THE EQUIVALENCE OF QUADRATIC FORMS

G. L. WATSON

1. Introduction. The main object of this paper is to find the number of classes in a genus of indefinite quadratic forms, with integral coefficients, in $k \geqslant 4$ variables, distinguishing for even k two cases, according as improper equivalence is or is not admitted. (Two forms are in the same genus, according to the classical definition of Minkowski, if either is equivalent, for every positive integer m, to one identically congruent to the other modulo m.) Meyer **(5)** considered this problem, but obtained only a very incomplete result, included in Theorem 4 below. Otherwise little was known till recently. The results I prove could perhaps be obtained by suitable specialization of the very deep work of Eichler **(2)**; but it seems worth while to give a more elementary treatment of the case when the coefficients and variables are in the ring of ordinary integers.

The present paper may be regarded as a sequel to **(3)**, which gives the result for $k = 3$. It is, however, independent of **(3)** in so far as the results for $k \geqslant 4$ are concerned. It turns out that the formula giving the exact value of the class-number (in either sense) for an indefinite form with $k \geqslant 3$ gives a lower bound for that of any form with $k \geqslant 3$. The forms considered are not therefore assumed to be indefinite unless so stated; nor (since the proofs are partly by induction on k) to have $k \geqslant 4$.

2. Notation. Small letters denote rational integers unless otherwise stated, p being a prime and $(n|p)$ $(p \neq 2)$ the Legendre symbol. (m, n) denotes as usual the greatest common divisor of m, n. The set of all square-free integers $(v, v_1, \dots)$ constitutes, with the operation

$$v_1 \cdot v_2 = v_1 v_2 (v_1, v_2)^{-2}, \tag{2.1}$$

a group, denoted by Γ. Any subset of Γ closed under this operation is a subgroup; so in particular is Γ_d, the subset with $(v, d) = 1$.

Latin capitals denote square matrices, of rank k unless otherwise indicated, with rational elements, I being the identity matrix. By the denominator of a matrix is meant the least common multiple of the denominators of its elements, and the determinant is denoted by modulus signs. The notation $[m_1, \dots, m_k]$ is used for a diagonal matrix; and similarly for a matrix made up of diagonal blocks. Transposition is indicated by an accent. Column vectors, or $k \times 1$ matrices, are written $\mathbf{x} = \{x_1, \dots, x_k\}$ and have integral elements unless otherwise stated.

Received September 6, 1956; in revised form April 24, 1957.

https://doi.org/10.4153/CJM-1957-061-4 Published online by Cambridge University Press

Congruences, vector or scalar, in which either side is fractional, but with denominator prime to the modulus, are to be interpreted in the usual way. $m|n$, $m \nmid n$, $p^\alpha||n$ denote respectively that m divides n, m does not divide n, p^α divides n but $p^{\alpha+1}$ does not.

3. The matrix and discriminant of a form. These are defined (see, for example, Brandt, **1**) without putting in the Gaussian binomial coefficients. That is, $a_{ij} = a_{ji}$ is the coefficient of $x_i x_j$ in $f(\mathbf{x}) = f(x_1, \ldots, x_k)$, and with the form f we associate the matrix

$$A = \left(\frac{\partial^2 f(x)}{\partial x_i \partial x_j} \right)$$

with elements $2a_{ii}$ and a_{ij} $(i \neq j)$. This gives $f(\mathbf{x}) = \frac{1}{2}\mathbf{x}'A\mathbf{x}$ in place of the "classical" $\mathbf{x}'A\mathbf{x}$. Since f is assumed to have integral coefficients, A has integral elements, those on its diagonal being even. It is thus congruent (mod 2) to a skew matrix, which for odd k is singular. The discriminant of f, defined by

$$d = d(f) = \begin{cases} (-1)^{\frac{1}{2}k}|A| & \text{for } k \text{ even} \\ \frac{1}{2}(-1)^{\frac{1}{2}(k-1)}|A| & \text{for } k \text{ odd} \end{cases}$$

is therefore always integral; and we assume always that f is not degenerate, that is, that $d \neq 0$.

If p^β is any power of a prime p not dividing d, then by a suitable integral unimodular transformation we may suppose **(1)** that, for odd k,

$$3.1 \qquad f(\mathbf{x}) \equiv x_1 x_2 + \ldots + x_{k-2}x_{k-1} + dx_k^2 \pmod{p^\beta},$$

or for even k,

$$3.2 \qquad f(\mathbf{x}) \equiv x_1 x_2 + \ldots + x_{k-3}x_{k-2} + \phi \pmod{p^\beta},$$

where ϕ is any binary form, with discriminant d, in x_{k-1}, x_k. Similarly we may suppose **(6)** for any odd p^β, whether or not p divides d, that

$$3.3 \qquad f(\mathbf{x}) \equiv \sum_{i=1}^{k} p^{\lambda_i} a_i x_i^2 \pmod{p^\beta}, \qquad p \nmid a_1 \ldots a_k,$$

where the exponents λ_i may be supposed arranged in ascending order. For $p = 2$ we must replace 3.3 by **(6**, 35, Lemma 3**)**

$$3.4 \qquad f(\mathbf{x}) \equiv \sum_{\rho=1}^{\nu} 2^{\mu_\rho}\phi_\rho(x_{2\rho-1}, x_{2\rho}) + \sum_{i=2\nu+1}^{k} 2^{\lambda_i} a_i x_i^2 \pmod{2^\beta}.$$

Here $0 \leqslant \nu \leqslant \frac{1}{2}k$, the a_i are odd, and the binary forms ϕ_ρ have odd discriminants d_ρ. The properties of such a form depend on the residue (1 or -3) of d_ρ (mod 8); but we shall see that this distinction is irrelevant for our purpose.

