^2)+\dots+ \\ & +2^{\gamma_v}(n_{2v-1}y_{s-1}^2+m^{(v)}y_{s-1}y_s+n_{2v}y_s^2), \end{aligned} \tag{20}$$

where (a) the β_i and γ_j are non-negative integers, the m_i and $m^{(j)}$ are odd, and $s = u+2v$, $u \geqslant 0$, $v \geqslant 0$;

(b) the $m^{(j)}$ may be taken to be arbitrary odd integers, and $n_1, n_3,\dots, n_{2v-1}$ to be odd;

(c) for no i and j is a β_i+1 equal to a γ_j.

In proving these lemmas we shall assume without loss of generality that f is primitive to modulus p (greater than or equal to 2 respectively), i.e. at least one of the integers a_{ii} and $2a_{ij}$ is prime to p.

In the case $p = 2$ and f even, at least one of the a_{ii} is prime to p. In the case $p > 2$ and every a_{ii} divisible by p, some $2a_{jk}$ is prime to p; we apply then the unitary transformation

$$S_{jk}: \qquad x_k = y_j+y_k, \quad x_l = y_l \qquad (l \neq k), \tag{21}$$

which replaces a_{jj} by $a_{jj}+2a_{jk}+a_{kk}$, which is prime to p. In view of the unitary transformation P_{1i}, where P_{ki} is

$$P_{ki}: \qquad x_k = y_i, \quad x_i = -y_k, \quad x_l = y_l \qquad (l \neq i, k), \tag{22}$$

we may assume a_{11} prime to p.

Suppose in (1) that a_{11} is prime to p. The transformation

$$x_1 = y_1+h_2y_2+\ldots+h_sy_s, \qquad x_l = y_l \quad (l \geqslant 2), \tag{23}$$

carries f into g with a_{11} as the coefficient of y_1^2 and with

$$b_{1l} = 2a_{1l}+2a_{11}h_l$$

as the coefficients of y_1y_l $(l = 2,\ldots,s)$. The h_l can be chosen to make each b_{1l} divisible by p^t, except when $p = 2$ and f is odd. Thus

$$g(y_1,\ldots,y_s) \equiv a_{11}y_1^2+p^\alpha g'(y_2,\ldots,y_s) \pmod{p^t}, \tag{24}$$

where g' is primitive to modulus p, and α is an integer $\geqslant 0$.

Even if f is odd and $p = 2$, f may be equivalent to a form of type (24). At any rate in view of transformation (22) we may assume $2a_{12}$ odd. We apply then the unitary transformation

$$\begin{aligned} x_1 &= y_1+h_2y_2+\ldots+h_sy_s, \\ x_2 &= y_2+k_3y_3+\ldots+k_sy_s, \qquad x_l = y_l \quad (l \geqslant 3). \end{aligned} \tag{25}$$

This yields a form g in which the coefficient of y_1y_2 is $2a_{11}h_2+2a_{12}$ and is odd; and the coefficients of y_1y_l and y_2y_l $(l \geqslant 3)$ are respectively

$$b_{1l} = 2a_{11}h_l+2a_{12}k_l+2a_{1l}$$

and

$$b_{2l} = b_{1l}h_2+2a_{12}h_l+2a_{22}k_l+2a_{2l}.$$

Now the congruences

$$\left.\begin{aligned} 2a_{11}h_l+2a_{12}k_l &\equiv -2a_{1l} \\ 2a_{12}h_l+2a_{22}k_l &\equiv -2a_{2l} \end{aligned}\right\} \pmod{2^t}$$

are solvable simultaneously for h_l and k_l, the determinant $4a_{11}a_{22}-(2a_{12})^2$ being odd. Thus

$$g(y_1,\ldots,y_s) \equiv n_1y_1^2+my_1y_2+n_2y_2^2+2^\alpha g''(y_3,\ldots,y_s) \pmod{2^t},$$

where m is odd and the notations are self-explanatory.

It is clear how Lemmas 2 and 3 (a) follow by repeated applications of these results. Lemma 3 (b) is a corollary of the following result.

LEMMA 4. *Let m be odd, n_1, n_2 be integral, and t be positive. Then $n_1x_1^2+mx_1x_2+n_2x_2^2$ is equivalent to a like form in which n_1 is odd and m has any desired odd residue, to modulus 2^t.*†

† It should be noted that then n_2 is odd or even according as the discriminant $m^2-4n_1n_2$ is congruent to 5 or 1 (mod 8).

If n_1 is not odd, but n_2 is odd, we employ P_{12}; if n_2 is even also, we employ S_{12}. Suppose n_1 to be odd. By the unitary transformation $x_1 = y_1+hy_2$, $x_2 = y_2$, m goes into $m' = m+2hn_1$, and h may be chosen to give m' any desired odd residue, to modulus 2^t.

To prove Lemma 3 (*c*) we have

LEMMA 5. *Let m, m' be odd, n_1, n_2 be integral, and t be positive. The form $mx_1^2+2(n_1x_2^2+m'x_2x_3+n_2x_3^2)$ is equivalent, to modulus 2^t, to a form*

$$m_1y_1^2+m_2y_2^2+m_3y_3^2 \tag{26}$$

in which m_1, m_2, m_3 are odd.

Replacing x_2 by y_2+y_1, x_1 by y_1, x_3 by y_3, we obtain

$$m_1y_1^2+2n_1y_1y_2+2m'y_1y_3+2n_1y_2^2+2m'y_2y_3+2n_2y_3^2,$$

where $m_1 = m+2n_1$ is odd. Now write

$$y_1 = z_1+h_2z_2+h_3z_3, \qquad y_2 = z_2, \qquad y_3 = z_3.$$

The coefficients $2m_1h_2+2n_1$ and $2m_1h_3+2m'$ of z_1z_2 and z_1z_3 can be made divisible by 2^t by choice of an odd h_3 and an integral h_2. The new form is congruent, to modulus 2^t, to $m_1z_1^2+\delta$, where δ is a binary form in z_2, z_3 in which the coefficient of z_3^2 is odd and that of z_2z_3 is even.

After arranging the s numbers

$$\beta_1+1, \beta_2+1, \ldots, \beta_u+1, \qquad \gamma_1, \gamma_1, \gamma_2, \gamma_2, \ldots, \gamma_v, \gamma_v, \tag{27}$$

where no β_i+1 is equal to any γ_j, in order of magnitude, we denote them by $\alpha_1, \alpha_2, \ldots, \alpha_s$. Thus $\alpha_1 \leqslant \alpha_2 \leqslant \ldots \leqslant \alpha_s$, and each α_i is either a $\beta+1$ or a γ. Let the number of distinct values among the α_i be q, and arrange them into q sets Σ_r ($r = 1, \ldots, q$) of elements of equal value, thus:

$$\Sigma_1 = (\alpha_1, \alpha_2, \ldots, \alpha_{s_1}), \ \Sigma_2 = (\alpha_{s_1+1}, \ldots, \alpha_{s_2}), \ldots, \ \Sigma_q = (\alpha_{s_{q-1}+1}, \ldots, \alpha_s). \tag{28}$$

We may write $s_0 = 0$, $s_q = s$.

