ON INDEFINITE TERNARY QUADRATIC FORMS

B. W. JONES AND G. L. WATSON

1. Introduction. The first systematic study of equivalence of indefinite ternary quadratic forms seems to be that of A. Meyer **(10)** (see also Bachmann **(1)**). By methods which are often obscure he showed that the number of classes in a genus is a power of 2, the exact power depending on certain quadratic characters associated with the form. These investigations, however, dealt only with forms of odd determinant, in the classical sense (in our notation, $A \equiv 0 \pmod 2$ and $d \equiv 4 \pmod 8$). Donald Marsh **(9)** established an algorithm by which the number of classes may be determined. Eichler **(4)** has, as a consequence of deep and general theory, thrown much light on these questions.

Here, using concepts closely related to the spinor genera of Eichler, we define a multiplicative group Γ_d of square-free integers prime to d, the determinant of f. Further we show that Γ_d has a subgroup $\gamma(f)$ consisting of all those elements of Γ_d which are denominators of rational automorphs of f, where by the demoninator of a matrix we mean the l.c.m. of the denominators of its elements. We show that the number of classes in the genus of f is equal to the order of the factor group $\Gamma_d/\gamma(f)$. In the process of deriving this result we get information about the automorphs which yield much new information (see Theorem 2) about the representation of numbers by indefinite ternary quadratic forms. An alternative definition of a group $\Gamma(p, f)$ is given in §3 by means of which the order of the factor group above can be determined.

2. Notation. For certain matrices with integral elements we shall use the notation:

$$x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \quad x' = (x_1, x_2, x_3), \quad \dot{x} = \begin{bmatrix} 0 & -x_3 & x_2 \\ x_3 & 0 & -x_1 \\ -x_2 & x_1 & 0 \end{bmatrix}.$$

Latin capitals will denote 3×3 non-singular matrices, with rational elements, I being the identity matrix. Other letters will denote integers unless otherwise stated, p being always a prime.

For a ternary form, we use the notation

$$f = f(\xi) = f(\xi_1, \xi_2, \xi_3) = \tfrac{1}{2}\xi' A \xi, \quad A = (a_{ij}) = (\partial^2 f / \partial \xi_i \, \partial \xi_j),$$

and define the invariant **(2**, pp. 4, 5**)**

$$d = d(f) = -\tfrac{1}{2}|A|.$$

Received September 19, 1955.

We assume that f has integral coefficients and is indefinite and non-degenerate (i.e. that $d \neq 0$). We also assume that f is primitive, that is, that its coefficients have greatest common divisor 1. The non-primitive case can easily be deduced from it. We note that A, being symmetrical and having even diagonal elements, is congruent (mod 2) to a skew matrix, which is singular (mod 2); hence d is integral.

As we are concerned with properties invariant under integral unimodular transformations, we may suppose when necessary that the form f is a representative of its class satisfying one or other of the following congruences:

$$f \equiv \sum_{i=1}^{3} p^{\lambda_i} a_i \xi_i^2 \pmod{p^\beta}, \qquad p \nmid a_1 a_2 a_3, \ 0 = \lambda_1 \leqslant \lambda_2 \leqslant \lambda_3; \tag{2.1}$$

$$f \equiv 2^{\lambda_1} \phi(\xi_1, \xi_2) + 2^{\lambda_2} a \xi_3^2 \pmod{2^\beta}, \qquad \lambda_1, \lambda_2 = 0, \lambda \text{ or } \lambda, 0 \tag{2.2}$$

$$f \equiv \xi_1 \xi_2 + d\xi_3^2 \pmod{p^\beta}, \qquad p \nmid d, \tag{2.3}$$

where in (2.2) a and the discriminant of ϕ are odd. This is possible for any prescribed β; we assume always that β exceeds the highest exponent on the right side of the congruence by at least $2 + (-1)^p$. For a proof that every f is equivalent to a form satisfying (2.1) if $p > 2$, or one of (2.1), (2.2) if $p = 2$, see, for example, Jones **(6**, pp. 84, 85**)**. Starting with either of these it is easy to obtain (2.3).

The exponents λ_i, λ are unique for a given f and are invariants of the genus, as are the possible values of the quadratic characters of the a_i and a modulo p or 8. But the latter are not always unique.

3. Definition of certain groups and statement of results. We consider the set of integers $b \neq 0$ for which, for any prescribed p and f, we can find t so that

$$t'A \equiv 0 \pmod{p^\delta}, \ f(t) \equiv b \pmod{p^\tau}, \ p \nmid t \tag{3.1}$$

with $\delta \geqslant 0$ such that $p^\delta || b$, and $\tau = \delta + 2 + (-1)^p$. Note that if (3.1) is soluble, then f has the automorphism $\xi \to -\xi + tt'A\xi/f(t)$ reducing in case $t' = (1, 0, 0)$ to

$$\xi_1, \xi_2, \xi_3 \to \xi_1 + 2a_{11}^{-1}(a_{12}\xi_2 + a_{13}\xi_3), \ -\xi_2, \ -\xi_3.$$

The denominator of this automorph is a divisor of $p^{-\delta} f(t)$, which is prime to p and congruent to $p^{-\delta} b$ modulo p or 8.

Now we observe that the set of positive and negative square-free integers v forms a group, Γ, with the operation

$$v_1 \cdot v_2 = v_1 v_2 (v_1, v_2)^{-2}. \tag{3.2}$$

Any subset of Γ closed under this operation is a group. For any b for which (3.1) can be satisfied, write

$$-db = u^2 v, \ v \in \Gamma. \tag{3.3}$$

Note that v is not altered by multiplying f by any integer. We define $\Gamma(p, f)$ to be the sub-group of Γ generated by all v arising from (3.3).

We denote by Γ_m the subgroup of Γ defined by $(v, m) = 1$; and we use the groups $\Gamma(p, f)$, $p|d$, to define a certain sub-group of Γ_d.

We define $\gamma(f)$ as follows: $q \in \gamma(f)$ if and only if $q \in \Gamma_d$ and there exists a w such that $w|d$ and

$$wq \in \bigcap_{p|d} \Gamma(p, f).$$

Note that with q, also $-q$ belongs to $\gamma(f)$; also that $\gamma(f)$ is a group since $(w_1q_1)\cdot(w_2q_2) = (w_1\cdot w_2)(q_1\cdot q_2)$.

By the denominator of a rational matrix we mean the least common denominator of its elements, with either sign. We shall show that f may be taken into a form in the same genus by a transformation whose matrix has any prescribed denominator q in Γ_d. On the other hand, f has an automorph with denominator q in Γ_d if and only if $q \in \gamma(f)$. We shall thus prove

THEOREM 1. *The number of classes in the genus of f is equal to the order of the factor group $\Gamma_d/\gamma(f)$.*

Alternatively, if $\nu \geqslant 0$ is the number of distinct characters in the set

$$(\pm 2|q) \text{ if } 2|d; \quad (q|p) \text{ if } p > 2,\ p|d \tag{3.4}$$

(where the symbols are Jacobi symbols), and if these are capable of 2^s distinct sets of values (each ± 1) for q in $\gamma(f)$, then the class-number is $2^{\nu-s}$.

Note that $\Gamma(p, f)$ and $\gamma(f)$ are invariants of the genus of f, since forms in the same genus have the same congruence properties. The same remark therefore applies to the invariant $d_0 = d_0(f)$ which we now define: d_0 is the product of all the distinct odd primes p for which $\Gamma_p \not\subset \Gamma(p, f)$, multiplied by 2 in case $5 \notin \Gamma(2, f)$.

We leave it to the reader to verify that the alternative statement of Theorem 1 remains valid on putting d_0 for d in (3.4). We shall see that $\Gamma(p, f) = \Gamma_p$ when $p \nmid d$, so that d_0 divides d. We can now state

THEOREM 2. *Suppose n is represented by at least one but not by all of the classes of forms in the genus of f, and write $dn = n_1n_2^2$, n_1 square-free. Then*

(i) $n_1 > 1$;

(ii) *n_1 divides d_0;*

(iii) $n_1 \equiv 1 \pmod 8$ *if d is odd;*

(iv) *if $(p, 2d) = 1$ and $(n_1|p) = -1$, p cannot divide n_1;*

(v) *the number of classes in the genus that represent n is equal to the number that do not.*

We conclude this section with an alternative definition of $\Gamma(p, f)$, in which f is assumed to satisfy (2.1) or (2.2) as the case may be and by means of which $\gamma(f)$ could be computed. Below σ_{ij} denotes 1 or 0, according as $\lambda_i + \lambda_j$ is odd or even.

https://doi.org/10.4153/CJM-1956-064-0 Published online by Cambridge University Press

ALTERNATIVE DEFINITION OF $\Gamma(p, f)$

(a) $p > 2$. $\Gamma(p, f)$ is the sub-group of Γ generated by
(i) the group of f with $(v|p) = 1$
(ii) the set of $v \equiv p^{\sigma_{ij}} a_i a_j \pmod{p^{1+\sigma_{ij}}}$ for any i, j;
(iii) the group Γ_p, if two of the exponents $\lambda_1, \lambda_2, \lambda_3$ are equal.

(b) $p = 2$ and (2.2) holds. $\Gamma(2, f) = \Gamma$ or Γ_2, according as λ is odd or even.

(c) $p = 2$ and (2.1) holds. $\Gamma(2, f)$ is generated by the set of $v \equiv 1 \pmod 8$ or $2^{\sigma_{ij}} a_i a_j \pmod{2^{3+\sigma_{ij}}}$, together with the following integers, reduced mod 8, if the stated conditions hold for any unequal i, j:
(i) $1 + a_i a_j$, if $\lambda_i = \lambda_j$ and $a_i \equiv a_j \pmod 4$;
(ii) 5, if $\lambda_i - \lambda_j = 0, 2$ or 4;
(iii) 3, if $\lambda_3 \leqslant 2$;
(iv) $1 + 2a_i a_j$, if $\lambda_i - \lambda_j = 1$ or 3.

The equivalence of this to the earlier definition will be proved in §5.

4. Rational automorphs. We make use of the rational automorphs $S, S_1, S_2, \ldots$ of the form f, or of its matrix A. We shall consider only automorphs with determinant 1; we lose nothing thereby, since f has always the trivial automorph $-I$ with determinant -1. By the denominator of S we mean the least common denominator of its elements with either sign.

We are thus concerned with matrices S satisfying

$$S'AS = A, \quad |S| = 1. \tag{4.1}$$

The solution of (4.1) was found by Hermite **(5)** and may be written (with $u \neq 0$, v square-free, $\bar{A} = \operatorname{adj} A$):

$$x_0^2 - df(x) = u^2 v, \tag{4.2}$$

$$u^2 v\,(I + S) = 2x_0^2\, I + x_0 \bar{A}\,\dot{x} - dxx'A. \tag{4.3}$$

We shall need the following results:

LEMMA 1. (i) *Whenever x_0, x have integral values such that the left member of* (4.2) *does not vanish, $S = S(x_0, x)$ defined by* (4.2), (4.3) *satisfies* (4.1).

(ii) *Conversely, if S satisfies* (4.1) *there exist integral x_0, x, u, v satisfying* (4.2), (4.3); *the integer $v = v(A, S)$ is uniquely determined by A, S as are the ratios of x_0, x_1, x_2, x_3.*

(iii) *$I + S$ is singular if and only if $x_0 = 0$.*

(iv) *We have with the notation of* (3.1)

$$S(x_0, -x) = S^{-1}(x_0, x), \tag{4.4}$$

$$v(A, S_1 S_2) = v(A, S_1) \cdot v(A, S_2). \tag{4.5}$$

(v) *If the transformation T is non-singular, then*

$$v(T'AT, T^{-1}ST) = v(A, S). \tag{4.6}$$

Formulas (4.2) and (4.3) are not new; see, for example, Bachmann **(1**, pp. 81–108**)**. However, for completeness, we here give a proof in modern

notation based on Cayley's theorem **(3)** which is easily derived **(8**, p. 66**)**. This theorem states that if S is an automorph in a field F of a symmetric matrix A in F such that $I + S$ is non-singular, then there exists a skew matrix Q in F such that $A + Q$ is non-singular and

$$(A + Q)S = A - Q,$$

and that all such automorphs can be expressed in this form.

In our notation, $A\bar{A} = -2dI$. If we choose $x_0 \neq 0$ and x so that $d\dot{x} = x_0 Q$, the product

$$(A + Q)(2x_0^2 I + x_0 \bar{A}\,\dot{x} - dxx'A)$$

reduces to

$$2x_0^2 A - dAxx'A + d\dot{x}\,\bar{A}\,\dot{x}. \tag{4.7}$$

We shall verify below that the following identity holds:

$$\dot{x}\,\bar{A}\,\dot{x} + (x'Ax)A = Axx'A. \tag{4.8}$$

Using this, (4.7) reduces to $\{2x_0^2 - 2df(x)\}\,A$ which, in virtue of the non-singularity of $A + Q$, yields formulas (4.2) and (4.3). Note that $I + S$ non-singular implies $x_0 \neq 0$. This, subject to verification of (4.8), completes the proof of sections (i) and (ii) for $I + S$ non-singular.

If $I + S$ is singular, a theorem of Stieltjes **(12)** states that $I + S$ is not of rank 2, a result not hard to verify directly. The theorem of Jones and Marsh **(7)** establishes our result or it may be proved as follows: $I + S$, being of rank 1, must be equal to $xy'A$ for two column vectors x and y. Then $S'AS = A$ yields

$$Ayx'Axy'A = Axy'A + Ayx'A.$$

Multiplying on the right by $A^{-1}\dot{y}$ and on the left by A^{-1} we see that $yx'\dot{y} = 0$, $x'\dot{y} = 0$ and hence $y = \lambda x$ for some non-zero scalar λ. Then $\lambda^2(x'Ax)xx' = 2\lambda xx'$ which implies $\lambda f(x) = 1$.