The variables y_i in (20) may be rearranged accordingly: thus with each Σ_r there is associated a form $2^{e_r}\psi_r$ in the variables y_k ($k = s_{r-1}+1, \ldots, s_r$), where e_r+1 is the constant value of the elements of Σ_r. If these elements are of type $\beta+1$,

$$\psi_r(\ldots, y_k, \ldots) = \sum_k m_k y_k^2,$$

where the m_k are odd. But if the elements are of type γ, s_r-s_{r-1} is necessarily even, say $s_r-s_{r-1} = 2h$, and

$$\psi_r(\ldots, y_k, \ldots) = 2\phi_1+2\phi_2+\ldots+2\phi_h,$$

where the ϕ_j are odd binary quadratic forms of the type in Lemma 4, in the successive pairs of variables y_k. By Lemma 3, every f is equivalent, to modulus 2^t, to a canonical form of the type

$$\phi = 2^{e_1}\psi_1 + 2^{e_2}\psi_2 + \ldots + 2^{e_q}\psi_q. \tag{29}$$

These results should be expressed in a form analogous to Lemma 2:

LEMMA 6. *Let $t > 0$. Any classical, integral quadratic form in s variables is equivalent, to modulus 2^t, to a form of the type* (29), *where $\psi_1, \ldots, \psi_q$ are classical, integral quadratic forms, each in variables different from those of the remaining forms, and each of odd determinant; and the e_r are integers* $(0 \leqslant e_1 < e_2 < \ldots < e_q)$.

LEMMA 7. *Let $t > 0$. Let ψ be a classical, integral quadratic form in ν variables, of odd determinant. Then, if ψ is even, ψ is equivalent, to modulus 2^t, to a form of the type*

$$m_1 x_1^2 + m_2 x_2^2 + \ldots + m_\nu x_\nu^2, \tag{30'}$$

where the m_i are odd integers. If ψ is odd, then ν is even, say $\nu = 2r$, and ψ is equivalent, to modulus 2^t, to a form of the type

$$2(m_1 x_1^2 + m^{(1)} x_1 x_2 + n_1 x_2^2) + \ldots + 2(m_r x_{\nu-1}^2 + m^{(r)} x_{\nu-1} x_\nu + n_r x_\nu^2), \tag{30''}$$

where the m_i are odd integers, the n_i are integers, and the $m^{(i)}$ are arbitrary odd integers.

A canonical form, (19) if $p > 2$, and (29) if $p = 2$, of f is called a *principal residue of f to modulus p^t*.

In connexion with (29) it is useful to define

$$\left.\begin{aligned} \theta_k = 0, &\text{ if } \alpha_k \text{ is a } \beta+1 \\ 1, &\text{ if } \alpha_k \text{ is an initial } \gamma \\ -1, &\text{ if } \alpha_k \text{ is a terminal } \gamma \end{aligned}\right\}. \tag{31}$$

An *initial* γ denotes a term α_k of type γ occupying an odd place of its set Σ_r in (28), that is, for which $s_{r-1} < k \leqslant s_r$ and $k - s_{r-1}$ is odd; a *terminal* γ occupies an even place. An initial $\gamma = \alpha_k$ and its succeeding terminal $\gamma = \alpha_{k+1}$ may be called *twins*.

With each pair of twin terms α_k, α_{k+1} of type γ is associated a matrix

$$\begin{pmatrix} a & b \\ b & c \end{pmatrix}, \tag{32}$$

where $\gamma = \alpha_k = \alpha_{k+1}$, $a = 2^{\gamma+1}m$, $b = 2^\gamma m'$, $c = 2^{\gamma+1}n$, m and m' being odd, n integral. If ϕ is a principal residue of f, to modulus 2^t, the matrix of 2ϕ consists of a series of single terms $2^{\beta+1}m_k$ $(\alpha_k = \beta+1)$ and binary matrices (32) situated along and symmetric with the

principal diagonal, all remaining elements being zero. Further, $\alpha_1,\ldots,\alpha_s$ are in order of magnitude, and any α_k of type γ is unequal to the nearest preceding and succeeding α's of type $\beta+1$. It should be noted that $ac-b^2 = 2^{\alpha_k+\alpha_{k+1}}M$, where $M = 4mn-m'^2$ is odd.

8. Proof of Theorems 1 and 2. With Minkowski let us denote the exponent of the power of p dividing d_k by $\partial_k = \partial_k(p)$. By (11), $\partial_0 = 0$. Forms which are equivalent, to modulus p^t, for a sufficiently large t have the same values ∂_k. It will suffice to have $t > \alpha_s$ in (19) and (29).

(i) $p > 2$. By (19) we have

$$\partial_i = \alpha_1+\alpha_2+\ldots+\alpha_i \qquad (i = 1,\ldots,s).$$

Hence $\partial_k \geqslant \partial_{k-1}$. The numbers ω_k defined, when $p > 2$, by

$$\omega_k = (\partial_{k+1}-\partial_k)-(\partial_k-\partial_{k-1}) \qquad (k = 1,\ldots,s-1), \tag{33}$$

are also positive or zero, since in fact

$$\omega_k = \alpha_{k+1}-\alpha_k. \tag{34}$$

Plainly, ω_k is the exponent of the power of p dividing o_k in (12).

(ii) $p = 2$. The exponent of the power of 2 dividing o_k is

$$\omega_k = \partial_{k+1}-2\partial_k+\partial_{k-1}+2\{1+(-1)^k\} \qquad (k = 1,\ldots,s-1). \tag{35}$$

Let us write

$$\rho_k = \alpha_1+\alpha_2+\ldots+\alpha_k, \tag{36}$$

$$\epsilon_k = 0, \text{ if } \alpha_k \text{ is a } \beta+1 \text{ or a terminal } \gamma,$$
$$= 1, \text{ if } \alpha_k \text{ is an initial } \gamma. \tag{37}$$

Hence, by (31), $\theta_k = \epsilon_k-\epsilon_{k-1}$.