It remains to verify (4.8). This is easily done directly for A a diagonal matrix. Suppose B is any symmetric matrix with rational elements. There is a matrix T of determinant 1 with rational elements such that $B = T'AT$. Then, letting $x = Ty$, we have $\bar{A} = T\bar{B}T'$ and (4.8) becomes a similar expression with x and A replaced by y and B by use of the following identity

$$R'(\dot{R}y)\,R = |R|\dot{y}, \tag{4.9}$$

which may be shown as follows: since $R'(\dot{R}y)R$ is skew, call it $\dot{x}$ and see that $\dot{x}y = 0$ implies that $y = g(R)x$, where $g(R)$ is a scalar dependent on R but not on y or x. Let I_{ij} and I_{ir} be the matrices obtained from I by interchaning the ith and jth rows, multiplying the ith row by r, respectively. Then it is easily shown that

$$g(I) = 1,\ g(I_{ij}) = -1,\ g(I_{ir}) = r,\ g(RS) = g(R)g(S).$$

Thus, $g(R)$ is a linear homogeneous function of the elements of each row of R and changes sign when two rows of R are interchanged. Since $g(I) = 1$, this implies from Weierstrass that $g(R) = |R|$.

Assertion (iii) is now obvious.

To obtain (4.4), note that with $(A + Q)S = A - Q$ we have $(A - Q)S^{-1} = A + Q$. Hence we may replace x_0, x, S, Q by $x_0, -x, S^{-1}, -Q$ in the foregoing argument, in the general case. In case $I + S$ is singular, we have only to prove $S^{-1} = S$ or $S^2 = I$. This is easily verified from (4.2), (4.3) with $x_0 = 0$.

To obtain (4.6), note that (4.2), (4.3) are unaltered (apart from multiplication of (4.3) on the left by T^{-1} and on the right by T) on putting $T'AT$, $T^{-1}ST$, $T^{-1}x$, tx_0 for A, S, x, x_0.

It remains only to establish (4.5). This is best done by using quaternions, following Eichler **(4)**, Pall **(11)** and others. We use a generalized quaternion algebra with multiplication defined by

$$(x_0, x)(y_0, y) = (x_0y_0 + \tfrac{1}{2}dx'Ay, \quad x_0y + y_0x - \tfrac{1}{2}\bar{A}\dot{x}y). \tag{4.10}$$

The vector x may be identified with the pure quaternion $(0, x)$; and the scalar x_0 with $(x_0, 0)$. The conjugate of (x_0, x) is $(x_0, -x)$, and its norm is $(x_0, -x)(x_0, x)$, which by (4.10) is $x_0^2 - df(x)$.

It is easily verified that (4.10) defines an associative algebra. The verification may be simplified by the device used in the proof of (4.8); for (4.10) is invariant under substitution of $T'AT$, $T^{-1}x$, $T^{-1}y$, where $|T| = 1$, for A, x, y. Thus we may suppose A to be diagonal and then (4.10) takes a familiar form. From the fact that multiplication is associative, it follows that the norm is multiplicative. Thus (4.5) will follow if we show that (4.2), (4.3) are equivalent to

$$(x_0, -x)(0, \xi)(x_0, x) = (x_0, -x)(x_0, x)(0, S\xi). \tag{4.11}$$

Noting that $\dot{\xi}x = -\dot{x}\xi$, we see that the left member of (4.11) is

$$(\tfrac{1}{2}dx_0\xi'Ax - \tfrac{1}{2}dx_0x'A\xi - \tfrac{1}{4}dx'A\bar{A}\,\dot{x}\xi, -\tfrac{1}{2}d(\xi'Ax)x + x_0^2\xi + \tfrac{1}{2}x_0\bar{A}\,\dot{x}\xi + \tfrac{1}{2}\bar{A}\,\dot{x}[x_0\xi + \tfrac{1}{2}\bar{A}\,\dot{x}\xi]).$$

The scalar component on the right is zero, and the vector component is

$$(x_0^2 + x_0\bar{A}\,\dot{x} - \tfrac{1}{2}dxx'A + \tfrac{1}{4}\bar{A}\,\dot{x}\,\bar{A}\,\dot{x})\xi,$$

since $(\xi'Ax)x = xx'A\xi$. On the other hand, after transposition of the term u^2vI, the right member of (4.3) becomes

$$x_0^2\,I + x_0\bar{A}\,\dot{x} - dxx'A + \tfrac{1}{2}d(x'Ax)I.$$

To prove (4.11) equivalent to (4.2), (4.3) we have therefore to show that

$$\tfrac{1}{2}dxx'A + \tfrac{1}{4}\bar{A}\,\dot{x}\,\bar{A}\,\dot{x} = \tfrac{1}{2}d(x'Ax)I.$$

We do so by multiplying (4.8) on the left by $\bar{A}$.

5. The denominator of the automorph S. It is clear from (4.3) that the denominator of S is a divisor of u^2v; we investigate whether any factor of u^2v can cancel out.

https://doi.org/10.4153/CJM-1956-064-0 Published online by Cambridge University Press

LEMMA 2. *Suppose* $(p, d) = (x_0, x_1, x_2, x_3) = 1$, *and let* p^α *be the highest power of* p *dividing* u^2v *and all the elements of the matrix* u^2vS; *then* $p^\alpha = 1$ *or* 4 *and divides also all elements of* u^2vS^{-1}. *Suppose* r *is the greatest integer prime to* d *that divides* u^2v; *then the denominators of* S *and* S^{-1} *have the same factor prime to* d, *which is either* r *or* $\frac{1}{4}r$, *provided* $(r, x_0, x_1, x_2, x_3) = 1$.

Proof. It is easily verified that the trace of $\bar{A}\dot{x}$ is identically zero; that of $xx'A = (x_i \partial f/\partial x_j)$ is $2f(x)$. We have therefore, from (4.3),

$$u^2v \operatorname{tr}(I + S) = 6x_0^2 - 2df(x) = 2u^2v + 4x_0^2. \tag{5.1}$$

If we multiply (4.3) on the right by $\bar{A}$, we see that, with the present hypothesis regarding p^α, we have

$$2x_0^2 \bar{A} + x_0 \bar{A}\, \dot{x}\, \bar{A} + 2d^2xx' \equiv 0 \pmod{p^\alpha}.$$

The second matrix on the left is skew, the other two symmetrical, so we deduce (by adding the transposed congruence)

$$4x_0^2 \bar{A} + 4d^2xx' \equiv 0 \pmod{p^\alpha}.$$

With (5.1) this gives that p^α divides $4x_0^2$ and $4d^2xx'$, hence $4xx'$. Now the hypothesis $(x_0, x_1, x_2, x_3) = 1$ gives $p^\alpha = 1$, 2 or 4.

To complete the proof of the first assertion, it only remains to show that if $2|u^2v$ and $u^2v\, S$ then 4 divides u^2v and both of $u^2vS^{\pm 1}$. This is easily proved on using (2.3). The second assertion is an obvious corollary of the first. We next prove

LEMMA 3. *If the denominator of* $S = S(0, x)$ *is prime to* p, *then* $v = v(S) \in \Gamma(p, f)$; *and the two definitions of this group given in* §3 *are equivalent.*

Proof. Putting $x_0 = 0$ in (4.2) and (4.3), and supposing without loss of generality that $p \nmid x$, we see that for some $\delta \geqslant 0$ we must have

$$p^\delta \| f(x) = -d^{-1}u^2v, \quad p^\delta | xx'A, \quad p^\delta | x'A. \tag{5.2}$$

Hence (3.1) and (3.3) are satisfied with $t = x$, $b = f(x)$, and $v \in \Gamma(p, f)$ follows.

We see from (3.1), (3.3) that $\Gamma(p, f)$ is generated by the group of f with $(v|p) = 1$, or $v \equiv 1 \pmod 8$, together with those given by

$$v \equiv p^\epsilon v' \pmod{p^{2+(-1)^p+\epsilon}}, \qquad \epsilon = 0 \text{ or } 1, \ p \nmid v' \tag{5.3}$$

for ϵ, v' such that (5.2) can be satisfied with $v = p^\epsilon v'$ and with $p \nmid x$; but note that if $p|x$ we may put $\delta - 2$, $p^{-1}x$ for δ, x. We may, without loss, replace (5.2_1) by a congruence mod p^τ with $\tau = \delta + 2 + (-1)^p$ and take $u = 2p^\theta$ where θ is an integer dependent on δ and d so chosen that v has the form of (5.3).

We first dispose of the case when $p = 2$ and f is not diagonalizable. Using (2.2) (mod 2^τ), the condition on ϵ, v', obtained from (5.2) as explained above, becomes, since

$$d = -2^{2\lambda_1+\lambda_2} \cdot d', \qquad d' \text{ odd},$$

$$(5.4) \qquad 2^\delta v' \equiv d'\{2^{\lambda_1}\phi(x_1, x_2) + 2^{\lambda_2}ax_3^2\},\ 2^\delta | (2^{\lambda_1}x_1, 2^{\lambda_1}x_2, 2^{\lambda_2+1}x_3),$$

$$\epsilon \equiv \lambda_2 + \delta \pmod 2.$$

There are two types of solution of (5.4):

(i) If

$$2^{\delta+1} \nmid 2^{\lambda_1}\phi(x_1, x_2)$$

we must have

$$2^\delta || 2^{\lambda_1}\phi(x_1, x_2),\ \delta = \lambda_1, \qquad \phi \text{ odd}.$$

In particular, with $x_3 = 0$ we have solutions of this type with $\epsilon \equiv \lambda_1 + \lambda_2 \equiv \lambda \pmod 2$ and $v' = d'\phi(x_1, x_2)$. Since $d'\phi$ has an odd discriminant, we can have v' congruent to any odd integer mod 8.

(ii) If

$$2^{\delta+1} | 2^{\lambda_1}\phi(x_1, x_2),$$

then

$$2^\delta || 2^{\lambda_2}x_3^2,\ \delta \equiv \lambda_2 \pmod 2.$$

It easily follows that $\Gamma(2, f) = \Gamma$ or Γ_2 according as λ is odd or even.

Now with $p \geqslant 2$ assume (2.1), and the condition on ϵ, v' becomes

$$(5.5) \qquad p^\delta v' \equiv a_1a_2a_3 \sum_{i=1}^{3} a_i p^{\lambda_i}x_i^2,\ p^\delta | 2p^{\lambda_i}x_i$$

$$(i = 1, 2, 3),\ \epsilon \equiv \lambda_1 + \lambda_2 + \lambda_3 + \delta \pmod 2$$

The case p odd is straightforward. Let $p^{\rho_i} || x_i$. From (5.5)

$$\lambda_i + \rho_i \geqslant \delta \geqslant \min(\lambda_i + 2\rho_i).$$

Hence if i is the index for which $\lambda_i + 2\rho_i$ is a minimum, we have $\rho_i = 0$ and $\delta = \lambda_i$. Now if $\lambda_j + 2\rho_j = \lambda_i$ it follows that $\rho_j = 0$. Hence we have two possibilities:

(1) No two λ_k are equal and δ is equal to one of them.

(2) Two λ_k are equal.

Let i, j, k be 1, 2, 3 in some order and in the first case $\delta = \lambda_i$, $\epsilon \equiv \lambda_j + \lambda_k \pmod 2$ and $(v'|p) = (a_1a_2a_3a_i|p) = (a_ja_k|p)$ which is condition (ii) of the alternative definition of $\Gamma(p, f)$. In the second case, condition (iii) is easily verified.

For $p = 2$, trivial solutions of (5.5) are obtained as for odd p. To obtain any others differing from these either in the value of ϵ or in the residue of v' mod 8 we must for some i, j have

$$2^{\delta+1} \nmid 2^{\lambda_i}x_i^2,\ 2^{\delta+3} \nmid 2^{\lambda_i}x_j^2.$$

https://doi.org/10.4153/CJM-1956-064-0 Published online by Cambridge University Press

A little calculation shows that, with $(5.5)_2$, this requires

$$\lambda_i \leqslant \delta \leqslant \lambda_i + 2,\ \lambda_j - 2 \leqslant \delta \leqslant \lambda_j + 4,$$

and so is impossible when the differences of the λ_i are too large. When they are not, the calculations are straightforward and we leave the rest to the reader.

We next show that the first assertion of Lemma 3 is true for the automorph $S(x_0, x)$ without the restriction $x_0 = 0$. This can be proved by straightforward calculations similar to those of Lemma 3; but these are complicated for $p = 2$. We give an alternative proof, based on the fact that every S is a product of S's with $x_0 = 0$.

LEMMA 4. *If the denominator of $S = S(x_0, x)$ is prime to p, then*

$$v = v(S) \in \Gamma(p, f).$$

Proof. We begin by making some preliminary simplifications in the case $p = 2$. First, we assume that the exponents λ_i in (2.1) are not all equal, and that in (2.2) $\lambda \neq 1$; for in these two cases, which transform into each other, Lemma 3 gives us $\Gamma(2, f) = \Gamma$, and we have nothing to prove. Next, we note that in all other cases we either have

$$A \equiv \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \pmod 4, \tag{5.6}$$

if f satisfies (2.1) or (2.2), or the reciprocal form has this property. To show that we need only prove the Lemma for one of two reciprocal forms, put $T = \bar{A}$ in (4.6); after a little reduction this gives $v(-2d\bar{A}, S'^{-1}) = v(A, S)$. Here S'^{-1} is an automorph of and $-2d\bar{A}$ is a multiple of the coefficient matrix of the reciprocal form of f.