By the sequel to (32), the exponent of the power of 2 dividing the leading principal minor determinant of order k (in the matrix of 2ϕ) is $\rho_k+\epsilon_k$, and this is the greatest power of 2 dividing all the principal minor determinants of order k. Further, the exponent of the greatest power of 2 dividing the doubles of all the secondary minors of order k is never less than ρ_k+1, and is ρ_k+1 if α_k is an initial γ. Consequently we have

$$\mu_k 2^{\partial_k} = 2^{\rho_k+\epsilon_k}, \tag{38}$$

$$f_k \text{ is odd or even according as } \epsilon_k = 1 \text{ or } \epsilon_k = 0. \tag{39}$$

Hence, at once, by (9), (38), (36), and (37),

$$\partial_{k+1}-\partial_k = \alpha_{k+1}-(-1)^k+\theta_{k+1} \qquad (k = 0,1,\ldots,s-1). \tag{40}$$

Except possibly when $\alpha_{k+1} = 0$ or 1 and $\theta_{k+1} = -1$, it is now obvious that $\partial_{k+1}-\partial_k \geqslant 0$. This is true even in that case, for then α_{k+1} is of type γ and equal to α_1, whence k is odd.

Finally, by (35) and (40),

$$\omega_k = \alpha_{k+1} - \alpha_k + 2 + \theta_{k+1} - \theta_k. \tag{41}$$

Since $\alpha_{k+1} \geqslant \alpha_k$, and, by (31),

$$\left.\begin{aligned} \omega_k = 0, \quad &\text{if and only if } \alpha_k \text{ is an initial } \gamma, \\ &\text{i.e. if and only if } \epsilon_k = 1, \\ &\text{i.e. if and only if } f_k \text{ is odd.} \end{aligned}\right\} \tag{42}$$

This completes Theorem 2. Also, for $k = 1,\ldots,s-1$, (41) yields

$$\left.\begin{aligned} &\omega_k = 0 \quad \text{or} \quad \omega_k \geqslant 2; \\ \text{if } \omega_k = 0, \quad &\text{then } \omega_{k-1} \geqslant 4 \ (k \geqslant 2), \qquad \omega_{k+1} \geqslant 4 \ (k \leqslant s-2). \end{aligned}\right\} \tag{43}$$

These facts involve Theorem 1.

Corresponding to (31) we now have the following values for θ_k:

$$\left.\begin{aligned} \theta_k &= -1, \text{ if } \omega_{k-1} = 0, \\ &= 1, \quad \text{if } \omega_k = 0, \\ &= 0 \quad \text{otherwise} \end{aligned}\right\} \quad (k = 1,\ldots,s-1). \tag{44}$$

We can thereby determine $\alpha_1,\ldots,\alpha_s$ and the type $\beta+1$ or γ of each α_i, uniquely in terms of ∂_1 and $\omega_1,\ldots,\omega_{s-1}$. For we have

$$\alpha_k = \omega_1 + \ldots + \omega_{k-1} - 2k - \theta_k + 3 + \partial_1, \tag{45}$$

α_k is of type γ, if and only if $\omega_k = 0$ or $\omega_{k-1} = 0$. (46)

8 a. The correspondence with the Minkowski-Smith invariants. By (41), $\alpha_{k+1} = \alpha_k$, if and only if

$$\omega_k = 2; \quad \text{or } \omega_k = 0; \quad \text{or } \omega_{k-1} = 0, \quad \omega_k = 4, \quad \omega_{k+1} = 0. \tag{47}$$

Thus α_{k+1} is the first element of its set Σ_r in (28), only for the values k not satisfying (47).

It is to be observed that the classical Minkowski's o_k and Smith's I_k, which are identical and which we denote temporarily by Smith's notation I_k, are related to ours by the equation

$$o_k = 4\sigma_{k-1} I_k \sigma_{k+1} / \sigma_k^2 \tag{48}$$

where σ_k is 1 or 2 according as o_k (or f_k) is even or odd. It is easily verified by use of (13) that the cases (47) are precisely those in which I_k is odd.

9. A special condition if o_1, o_3,..., o_{s-1} are odd, s even. Let o_1, o_3,..., o_{s-1} be odd, s even, whence, in (20), $s = 2v$, $u = 0$. We may suppose $d_1 = 1$. Then (29) is of the type

$$g = \psi_1 + 2^{\alpha_3}\psi_3 + 2^{\alpha_5}\psi_5 + \ldots + 2^{\alpha_{2v-1}}\psi_{2v-1}, \tag{49}$$

where each ψ_i is an odd, primitive binary quadratic form in the variables y_i, y_{i+1}. By (10) and (14) the determinant of $2g$ is of the form

$$(-)^I o_1 o_3 \dots o_{s-1} 2^\lambda (8M+1),$$

where λ and M are non-negative integers. But the product of the determinants of the $2\psi_i$ is the product of $\frac{1}{2}s$ numbers of the form $4n-1$. Since the modulus 2^t can be taken arbitrarily large, we must have

$$(-)^{(s-2I)/2} o_1 o_3 \dots o_{s-1} \equiv 1 \pmod 4. \tag{50}$$

THEOREM 3. *The condition* (50) *is satisfied by the signature* $s-2I$ *of any order of forms* (1) *in which* s *is even and* o_1, o_3,..., o_{s-1} *are odd.*

10. Necessary and sufficient conditions on $(1, I; o_1, \dots, o_{s-1})$ **for an order to exist.** Smith's enumeration† of the further relations, in addition to (13) and Theorem 3, which the invariants defining an order must satisfy in order that corresponding forms may exist, is incomplete; his specification of certain relations to be satisfied by the generic characters probably covers this omission, but is, of course, complicated to apply. Minkowski's discussion, covering the generic characters, is rather intricate.‡ The relations in question take a distinctive form in our notations. In view of these circumstances we shall now present a direct investigation for the simpler case of an order. The extension to a genus is then in fact more perspicuous.

Analogously to § 4, let

$$\sigma = (1,\dots,k), \quad \sigma' = (1,\dots,k-1,k+1),$$
$$\rho = (1,\dots,k-1), \quad \tau = (1,\dots,k+1) \qquad (0 < k < s).$$

Then we have the identity

$$A[\sigma\sigma]A[\sigma'\sigma'] - A[\sigma\sigma']A[\sigma'\sigma] = A[\rho\rho]A[\tau\tau], \tag{51}$$

for any square matrix A of order s, a well-known relation for a second-order minor in the adjoint of the determinant $A[\tau\tau]$.