Now by (5.6), if $p = 2$, or (2.1), if $p > 2$, we may remove from $f(\xi)$ the terms in $\xi_1\xi_2$, $\xi_1\xi_3$. We do this by an obvious transformation with denominator prime to p, which affects neither the hypothesis nor the conclusion of this Lemma, nor the assumption (5.6); see (4.6). Thus we may assume (5.6) and

$$f(\xi) = a\xi_1^2 + g(\xi_2, \xi_3),\ p \nmid a, \tag{5.7}$$

where the binary form g has a divisor 2 if $p = 2$, by (5.6), and we may suppose that the coefficient of $\xi_2\xi_3$ is divisible by at least as high a power of p as that of ξ_2^2. Writing for convenience

$$y = (1, 0, 0)', \quad z = (0, 1, 0)'. \tag{5.8}$$

we must have that $t = z$ satisfies (3.1) and

$$z'Ay = 0. \tag{5.9}$$

For convenience write $U(t) = S(0, t)$, and note that $U(t)t = t$, $U(t)\xi = -\xi$ if $t'A\xi = 0$, as is clear from (4.2), (4.3) with $x_0, x = 0, t$.

First suppose that $Sy = -y$. Then Lemma 1 (iii) shows that $x_0 = 0$, whence $v(S) \in \Gamma(p, f)$ follows from Lemma 3.

Next suppose $Sy = y$. Then from (5.9) we have $U(z)Sy = -y$, and by the case just considered

$$v(U(z)S) = v(U(z)) \cdot v(S) \in \Gamma(p, f).$$

But as $t = z$ satisfies (3.1), $U(z)$ has denominator prime to p, so by Lemma 3 $v(U(z))$ is in $\Gamma(p, f)$ and so must be $v(S)$.

Now note that $U(y + Sy)$ takes $y - Sy$ into $Sy - y$, because

$$(y' + y'S')\, A\, (y - Sy) = y'S'Ay - y'ASy = 0,$$

and leaves $y + Sy$ invariant. Hence this transformation takes Sy into y. Similarly, $U(y - Sy)$ takes Sy into $-y$.

Our conclusion will thus follow from the special cases already considered if we can show that at least one of $y \pm Sy$ is a solution of (3.1). We have, however,

$$f(y \pm Sy) = \tfrac{1}{2}(y' \pm y'S')\, A\, (y \pm Sy) = 2f(y) \pm y'ASy = 2a \pm y'ASy,$$

and by proper choice of the sign $f(y \pm Sy)$ is not divisible by p, if $p > 2$, or 8, if $p = 2$.

This completes the proof for $p > 2$. For $p = 2$ we need to prove

$$4 \mid (y' \pm y'S')A,$$

i.e., if $y'S' = (\eta_1, \eta_2, \eta_3)$, $2 \mid (1 + \eta_1)$. This follows from (5.6) and $f(y) = f(Sy)$.

6. The groups and the automorphs. We construct automorphs with certain desired properties, making use of the assumption that f is indefinite.

LEMMA 5. *If f has an automorph S with denominator q in Γ_d, then $q \in \gamma(f)$. Conversely, suppose $q \in \gamma(f)$, whence by the definition of $\gamma(f)$ there exists a w with*

$$w \mid d,\ wq \in \bigcap_{p \mid d} \Gamma(p, f).$$

Then for every such w there exists an automorph S of f with $f(S) = wq$.

Proof. With $v(S) = wq$, $w = \pm (v, d)$, $(q, d) = 1$, the denominator of S must, if it is in Γ_d, be q or $-q$. For by Lemma 2 it must be qu_1^2 or $\frac{1}{4}qu_1^2$, u_1 some factor of u, and so it is square-free only if, with $u_1 = 1$ or 2, it is equal to q. Then the hypothesis of the first part of the Lemma gives, with Lemma 4,

$$v = wq \in \bigcap_{p \mid d} \Gamma(p, f),$$

whence $q \in \gamma(f)$. It turns out that the two cases $u_1 = 1, 2$ correspond to the same set of possible values of v, which simplifies our proof of the second assertion.

If now $v = wq \in \Gamma(p, f)$, suppose first that v is in the set of generators of $\Gamma(p, f)$ defined in §3. Take any solution of (3.1) with b satisfying (3.3) and construct the automorph $S(0, t) = S_1$, say. Plainly $v(S_1) = v_1$ is such that $v \cdot v_1$ is a quadratic residue modulo p or 8, if $p = 2$, and S_1 must have denomina-

https://doi.org/10.4153/CJM-1956-064-0 Published online by Cambridge University Press

tor prime to p, though possibly not square-free. We thus have a solution with $t_0 = 0$ of

$$t_0^2 - df(t) \equiv u^2 v \pmod{p^\beta}, \tag{6.1}$$

$$2t_0^2 I + t_0 \bar{A}\, \dot{t} - dtt'A \equiv 0 \pmod{p^\alpha}, \tag{6.2}$$

for α, β with $p^\alpha || u^2 v$, $\beta = \alpha + 2 + (-1)^p$.

By multiplying together two or more such automorphs S_1 we can construct a solution of (6.1), (6.2) when v, though in $\Gamma(p, f)$, is not one of the generators. From the solution thus found, we can obviously construct another in which u has no factor prime to p.

Next, if

$$v \in \bigcap_{p|d} \Gamma(p, f)$$

we can find t_0, t, u so that all the pairs of congruences (6.1), (6.2), for p ranging over the prime divisors of d, hold simultaneously; and so that u is a product of powers of primes all dividing d. Suppose now that we can solve

$$x_0^2 - df(x) = u^2 v;\ x_0, x \equiv t_0, t \pmod{p^\alpha}, \tag{6.3}$$

for each $p|d$. Then from (4.2), (4.3) it is clear that $S(x_0, x)$ has denominator prime to d, while the number r of Lemma 2 is q, so the denominator cannot be $\frac{1}{4}r = \frac{1}{4}q$ but must be q. Thus $S(x_0, x)$ will give us all we require.

We have therefore only to prove the solubility of (6.3). We note first the obviously necessary congruence condition, namely the solubility of

$$x_0^2 - df(x) \equiv u^2 v \pmod{p'^\theta}, \tag{6.4}$$

for every prime power p'^θ, subject to the restriction, vacuous if $p' \nmid d$, that the solution must satisfy $(6.3)_2$. The solubility of (6.4) for $p' \nmid d$ is obvious from (2.3); for, using (2.3), (5.4) becomes

$$x_0^2 - dx_1x_2 - d^2x_3^2 \equiv u^2 v.$$

So we take $p' = p$, $p|d$, and we may suppose $\theta = \beta$ by elementary properties of quadratic residues. Now the desired solution of (6.4), $(6.3)_2$ is $x_0, x = t_0, t$.

Hence the necessary condition is satisfied, and the proof is completed by remarking that it is also sufficient. For $x_0^2 - df(x)$ is a non-degenerate, indefinite form in more than three variables, and so a recent result of one of us **(13)** gives what is required.

7. Forms in the genus of f. Let the forms f, f_1 be in the same genus. This means, by the classical definition, that f goes into f_1 by a rational unimodular transformation with denominator prime to $2d$. Then by the classical theory we know that the transformation may be chosen so as to have its denominator prime to any prescribed positive integer. We can therefore find R_1, R_2, with denominators r_1, r_2, such that

$$f_1(\xi) = f(R_1\xi) = f(R_2\xi),\ (r_1, d) = (r_2, dr_1) = 1. \tag{7.1}$$

The following lemmas will tell us more about the possible values of the denominator.

LEMMA 6. *Suppose that q is square-free and prime to d and that qr_2 is a quadratic residue modulo every odd prime factor of dr_1, and also modulo 8 if dr_1 is even. Then Q may be found so that $f_1(\xi) = f(Q\xi)$ and Q has denominator q.*

Proof. By (7.1), $R_2R_1^{-1}$ and its reciprocal $R_1R_2^{-1}$ are automorphs of f whose denominators, dividing $r_1^2r_2$, $r_2^2r_1$, are prime to d and hence equal, by the last part of Lemma 2. Hence it is easily seen that each denominator must be equal to r_1r_2, whence by Lemmas 1 and 2 we must have

$$R_2R_1^{-1} = S(y_0, y),\ y_0^2 - df(y) = u_0^2u_1^2wr_1r_2, \tag{7.2}$$

with $w|d$, $u_1 = 1$ or 2, $(u_1, d) = 1$ and u_0 having no prime factor that does not divide d.

The conditions on q ensure that we can solve for θ,

$$u_1^2r_2\theta^2 \equiv q \pmod{d^4u_0^2wr_1^4},\ (\theta, dr_1) = 1. \tag{7.3}$$

We now seek a solution of

$$x_0^2 - df(x) = u_0^2wr_1q, \tag{7.4}$$

subject to

$$x_0 \equiv \theta y_0,\ x \equiv \theta y \pmod{u_0^2wr_1^2}. \tag{7.5}$$

By the result used in the proof of Lemma 5, (7.4) and (7.5) are soluble if, for every prime p, with $\alpha = \alpha(p)$ such that $p^\alpha || u_0^2wr_1^2q$, (7.4), treated as a congruence modulo p^β, has a solution consistent with (7.5) for any prescribed β. Now if $p \nmid dr_1$, (7.5) is vacuous and the solubility of (7.4) modulo p^β is trivial. On the other hand, if $p|dr_1$, (7.2) and (7.3) show that $x_0 = \theta y_0$, $x = \theta y$ is such a solution for a value of β certainly not less than $\alpha + 3$. We need not, by elementary properties of quadratic residues, consider any greater value of β; so (7.4) and (7.5) are simultaneously soluble.

We now show that $Q = S(x_0, x)R_1$, which clearly takes f into f_1, has denominator q. By (4.3), with $u^2v = u_0^2wr_1q$, and the corresponding equation for $S(y_0, y)$, and (7.3), we have the following congruences, in which the matrices occurring on both sides of the congruences are integral:

$$r_2u_0^2wr_1qS(x_0, x) \equiv r_2u_0^2wr_1qR_2R_1^{-1} \pmod{u_0^2wr_1^2},$$

$$qr_1r_2Q \equiv qr_1r_2R_2 \equiv 0 \pmod{r_1}.$$

Hence r_2qQ is integral, and so is qQ, since it has denominator prime to r_2. On the other hand, since R_1 is unimodular with denominator prime to q, if Q had as denominator a proper divisor of q, so would $S(x_0, x)$, contradicting Lemma 2. This completes the proof.

DEFINITION. $\gamma(f_1, f)$ is the set of all q in Γ_d that are denominators of matrices taking f into f_1, f_1 being any form in the genus of f.

Lemma 6 shows that the set $\gamma(f_1, f)$ is not empty; we prove

LEMMA 7. *$\gamma(f_1, f)$ is a coset of $\gamma(f)$ in Γ_d.*

Proof. We first show that if q_1 and q_2 are in $\gamma(f_1, f)$ then $q_1 \cdot q_2$ is in $\gamma(f)$. In case $(q_1, q_2) = 1$, this is clear; for with an obvious notation we see that the automorph $Q_2 Q_1^{-1}$ of f must, as in the proof of Lemma 6, have denominator $q_1 q_2 = q_1 \cdot q_2 \in \gamma(f)$.

If $(q_1, q_2) > 1$, we may argue as above with a suitably chosen q_3 prime to q_2 in place of q_1. We have only to make q_3 satisfy the sufficient condition of Lemma 6, with any r_1 prime to $q_1 q_2$, and with q_2 for r_2. This sufficient condition obviously ensures that q_2 and q_3 belong to the same coset of $\gamma(f)$ in Γ_d; and the conclusion of Lemma 6 gives $q_3 \in \gamma(f_1, f)$.

Conversely, we show that, with q_1, $\gamma(f_1, f)$ contains all q_2 in the coset to which q_1 belongs. This follows for $q_2 = q_0 q_1$, $(q_0, q_1) = 1$, $q_0 \in \gamma(f)$, if we replace Q_1 by SQ_1, S being an automorph of f with denominator q_0. When q_2 does not satisfy these conditions, we consider, as in the first part of the proof, a suitable q_3 that does. The conclusion follows.

We note some properties of the cosets $\gamma(f_1, f)$.

LEMMA 8. *$\gamma(f_1, f)$ depends only on the classes of f_1, f, $\gamma(f, f) = \gamma(f)$, $\gamma(f, f_1) = \gamma(f_1, f)$ and $\gamma(f_1, f_2) = \gamma(f_1, f) \cdot \gamma(f_2, f)$.*

Proof. The first two assertions are obvious. The first part of the proof of Lemma 6 shows that R_1 and R_1^{-1} must have the same denominator r_1; hence the third assertion, taking r_1 to be in $\gamma(f_1, f)$. To prove the last assertion, consider coprime representatives of the cosets $\gamma(f_1, f)$, $\gamma(f_2, f)$ and multiply the corresponding Q.

8. Proof of Theorem 1; a set of forms representing the genus. Theorem 1 follows from Lemmas 7, 8 if we show that every q in Γ_d is the denominator of a matrix taking f into a form in its genus. We do this by constructing certain forms which we shall also use for the proof of Theorem 2.

We may suppose, see (2.3), that, for any prescribed q in Γ_d,

$$f(\xi) \equiv \xi_1 \xi_2 + d\xi_3^2 \pmod{q^3}. \tag{8.1}$$

Putting $x_0 = 0$, $u^2 v = -dq$, and R for S in (4.2), (4.3), we define an automorph $R = R(x)$ of the form on the right of (8.1), for any x for which

$$x_1 x_2 + d x_3^2 = q \tag{8.2}$$

holds, by

$$q(I + R) = xx' \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 2d \end{pmatrix}. \tag{8.3}$$

By Lemma 2, R has denominator q, and we note that $R^2 = I$. Now we define $\psi = \psi(f, R)$ by

$$\psi(\xi) = f(R\xi) \equiv f(\xi) \pmod{q}. \tag{8.4}$$

https://doi.org/10.4153/CJM-1956-064-0 Published online by Cambridge University Press

When q is odd, ψ is in the genus of f, by the classical definition. This is also true for even q; to prove it we use the automorph $S(4, x)$ of f, and we verify from (4.2), (4.3), (8.1), (8.2), (8.3) that $S(4, x)R$ has an odd denominator prime to d.