Let A be the matrix of $2f$, whence $A[\sigma\sigma'] = A[\sigma'\sigma]$. The leading principal minor determinant of order k, namely, $A[\sigma\sigma]$, is of the form $\mu_k d_k l_k$, where l_k is an integer. In particular, by (10) and (11),

$$l_0 = 1, \qquad l_s = (-1)^I. \tag{52}$$

The sequence of numbers $\qquad l_0, l_1, \dots, l_s \qquad (53)$

forms a *reduced leading chain of minor determinants of* f; l_k is the leading coefficient of F_k $(k = 1,\dots,s-1)$.

† Loc. cit. 512–13. ‡ Loc. cit. 78–9.

We require the following theorem of Minkowski and Smith:

LEMMA 8. *In the class of forms equivalent to f there are forms in whose reduced chain* (53)

$$l_k \text{ is prime to } 2l_{k-1}l_{k+1}o_1o_2\dots o_{s-1} \qquad (k = 1,\dots,s-1). \qquad (54)$$

The proof, which is worth our while to review, is based by Minkowski (whose proof, pp. 21–2, is faulty) on the lemma that if $\phi_1,\dots,\phi_r$ are any r forms in the class of f, and $N_1,\dots,N_r$ are any r non-zero integers which are relatively prime in pairs, then there exists a form ϕ in the class of f such that $\phi \equiv \phi_i \pmod{N_i}$ $(i = 1,\dots,r)$. Smith† gives a satisfactory proof of a more fundamental lemma, from which Minkowski's follows: if a determinant $|t_{ij}| \equiv 1 \pmod{N}$, we can alter the elements t_{ij} by multiples of N to secure a determinant actually equal to 1; the extension to moduli $N_1,\dots,N_r$ relatively prime in pairs is obvious.

Consequently, by Lemmas 2 and 3, there exists in the class of f a form ϕ which is, to modulus $p_j^{n_j}$, a principal residue of f to the same modulus for any number of powers of different primes. Such a form is called a *principal representative*‡ of f to modulus $\prod p_j^{n_j}$. We shall include among the p_j all the primes dividing $2o_1\dots o_{s-1}$, and shall always suppose $n_j > \alpha_s(p_j)$. The latter convention ensures that the leading principal minor determinant of order k in the matrix of 2ϕ is of the form

$$\mu_k p_j^{\bar{\rho}_k(p_j)} m_j,$$

where m_j is prime to p_j, for each j; hence it is of the form $\mu_k d_k l_k$, where l_k is prime to all the p_j.

It remains to secure that l_k be prime to l_{k-1}. Minkowski's treatment at this point (p. 72) seems to be not quite complete, but is supplemented by Bachmann.§ We have $l_s = \pm 1$. If k is the largest integer for which l_k is not prime to l_{k-1}, consider

$$\psi(x_1,\dots,x_k) = \phi(x_1,\dots,x_k,0,\dots,0).$$

Then $d_1,\dots,d_{k-1}$ are the same for ψ as for ϕ, but $d_k(\psi) = \pm d_k l_k$. If we apply to f any unitary transformation T leaving $x_{k+1},\dots,x_s$ unaltered, the determinants of ψ and of $\phi(x_1,\dots,x_i,0,\dots,0)$ $(k \leqslant i \leqslant s)$ are unchanged, whence $l_k, l_{k+1},\dots, l_s$ are unchanged. We employ such a transformation T which carries ψ into a principal representative

† Op. cit. ii. 635–6.

‡ The determination of a principal representative in a finite number of steps is discussed by Minkowski (pp. 33–5).

§ P. Bachmann, *Die Arithmetik der quadratischen Formen*, i. 452–3.

of itself for the primes dividing l_k as well as $2o_1 o_2 \dots o_{s-1}$. Then the new l_{k-1} will be prime to l_k, and we have reduced the problem to a lower value of k.

To proceed: by (9), we may write (51) in the form

$$(\mu_k d_k l_k)(\mu_k d_k l'_k) - \tfrac{1}{4}(\mu_k d_k)^2 z^2 = (\mu_{k-1} d_{k-1} l_{k-1})(\mu_{k+1} d_{k+1} l_{k+1}),$$

where z and l'_k are integers; and hence by (12) we have

$$-o_k l_{k-1} l_{k+1} = z^2 - 4 l_k l'_k. \tag{55}$$

Consequently Lemma 8 implies

LEMMA 9. *If the order* $(1; I; o_1, \dots, o_{s-1})$ *actually contains forms, there exist integers* $l_0 = 1, l_1, \dots, l_{s-1}, l_s = (-1)^I$ *satisfying* (54) *and such that the congruences*

$$-o_k l_{k-1} l_{k+1} \equiv z_k^2 \pmod{4 l_k} \tag{56}$$

are solvable in integers z_k $(k = 1, \dots, s-1)$.

The index I of f is equal to the number of consecutive sign-changes in a chain of principal minor determinants and hence in the sequence (53). We shall hereafter assume (54), so that none of the l_k are zero. We write $\epsilon_k = +1$ or -1 according as l_k is positive or negative, whence $\epsilon_0 = 1$, $\epsilon_s = l_s = (-1)^I$, $\epsilon_k l_k > 0$ $(k = 0, \dots, s)$.

Since (54) holds, (56) implies both of

$$\zeta_k \equiv (-o_k l_{k-1} l_{k+1} | \epsilon_k l_k) = 1 \qquad (k = 1, \dots, s-1) \tag{57}$$

and

$$-o_k l_{k-1} l_{k+1} \equiv 1 \pmod 4, \quad \text{if } o_k \text{ is odd.} \tag{58}$$

It is easily verified that

$$(l_{i+1} | \epsilon_i l_i)(-l_i | \epsilon_{i+1} l_{i+1}) = \kappa_i \lambda_i \qquad (i = 0, \dots, s-1), \tag{59}$$

where

$$\kappa_i = (-1)^{(l_i+1)(l_{i+1}-1)/4}, \quad \lambda_i = (-1)^{(\epsilon_i+1)(\epsilon_{i+1}-1)/4} \qquad (i = 0, \dots, s-1); \tag{60}$$

and it is plain that $\zeta_1 \dots \zeta_{s-1}$ is the product of the s left-hand members of (59) by the $s-1$ numbers

$$\nu_k = (o_k | \epsilon_k l_k) \qquad (k = 1, \dots, s-1). \tag{61}$$

Consequently, by (57), (56) requires $\zeta_1 \dots \zeta_{s-1} = 1$, that is,

$$\kappa_0 \dots \kappa_{s-1} \lambda_0 \dots \lambda_{s-1} \nu_1 \dots \nu_{s-1} = 1. \tag{62}$$

Now I is the number of consecutive sign-changes in $(\epsilon_0, \dots, \epsilon_s)$. (63)

To each change from $+$ to $-$ corresponds a factor $\lambda_i = -1$. Hence

$$\lambda_0 \dots \lambda_{s-1} = (-1)^{[(I+1)/2]},$$

and (62) reduces to

$$\kappa_0 \dots \kappa_{s-1} \nu_1 \dots \nu_{s-1} = (-1)^{[(I+1)/2]}. \tag{64}$$

We shall now show that, if there exist integers $l_0 = 1, l_1, \ldots, l_{s-1}$, $l_s = (-1)^I$ (the sign ± 1 of l_k being represented by ϵ_k) satisfying

$$(54),\ (58),\ (63),\ \text{and}\ (64), \tag{P}$$

then there exist other integers l_k having the same properties and signs and also satisfying (56); and hence we shall be able to construct a form in the order $(1; I; o_1, \ldots, o_{s-1})$.