For integral ξ, $R\xi$ is integral if

$$x'\begin{pmatrix}0 & 1 & 0\\ 1 & 0 & 0\\ 0 & 0 & 2d\end{pmatrix}\xi = x_1\xi_2 + x_2\xi_1 + 2dx_3\xi_3 \equiv 0 \pmod{q}. \tag{8.5}$$

By Lemmas 7, 8, the class of ψ depends only the coset of $\gamma(f)$ in Γ_d to which q belongs; so we are free to choose x so that any ξ in which we are interested satisfies (8.5).

LEMMA 9. *Given any q in Γ_d and any $\theta_1, \theta_2 \not\equiv 0, 0$, there exists an x satisfying* (8.2) *such that, for $R = R(x)$ defined by* (8.3), *$R\xi$ is integral when*

$$\xi_2\theta_1^2 + 2d\xi_3\theta_1\theta_2 - d\xi_1\theta_2^2 \equiv 0 \pmod{q}. \tag{8.6}$$

Proof. Without loss of generality we may suppose $\theta_1 = 1$. Then (8.6) becomes (8.5) and (8.2) holds, if $x_1, x_2, x_3 = 1, q - d\theta_2^2, \theta_2$.

We note that, regarding ξ as given and (8.6) as a quadratic congruence for the ratio $\theta_1 : \theta_2$, the discriminant of the congruence is $4d(\xi_1\xi_2 + d\xi_3^2)$, which by (8.4) is congruent to $4df(\xi)$ modulo q.

9. Representation of integers. We study in this section the representation of an integer $n \not\equiv 0$ by forms in the genus of f; and as in the statement of Theorem 2 we write $dn = n_1n_2^2$, n_1 square-free. We prove three lemmas and deduce Theorem 2.

LEMMA 10. *Suppose f_1 is the genus of f, $q \in \gamma(f_1, f)$, and f represents n. Then a sufficient condition for f_1 to represent n is that $(dn|p)$, the Legendre symbol, is* 0 *or* 1 *for each odd prime p dividing q.*

Proof. For any ξ with $f(\xi) = n$ we can solve (8.6) by the hypothesis of this Lemma (see the remark following Lemma 9). With the x, $R(x)$ whose existence is asserted by Lemma 9, consider the form $\psi = \psi(f, R)$ defined by (8.4). We have

$$n = f(\xi) = \psi(R^{-1}\xi) = \psi(R\xi), \tag{9.1}$$

and $R\xi$ is integral; so ψ represents n. But since $q \in \gamma(f_1, f)$ and f goes into ψ by R with denominator q, we see from the definition of $\gamma(f_1, f)$ and Lemmas 7, 8 that ψ is equivalent to f_1; hence f_1 represents n.

LEMMA 11. *If f represents n, then so does f_1 in the genus of f if there exist q_0, q_1 satisfying*

$$q_0|2n_2,\ q_0 \in \Gamma_d,\ q_1 \in \gamma(f_1, f),\ (q_0q_1, n_1) = 1, \tag{9.2}$$

$$\prod(n_1, q_0q_1)_p = 1 \tag{9.3}$$

https://doi.org/10.4153/CJM-1956-064-0 Published online by Cambridge University Press

where the symbol in (9.3) *is the Hilbert Symbol* (**6**, p. 27) *and the product is over all primes p dividing* n_1 *if d is odd or* $n_1 \not\equiv -1 \pmod 4$; *over all primes dividing* $2n_1$ *if d is even and* $n_1 \equiv -1 \pmod 4$.

Proof. By Dirichlet's theorem we may choose a positive prime

$$p_1 \equiv q_0 q_1 \pmod{d^3 n_1^3},\ p_1 \nmid 2n_2. \tag{9.4}$$

Then, taking $q = q_0 p_1$ in Lemma 10, we need only verify $(dn, p_1)_{p_1} = (n_1|p_1) = 1$.

Now (9.3) and (9.4) imply if d is odd or $n_1 \not\equiv -1 \pmod 4$,

$$1 = \prod_{p|n_1} (n_1, q_0 q_1)_p = \prod_{p|n_1} (n_1, p_1)_p.$$

By a fundamental property of the Hilbert symbol the last product is equal to $(n_1, p_1)_{p_1}\,(n_1, p_1)_\infty$ multiplied by $(n_1, p_1)_2$ if n_1 is odd; that is $(n_1|p_1)$ or $(n_1|p_1)(n_1, p_1)_2$ according as n_1 is even or odd. But $(n_1, p_1)_2 = 1$ if $n_1 \equiv 1 \pmod 4$, while if $n_1 \equiv -1 \pmod 4$ and d is odd we may choose $p_1 \equiv 1 \pmod 4$ consistent with (9.4). The case d even and $n_1 \equiv -1 \pmod 4$ is similar but simpler.

Putting $q_0 = q_1 = 2$, we see that f and f_1 represent the same integers if $2 \in \gamma(f_1, f)$. Notice that if d is odd and $n_1 \equiv -1 \pmod 4$ we can choose $p_1 \pmod 4$ consistent with (9.4) so that

$$1 = (n_1|p_1) = (n_1, p_1)_2 \prod_{p|n_1} (n_1, q_0 q_1)_p$$

whatever the value of the product in (9.3).

LEMMA 12. *Suppose f represents n. Then all forms in the genus of f represent n if* (*for suitable* p_1, p_2) *one of the following holds*:

$$q \in \Gamma(p_2, f),\ (q, n_1 d) = 1,\ p_2|n_1,\ (n_1, q)_{p_2} = -1, \tag{9.5}$$

$$n_1 < 0 \text{ or } n_1 \equiv -1 \pmod 4 \text{ with } d \text{ odd}, \tag{9.6}$$

$$q \in \gamma(f),\ (q, n_1) = 1,\ \prod (n_1, q)_p = -1, \tag{9.7}$$

$$p_1|2n_2,\ (p_1, n_1 d) = 1,\ \prod (n_1, p_1)_p = -1, \tag{9.8}$$

where the products are over the same range as in (9.3).

Proof. We first show that f_1 represents n if (9.5) holds and

$$(q|p) = 1 \text{ for each odd } p \neq p_2 \text{ dividing } dn_1, \text{ and} \tag{9.9}$$
$$q \equiv 1 \pmod 8 \text{ if } p_2 \neq 2.$$

We have from $(9.5)_1$, in case $p_2|d$, and (9.9), that

$$q \in \bigcap_{p|d} \Gamma(p, f);$$

thus q is in the subgroup of $\gamma(f)$ for which w may be taken equal to 1 in the definition of $\gamma(f)$. Thus if the product in (9.3) with $q_0 = 1$ is -1, then the product $\prod (n_1, q_1 q)_p$ is $+1$ since

$$\prod_{p|2n_1} (n_1, q)_p = \prod_{p|n_1} (n_1, q)_p = -1.$$

https://doi.org/10.4153/CJM-1956-064-0 Published online by Cambridge University Press

But $q \in \gamma(f)$ implies $q_1 q \in \gamma(f_1, f)$ and hence (9.5) and (9.9) are sufficient. But if (9.5) is soluble at all it must have a solution satisfying (9.9); for the two formulae, for given p_2, are congruences for q to coprime moduli. Hence (9.5) alone is sufficient.