For set $m_0 = l_0 = 1$. Without affecting the validity of (P) we can replace l_1 by m_1, where $\epsilon_1 m_1$ is a positive prime (or 1) and $m_1 \equiv l_1 \pmod{8o_1}$. Next, by (54) and (58), we can replace l_2 by m_2, where $\epsilon_2 m_2$ is a positive prime, $m_2 \equiv l_2 \pmod{8o_2}$, and the congruence

$$-o_1 m_0 m_2 \equiv z_1^2 \pmod{4m_1}$$

is solvable for an integer z_1; the truth of (P) being retained. We can proceed in this fashion until we have chosen $\epsilon_{s-1} m_{s-1}$ to be a positive prime (or unity) satisfying

$$-o_{s-2} m_{s-3} m_{s-1} \equiv z_{s-2}^2 \pmod{4m_{s-2}}, \qquad m_{s-1} \equiv l_{s-1} \pmod{8o_{s-1}};$$

while the system $l_0 \to 1$, $l_1 \to m_1$, ..., $l_{s-1} \to m_{s-1}$, $l_s \to m_s = (-1)^I$ satisfies (P). Further, with the m_i substituted for the l_i,

$$\zeta_1 = \ldots = \zeta_{s-2} = 1,$$

whence (64) shows that $\zeta_{s-1} = 1$, and hence that the last of the congruences

$$-o_k m_{k-1} m_{k+1} \equiv z_k^2 \pmod{4m_k} \qquad (k = 1, \ldots, s-1) \tag{65}$$

is solvable for an integral z_{s-1}.

We shall now try to construct a form ϕ in the order $(1; I; o_1, \ldots, o_{s-1})$ with a matrix for 2ϕ of the type

$$\begin{bmatrix} 2v_0 & w_1 & & & & \\ w_1 & 2v_1 & w_2 & & & \\ & w_2 & 2v_2 & w_3 & & \\ & & w_3 & 2v_3 & \ldots & \\ & & & \ldots & & \\ & & & & & 2v_{s-1} \end{bmatrix} \tag{66}$$

with zeros elsewhere. Let M_k denote the leading principal minor determinant of order k. We wish to identify M_k with $\mu_k d_k m_k$. Thus $M_0 = 1$, $M_1 = 2v_0 = 2d_1 m_1$, whence $v_0 = m_1$, and generally, if $0 < k < s$,

$$M_{k+1} = 2v_k M_k - w_k^2 M_{k-1},$$

$$\mu_{k+1} d_{k+1} m_{k+1} + w_k^2 \mu_{k-1} d_{k-1} m_{k-1} = 2v_k \mu_k d_k m_k. \tag{67}$$

Now, since by (12) or (14)

$$4^{k-1}\mu_k d_k = 2o_1 o_2 \dots o_{k-1}\mu_{k-1} d_{k-1}, \tag{68}$$

we must have (for $k = 1,\dots,s-1$)

$$4^{2-2k}o_1^2 \dots o_{k-1}^2 o_k m_{k+1} + m_{k-1} w_k^2 = 4^{2-k} o_1 \dots o_{k-1} v_k m_k. \tag{69}$$

We shall therefore, in view of (65), write†

$$o_k m_{k+1} + m_{k-1} z_k^2 = 4 m_k t_k, \qquad v_0 = m_1,$$

$$w_k = 4^{1-k} o_1 \dots o_{k-1} z_k, \qquad v_k = 4^{1-k} o_1 \dots o_{k-1} t_k \quad (k = 1,\dots,s-1). \tag{70}$$

By this construction the leading minor M_k has the value $\mu_k d_k m_k$, $(k = 0,\dots,s)$. Hence the index, determined by the signs of the m_k, is I. Since m_k is prime to $\mu_{k+1} d_{k+1} m_{k+1} = M_{k+1}$, we have merely to see that all the remaining principal minors and twice all the secondary minors of (66), of order k, are divisible by $\mu_k d_k$, to ensure that d_k is the g.c.d. of order k. Every such minor M' of order k is obtained by bordering some M_r $(0 \leqslant r < k \leqslant s)$ with $k-r$ rows and columns, the first row being at least the $(r+2)$th, the first column at least the $(r+1)$th.

On bordering M_{k-1} with the $(k+2)$th row and column, we obtain a determinant having the value $2v_{k+1}\mu_{k-1} d_{k-1} m_{k-1}$. The quotient of this by $\mu_k d_k$ is $\frac{1}{4} m_{k-1} o_k t_{k+1}$, by (68) and (70), and must be integral. By (70), if o_{k+1} is even, $4|z_{k+1}$ if and only if $4|t_{k+1}$; hence we need

$$4|z_{k+1} \text{ and } 4|t_{k+1} \text{ for each } k \text{ such that } o_k \text{ is odd } (0 < k < s-1). \tag{71}$$

To satisfy this condition we replace z_{k+1} by $2|m_{k+1}| - z_{k+1}$, which is also a solution of (65), if $z_{k+1} \equiv 2 \pmod 4$. Condition (71) is finally seen to be sufficient.

For, generally, the minor M' is equal to $\mu_r d_r m_r$ multiplied by zero, or by a sum of terms of a type $\pm u_1 \dots u_{k-r}$ characterized as follows: let $r+2 \leqslant h_1 < h_2 < \dots < h_{k-r} \leqslant s$; u_i is one of the numbers

$$w_{h_i-1}, \qquad 2v_{h_i-1}, \qquad w_{h_i}$$

chosen from the h_ith row, no two factors $u_1,\dots,u_{k-r}$ belonging to the same column in (66). The terms of a secondary minor M' are distinguished by containing at least one factor $u_i = w_h$ such that neither u_{i+1} nor u_{i-1} is also w_h; in such a case we can prefix a factor 2 to each term.

† Minkowski (loc. cit., 77) introduces an extra factor o_k in his definitions corresponding to v_k and w_k, in order to simplify his discussion. But this weakens the analogy with the best treatment for $s = 2$ and 3, and hampers an extension to the case m_k not prime to o_k.

By (68), $\mu_k d_k = \mu_r d_r 2\xi_{r+1} 2\xi_{r+2} \dots 2\xi_k$, where

$$\xi_h \equiv o_1 \dots o_{h-1}/4^{h-1} \qquad (h = 1,\dots,s). \tag{72}$$

Hence we have merely to prove the integrality of

$$\{u_1/(2\xi_{r+1})\} \dots \{u_{k-r}/(2\xi_k)\}, \tag{73}$$

or of its double, if M' is secondary. We abbreviate

$$\xi_{ij} = \xi_{r+j}/\xi_{r+i} = o_{r+i} \dots o_{r+j-1}/4^{j-i} \quad (0 < i \leqslant j \leqslant s-r). \tag{74}$$

By (70), $w_k = \xi_k z_k$, $v_k = \xi_k t_k$, and the ith factor of (73) is of type

$$2v_{r+j}/(2\xi_{r+1}) = \xi_{ij} t_{r+j} \quad \text{or} \quad w_{r+j}/(2\xi_{r+1}) = \tfrac{1}{2}\xi_{ij} z_{r+j}. \tag{75}$$

Now, by (13), ξ_{ij} is an integer unless

$$o_{r+i}, o_{r+i+2}, \dots, o_{r+j-1} \text{ are odd} \quad (j-i \text{ odd}); \tag{76}$$

and in this case $4\xi_{ij}$ is an integer, and hence $\xi_{ij} t_{r+j}$, $\xi_{ij} z_{r+j}$ are still integral by (71). If then there is only one factor of type $\frac{1}{2}\xi_{ij} z_{r+j}$ in (73), M' is secondary and the prefixed factor 2 ensures the integrality.

Finally, if there are two or more such factors, consider any of them other than the last, say $\frac{1}{2}\xi_{ij} z_{r+j}$. If o_{r+j} is even, z_{r+j} is even by (70), and ξ_{ij} is an integer save in case (76); if o_{r+j} is odd, $16 | o_{r+j-1}$ and hence, by (13), ξ_{ij} is a multiple of 4 unless

$$o_{r+i}, o_{r+i+2}, \dots, o_{r+j-2} \text{ are odd} \quad (j-i \text{ even}), \tag{76'}$$

in which case ξ_{ij} is still an integer. Thus $\frac{1}{2}\xi_{ij} z_{r+j}$ may be half an integer only in case

$$o_{r+i}, o_{r+i+2}, \dots, o_{r+j-\kappa} \quad (\kappa = 0 \text{ or } 1) \text{ are odd}. \tag{77}$$

The succeeding factor in (73) may be (i) $\frac{1}{2}\xi_{i+1,j} z_{r+j}$ $(i < j \leqslant s-r)$, (ii) $\frac{1}{2}\xi_{i+1,j+h} z_{r+j+h}$ $(i \leqslant j < j+h \leqslant s-r)$, or (iii) $\xi_{i+1,j+h} t_{r+j+h}$. In case (i), (77) implies that $16 | o_{r+i+1}$ whence either $\xi_{i+1,j}$ or z_{r+j} is a multiple of 4 and both are integral; in case (ii) or (iii) similarly, (77) and (71) compel the factor to be a multiple of 4.

What, finally, are the conditions on I and the o_k, beyond (13) and Theorem 3, that there shall exist integers $l_0 = 1, l_1, \dots, l_{s-1}, l_s = (-1)^I$ (with signs $\epsilon_0, \dots, \epsilon_s$), satisfying (P)?

We can choose infinitely many sets of integers $l_1, \dots, l_{s-1}$, with arbitrary signs ϵ_k and arbitrary odd residues $\pm 1 \pmod 4$, to satisfy (54). Condition (58) limits the possible residues, to modulus 4, but leaves the choice of signs unrestricted except when $o_1, o_3, \dots, o_{s-1}$ are odd and s is even; then (58) requires that

$$(-)^{s/2} o_1 o_3 \dots o_{s-1} l_0 l_s \equiv 1 \pmod 4,$$

where $l_0 = 1$ and $l_s = (-1)^I$, which is condition (50).

With this one restriction on I satisfied, we consider the effect on ν_k of replacing l_k by l_k+4n, where n is an integer of the same sign as l_k and (54) still holds. If o_k is not a square there are infinitely many values n for which $\nu_k = 1$ and infinitely many for which $\nu_k = -1$. Consequently (64) can be satisfied except when

$$\text{all of } o_1, o_2, \ldots, o_{s-1} \text{ are perfect squares.} \tag{78}$$

When (78) holds, $\nu_1 = \ldots = \nu_{s-1} = 1$ and (58), (64) become

$$l_{k+1} \not\equiv l_{k-1} \pmod 4 \text{ whenever } o_k \text{ is odd,} \tag{79}$$

$$\kappa_0 \kappa_1 \ldots \kappa_{s-1} = (-1)^{[(I+1)/2]} \qquad (\kappa_i = (-1)^{(l_i+1)(l_{i+1}-1)/4}). \tag{80}$$

Evidently $\kappa_i = -1$, if and only if $l_i \equiv 1$ and $l_{i+1} \equiv 3 \pmod 4$. We call such a consecutive pair l_i, l_{i+1} a $(1,3)$-*change*. Then (80) gives

$$\text{the number of } (1,3)\text{-changes in } l_0, \ldots, l_s \text{ is congruent, to modulus 2, to } [(I+1)/2]. \tag{81}$$

Given an index I and square invariants $o_1, \ldots, o_{s-1}$, the remaining question is: can we choose odd l_k, whose signs ϵ_k agree with (63), to satisfy (79) and (81)? We shall now see that such a choice can be made, if there are three different values of k $(0 \leqslant k \leqslant s-1)$ such that $o_k \equiv o_{k+1} \equiv 0 \pmod 4$; and that, when there are not more than two such values of k, the choice can be made if and only if

$$s-2I \not\equiv 3, 4, 5 \pmod 8. \tag{82}$$

For the only restrictions on the residues of the l_i to modulus 4 are (79) and the values $l_0 = 1$ and $l_s = (-1)^I$. We are free to assign to any particular l_i either residue $\pm 1 \pmod 4$, unless either $o_1, o_3, \ldots, o_{i-1}$ are odd, in which case $l_i = (-1)^{i/2}$, or $o_{i+1}, o_{i+3}, \ldots, o_{s-1}$ are odd, whence $l_i = (-1)^{I+(s-i)/2}$.