Next $(9.6)_2$ follows from the remark after the proof of Lemma 11. Suppose $n_1 < 0$. Then

$$\prod_{p|n_1} (n_1, -1)_p = (n_1, -1)_\infty = -1$$

if n_1 is even and $-(n_1, -1)_2$ if n_1 is odd. Both are -1 unless $n_1 \equiv -1 \pmod 4$. We have just excluded $n_1 \equiv -1 \pmod 4$ when d is odd. If d is even the product in (9.3) with $q_0 q_1$ replaced by -1 is over primes dividing $2n_1$ and hence is -1. Thus one of

$$\Pi(n_1, q_0 q_1)_p, \quad \Pi(n_1, -q_0 q_1)_p$$

is $+1$; we may put $-q_0$ for q_0 in (9.2), (9.3).

If (9.7) holds and (9.3) is denied for $q_0 = 1$, then $q_1 q$ is an element of $\gamma(f_1, f)$ and (9.3) holds for q_1 replaced by $q\, q_1$.

If (9.8) holds, then (9.3) can be satisfied either with $q_0 = 1$ or $q_0 = p_1$.

Proof of Theorem 2. We write as in the foregoing lemmas $dn = n_1 n_2^2$, n_1 square-free; and by the hypothesis of the theorem, some form f in the genus considered represents n, but there is at least one form in the genus that does not. It follows that none of the sufficient conditions of Lemma 12 can be satisfied, while that of Lemma 11 must fail for some f_1.

(i) Condition (9.6) gives us $n_1 > 0$. If $n_1 = 1$, (9.2) can be satisfied with $q_0 = 1$ and some q_1, and then (9.3) necessarily holds. Hence $n_1 > 1$.

(ii) Suppose $p_2 | n_1$, with p_2 odd. Then $(9.5)_3$, $(9.5)_4$ hold if $(q|p_2) = -1$ and so $(9.5)_1$ must fail for such q satisfying $(9.5)_2$. This means that $\Gamma(p_2, f)$ does not contain the group Γ_{p_2} of v prime to p_2. By the definition of d_0 this means that $p_2 | d_0$.

Now take $p_2 = 2$ in (9.5). Then $(9.5)_1$ must fail for $q \equiv 5 \pmod 8$, with which $(9.5)_2$ to $(9.5)_4$ can be satisfied. Hence 5 is not in $\Gamma(2, f)$; this means, by the definition of d_0, that $2 | d_0$. We have thus shown that $p_2 | n_1$ implies $p_2 | d_0$ and hence $n_1 | d_0$.

(iii) For odd d, $n_1 | d_0 | d$ and hence we have $n_1 \equiv 1 \pmod 4$ by $(9.6)_2$. If $n_1 \equiv 5 \pmod 8$, then (9.8) is satisfied by $p_1 = 2$. Hence $n_1 \equiv 1 \pmod 8$ for odd d.

(iv) By the hypotheses of this part of the theorem, $(9.8)_2$ and $(9.8)_3$ hold with $p_1 = p$; for by (ii) p prime to d cannot divide n_1, while $\Pi(n_1, p_1)_p$ reduces to $(n_1 | p_1)$. Hence $(9.8)_1$ must fail and $p = p_1$ does not divide n_2.

(v) From (ii) we see that $(9.7)_2$ is implied by $(9.7)_1$; hence the failure of (9.7) for any f_1 means that $\Pi(n_1, q)_p = 1$ for all q in $\gamma(f)$. This means that $\Pi(n_1, q)_p$ has a fixed value ± 1, say $\chi(f_1, f)$, for all q in $\gamma(f_1, f)$. Now Lemma 11, with $q_0 = 1$, tells us that f_1 represents n if $\chi(f_1, f) = 1$. We see from Lemma 8

https://doi.org/10.4153/CJM-1956-064-0 Published online by Cambridge University Press

that this condition holds for just half the classes in the genus. It may be, however (since the condition of Lemma 11 is only sufficient), that n is represented by some form f_2 with $\chi(f_2, f) = -1$. If so, we have to show that, contrary to hypothesis, all forms in the genus represent n. But Lemma 11, with this assumption regarding f_2, shows that either $\chi(f_1, f) = 1$ or $\chi(f_1, f_2) = 1$ is sufficient for representation of n by f_1. And from Lemma 8 it is clear that

$$\chi(f_1, f_2) = \chi(f_1, f)\ \chi(f_2, f) = -\chi(f_1, f).$$

The proof of the assertion (v) is thus complete.

References

1. P. Bachmann, *Die Arithmetik der quadratischen Formen* (Leipzig and Berlin, 1925).
2. H. Brandt, *Ueber Stammfaktoren bei ternären quadratischen Formen*, Ber. Ver. Sächsischen Akad. Wiss. zu Leipzig, Math.-nat. Klasse, *100.1* (1952), 24 pp.
3. A. Cayley, *A memoir on the automorphic linear transformation of a linear bipartite quadric function*, Phil. Trans. Roy. Soc. London *148* (1858), 39–46.
4. Martin Eichler, *Quadratische Formen and orthogonale Gruppen* (Berlin, 1952).
5. Ch. Hermite, *Sur la théorie des formes quadratiques ternaires indéfinies*, Jour. für Math. *47* (1854), 307–312.
6. B. W. Jones, *The arithmetic theory of quadratic forms* (New York, 1950).
7. B. W. Jones and Donald Marsh, *Automorphs of quadratic forms*, Duke Math. J. *21* (1954), 179–193.
8. C. C. MacDuffee, *The theory of matrices* (Berlin, 1933).
9. Donald Marsh, *An investigation of the number of classes in the genus of certain indefinite ternary quadratic forms*, unpublished thesis, University of Colorado (1953).
10. A. Meyer, *Ueber indefinite ternäre quadratische Formen*, J. für Math. *113* (1894), 186–206; *114* (1895), 233–254; *115* (1896), 150–182; *116* (1896), 307–325.
11. Gordon Pall, *On generalized quaternions*, Trans. Amer. Math. Soc. *59* (1946), 280–332. Also, *Quaternions and Sums of Three Squares*, Amer. J. Math. *64* (1942), 503–513.
12. T. J. Stieltjes, *Un théorême d'algèbre*, Acta Math. *6* (1955), 319–320.
13. G. L. Watson, *Representation of integers by indefinite quadratic forms*, Mathematika *2* (1955), 32–38.

Queen Mary College, London
and
University of Colorado

University College
London