To expedite the counting of $(1,3)$-changes consider the case of

$$o_{i+2}, o_{i+4}, \ldots, o_{j-1}, \; o_{j+2}, o_{j+4}, \ldots, o_{k-1} \text{ odd} \tag{83}$$

(whence o_j and o_{j+1} are even), where $-1 \leqslant i < j < k \leqslant s$, and $j-i$ and $k-j$ are odd. The number of $(1,3)$-changes in $l_{i+1}, l_{i+2}, \ldots, l_k$ is independent of j, and depends only on i, k, and the choices of l_{i+1} and l_k; it is therefore the same as in the case

$$o_{i+2}, o_{i+4}, \ldots, o_{k-2} \text{ odd}, \qquad o_{k-1} \text{ and } o_k \text{ even}, \tag{84}$$

with the same choices of l_{i+1} and l_k. For the residues of $l_{i+1}, l_{i+3}, \ldots, l_j$ and of $l_k, l_{k-2}, \ldots, l_{j+1}$ are alternately 1 and 3, or 3 and 1, depending on l_{i+1} and l_k; the values of $l_{i+2}, l_{i+4}, \ldots, l_{j-2}$ and $l_{j+3}, l_{j+5}, \ldots, l_{k-2}$ are

therefore immaterial and may be disregarded in counting $(1,3)$-changes. If now $j < k-1$ and we replace j by $j+2$, the number of $(1,3)$-changes is unaltered: e.g.

$$131,313 \to 1313,13;\ 131,1313 \to 1313,313.$$

Suppose then that o_h and o_{h+1} are even for the three values $h = i,j,k$ at least, where $0 \leqslant i < j < k \leqslant s-1$. Employing the preceding transformation we can suppose that there are four consecutive even o_k, say o_{k-2}, o_{k-1}, o_k, o_{k+1}. Since the residues 1 or 3 of l_{k-1} and l_k are unconstrained, we can satisfy (81), whatever be the values of l_{k-2} and l_{k+1}, as is plain from the following schemes:

$$1111 \text{ or } 1331;\ 3113 \text{ or } 3333;\ 1133 \text{ or } 1313;\ 3131 \text{ or } 3311.$$

Next let there be only two values h for which $o_h \equiv o_{h+1} \equiv 0 \pmod 4$, say i and j $(0 \leqslant i < j \leqslant s-1)$. Then $o_1, o_3, \ldots, o_{i-1}, o_{i+2}, o_{i+4}, \ldots, o_{j-1}, o_{j+2}, o_{j+4}, \ldots, o_{s-1}$ are odd; $i-1$, j, $s-j$ are odd, s is even. By the above transformation we can suppose (without loss) that $o_1, o_3, \ldots, o_{s-3}$ are odd; o_{s-2}, o_{s-1}, and o_s even. Then $l_{s-2} = (-1)^{(s-2)/2}$, $l_s = (-1)^I$. If $\frac{1}{2}(s-2) \equiv I \pmod 2$ the choice $l_{s-1} \equiv 1$ or 3 gives at will an even or an odd number of $(1,3)$-changes. If, however, $s-2I \equiv 0 \pmod 4$ the number of $(1,3)$-changes is $\frac{1}{4}\{s+1-(-1)^I\}$, whence (81) excludes only $s-2I \equiv 4 \pmod 8$.

If $o_1, o_3, \ldots, o_{s-1}$ are odd, $s-2I \equiv 0 \pmod 4$ by (50), and, as the number of $(1,3)$-changes is again $\frac{1}{4}\{s+1-(-1)^I\}$, $s-2I \equiv 4 \pmod 8$ is the only excluded possibility.

Finally, if o_h and o_{h+1} are even for only one value of h, we can transform it to be $h = s-1$. Then s is odd, and the number of $(1,3)$-changes is $\frac{1}{4}\{s+2-(-1)^I\}$, and (81) thereby rejects only $s-2I \equiv \pm 3 \pmod 8$.

THEOREM 4. *Let $0 \leqslant I \leqslant s$, let $o_1, \ldots, o_{s-1}$ be positive integers, and let $o_0 = o_s = 0$. Then a form exists having these invariants, if and only if*

(i) $o_k \not\equiv 2 \pmod 4 \qquad (0 \leqslant k \leqslant s)$;

(ii) *if o_k is odd, $o_{k-1} \equiv o_{k+1} \equiv 0 \pmod{16}$;*

(iii) *if $o_1 o_3 \ldots o_{s-1}$ is odd, s even, then $(-)^{\frac{1}{2}(s-2I)} o_1 o_3 \ldots o_{s-1} \equiv 1 \pmod 4$;*

(iv) *if all the o_k are squares, and if $o_k \equiv o_{k+1} \equiv 0 \pmod 4$ for not more than two values of k $(0 \leqslant k < s)$, then $s-2I \not\equiv 3,4,5 \pmod 8$.*

It is worth while to remark the special result:

If $s = 2$, 3, or 4, and $I = 0$, and if all the o_k are squares, then none of the o_k can be odd. (85)

11. The o-invariants of the comitants of the comitants. Smith, who was apparently the first to recognize the intermediate concomitants [comitants] $f_2,\ldots,f_{s-2}$, left an interesting point unsettled. This we now propose to elucidate.

If $s > 3$, there are, besides the fundamental concomitants $f_1,\ldots,f_{s-1}$, an infinite number of others, namely the concomitants of the concomitants, and so on indefinitely. Their invariants being also invariants of f, Smith remarks† that 'it is important to know whether, in order to obtain the distribution into orders, it is, or is not, necessary to consider these other concomitants'. He states that 'it can be shown that it is unnecessary to consider any concomitants other than the fundamental ones, as regards the primary divisors' [the g.c.d.'s of all the minor determinants of any given order]. 'It is probable (but it seems difficult to prove) that the same thing is true for the secondary divisors' [the g.c.d.'s of all the principal and doubles of the secondary minors of any given order].

By our results (Theorem 2) the primary divisors are completely determined by the secondary divisors, and it is required only to show precisely how to find the o-invariants of f_k from those of f_1.

The simplest relationship among these invariants, namely,

$$o_1(f_k) = o_k(f_1) \qquad (k = 1,\ldots,s-1), \tag{86}$$

is of some importance and easily proved otherwise. The index I' of f_k is readily expressed by the following formula in terms of the index I of f_1:

$$I' = \sum_{\mu=1}^{\infty} \binom{I}{2\mu-1}\binom{s-I}{k-2\mu+1}. \tag{87}$$

To proceed, denote by p^{ω_i} the power of p dividing $o_i(f_1)$ $(i = 1,\ldots,s-1)$, and by $p^{\omega_{kh}}$ the power of p dividing $o_h(f_k)$, where $0 < k < s$ and $0 < h < \lambda$ $(\lambda = {}_sC_k)$.

In (19) or (29), there are λ sums of the numbers $\alpha_1,\ldots,\alpha_s$ taken k at a time. Arranged in ascending order of magnitude they may be denoted by $\delta_1,\ldots,\delta_\lambda$; thus $\delta_1 = \alpha_1+\ldots+\alpha_k$, $\delta_2 = \alpha_1+\ldots+\alpha_{k-1}+\alpha_{k+1},\ldots$ $(0 \leqslant \delta_1 \leqslant \delta_2 \leqslant \ldots \leqslant \delta_\lambda)$.

First, suppose $p > 2$. If we take the kth comitant of the canonical

† Loc. cit., 415.

form (19) of f we obtain a canonical form χ of like pattern for f_k, the modulus p^l being sufficiently large. It is plain from χ and (34) that

$$\omega_{hk} = \delta_{h+1} - \delta_h \qquad (h = 1,\ldots,\lambda-1). \tag{88}$$

In particular as regards (86), $\omega_{1k} = \alpha_{k+1} - \alpha_k = \omega_k$.

Secondly, suppose $p = 2$ and t sufficiently large. The kth comitant of (29) is not in general in the pattern of (29), but we shall see how to put it into that form.

Each sum δ_j is of the form

$$\alpha_{i_1} + \alpha_{i_2} + \ldots + \alpha_{i_k} \qquad (1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant s). \tag{89}$$

With the sum δ_j we associate the subsequence $(i_1,\ldots,i_k)$, and denote this subsequence by σ_j. The λ subsequences of $(1,\ldots,s)$ of k elements are, in a certain order, $\sigma_1,\ldots,\sigma_\lambda$.

There is an indeterminacy in the arrangement of equal sums (89). Each α_h of type γ is associated with its *twin*, which is α_{h+1} or α_{h-1} according as α_h is an initial or a terminal γ. If r $(\geqslant 0)$ terms α_h $(h = h_1,\ldots,h_r$, say) occur in a sum (83) without their twins, that sum forms part of a *system of* 2^r *twin sums*, obtained by replacing some or all of the terms α_h $(h = h_1,\ldots,h_r)$ by their twins. The sums δ_j may be so ordered that a system of twin sums occurs consecutively.

Let M denote the matrix of (29). The matrix of the kth comitant of (29) has as its element in the ith row and jth column the value of the determinant $M[\sigma_i\,\sigma_j]$. Now the elements of one row of $M[\sigma_i\,\sigma_j]$ are all zero unless δ_i and δ_j belong to the same system of twin sums. Consequently the matrix of the kth comitant consists of a series of square matrices situated one after the other down and symmetric with the principal diagonal, with zeros everywhere else; one square matrix of order 2^r corresponding to each system of twin sums (89).

Consider such a system of 2^r twin sums, and denote the corresponding matrix of order 2^r by R. We may suppose $r \geqslant 2$. Necessarily $r \leqslant k$. Let $l_1,\ldots,l_{k-r}$ be the indices i of those α_i which are common to all the twin sums of the system; and let α_h $(h = h_1,\ldots,h_r)$ be the initial γ's of the system, so that α_h $(h = h_1+1,\ldots,h_r+1)$ are the terminal γ's of the system. Then all the elements of R have a common factor of the type

$$2^\tau m \qquad (\tau = \alpha_{l_1} + \alpha_{l_2} + \ldots + \alpha_{l_{k-r}}),$$

where m is an odd integer. Write R' for the matrix $R/(2^\tau m)$ obtained

by removing this factor. Then R' may be described as follows. We may set

$$\gamma_i \equiv \alpha_{h_i} = \alpha_{h_i+1}, \qquad \nu_i = \begin{pmatrix} a_i & b_i \\ b_i & c_i \end{pmatrix}, \tag{90}$$

where $a_i = 2^{\gamma_i+1}m_i$, $b_i = 2^{\gamma_i}m^{(i)}$, $c_i = 2^{\gamma_i+1}n_i$ $(i = 1,\ldots,r)$, the m_i and $m^{(i)}$ being certain odd integers, the n_i certain integers. The elements of R' are the 4^r possible products of r elements, one chosen from each of the matrices ν_i. Thus the first row consists of all products in which one element is taken from the first rows of each of $\nu_1,\ldots,\nu_r$; the second row employs similarly the first rows of $\nu_1,\ldots,\nu_{r-1}$ and the second row of ν_r; and so on, the selection of rows being parallel with the selection of columns:

$$\begin{array}{cccccc} a_1a_2\ldots a_r & a_1\ldots a_{r-1}b_r & a_1\ldots a_{r-2}b_{r-1}a_r & . & . & . & b_1b_2\ldots b_r \\ a_1\ldots a_{r-1}b_r & a_1\ldots a_{r-1}c_r & a_1\ldots a_{r-2}b_{r-1}b_r & . & . & . & b_1\ldots b_{r-1}c_r \\ & & . \quad . \quad . \quad . & & & & \end{array}$$

In the notations (90), if we set $\eta = \gamma_1+\ldots+\gamma_r$, then $\tau+\eta$ is the common value of the sums δ_j of the system. The factor 2^η can now be removed from every row of R'. The matrix left behind is evidently the matrix of a classical, odd form, since the diagonal elements are all even while at least one secondary element $(b_1\ldots b_r/2^\eta)$ is odd. The form is, in fact, also of odd determinant, since, reducing the elements to modulus 2, we substitute 0 for a_i and c_i, 1 for b_i in (90) $(i = 1,\ldots,r)$, and obtain in place of R' a matrix in which a unique element in each row and column is 1, the rest zero.† Thus Lemma 7 applies and shows that the form of matrix R is equivalent, to modulus 2^t, to a form of the type $(30'')$, multiplied by $2^{\tau+\eta}$.

Among the sums δ_j in (89) certain ones may have no twin sums; these correspond in R to an isolated term $2^{\delta_j+1}m_j$ (m_j odd) as the jth element on the principal diagonal. If any such isolated term exists with δ_j+1 equal to the value $\tau+\eta$ of a system like that considered above, that system together with the isolated term can be brought as in Lemma 5 to a diagonal form.

The kth comitant of (29) is thereby transformed into a form of the same kind as (29), in a manner which determines uniquely the powers of 2 dividing the various quantities $o_h(f_k)$ in terms of the powers of 2 dividing $o_1,\ldots,o_{s-1}$.

† It can indeed be shown that the determinant of R' is equal to the product of the determinants $4m_in_i-m^{(i)2}$ each raised to the (2^{r-1})th power.