From 3.1, 3.2 we see that the arithmetical properties of f to a modulus prime to d are trivial; they are given uniquely when k and d are known. The properties of f to any modulus may thus be studied by means of 3.3, 3.4, with p ranging over the divisors of d; and it is convenient to replace this system of

https://doi.org/10.4153/CJM-1957-061-4 Published online by Cambridge University Press

congruences by a single one, with a power of d as modulus; we shall see that the fourth power of d is high enough. Combining the results 3.3, 3.4 (for $p|d$) we see that we may suppose

$$3.5 \qquad f(\mathbf{x}) \equiv \sum_{\rho=1}^{\nu} \{q_{2\rho-1}n_{2\rho-1}(x_{2\rho-1} - \tfrac{1}{2}x_{2\rho})^2 + \tfrac{1}{4}q_{2\rho}n_{2\rho}x_{2\rho}^2\} + \sum_{i=2\nu+1}^{k} q_i n_i x_i^2 \pmod{d^4}.$$

Here the n_i are products of primes dividing d, while the q_i may without loss of generality be taken to be in Γ_{2d}; ν is as in 3.4 if d is even, 0 otherwise; and for $\rho = 1, \ldots, \nu$ we must have

$$2^{\mu_\rho}||n_{2\rho} \equiv -q_{2\rho-1}q_{2\rho}n_{2\rho-1} \pmod{2^{\mu_\rho+2}},$$

the expression in $\{\}$ being a binary form with odd discriminant, multiplied by

$$2^{\mu_\rho}.$$

Alternatively, we might obtain 3.5 by the same elementary method (essentially completing the square) which gives 3.3, 3.4.

We see from 3.5 that

$$3.6 \qquad d \equiv (-4)^{[\frac{1}{2}k]}4^{-\nu}(q_1 \ldots q_k)(n_k \ldots n_k) \pmod{d^4},$$

whence $4^{[\frac{1}{2}k]-\nu}n_1 \ldots n_k$ is a divisor of d; so since the q_i are prime to d we must have

$$3.7 \qquad q_1 \ldots q_k \equiv \pm 1 \pmod{d^3}.$$

4. The groups and automorphs of a form. We define

$$4.1 \qquad U(\mathbf{t}) = U(\mathbf{t}, f) = U(\mathbf{t}, A) = I - \mathbf{t}\mathbf{t}'A/f(\mathbf{t}),$$

for $\mathbf{t}$ with $f(\mathbf{t}) \neq 0$. This matrix (which is $-U(\mathbf{t})$ in the notation of **(3)**) is well known, and may be immediately verified, to be an automorph of f, or of A. That is, we have identically $f(U(\mathbf{t})\mathbf{x}) = f(\mathbf{x})$. The first two of the following formulae are immediate consequences of 4.1, and as they show that $U(\mathbf{t})$ has linearly independent characteristic vectors with characteristic roots -1, $1, \ldots, 1$, the other two follow:

$$4.2 \qquad U(\mathbf{t})\mathbf{t} = -\mathbf{t}; \; U(\mathbf{t})\mathbf{x} = \mathbf{x}, \text{ if } \mathbf{t}'A\mathbf{x} = 0; \quad |U(\mathbf{t})| = -1; \; U^2(\mathbf{t}) = I.$$

Since 4.1 gives $U(n\mathbf{t}) = U(\mathbf{t})$ for $nf(\mathbf{t}) \neq 0$, we may allow fractional $\mathbf{t}$, and then we have for all non-singular R

$$4.3 \qquad U(R^{-1}\mathbf{t}, R'AR) = R^{-1}U(\mathbf{t}, A)R;$$

that is, any linear transformation takes U's into U's.

On the other hand, if we take $\mathbf{t}$ to be integral and primitive, that is, assume that the greatest common divisor of $t_1, \ldots, t_k$ (all integers) is 1, then some linear combination of the rows $t_i\mathbf{t}'A$ of the matrix $\mathbf{t}\mathbf{t}'A = (t_it_j)A$ is $\mathbf{t}'A$.

https://doi.org/10.4153/CJM-1957-061-4 Published online by Cambridge University Press

Hence if n is the greatest common divisor of $f(\mathbf{t})$ and the k elements of $\mathbf{t}'A$, then $n^{-1}f(\mathbf{t})$ is the denominator of $U(\mathbf{t})$. We are interested in $U(\mathbf{t})$ with denominator prime to d. The residue modulo d^3 of the denominator of $U(\mathbf{t})$ will be considered first.

We consider the n, $\mathbf{t}$, q satisfying

4.41 $\quad n|f(\mathbf{t}),$

4.42 $\quad n|\mathbf{t}'A,$

4.43 $\quad n|d,$

4.44 $\quad q \in \Gamma_d,$

4.45 $\quad f(\mathbf{t}) \equiv qn \pmod{d^4},$

4.46 $\quad qnf > 0$ if f is definite.

4.46 means that qn has the sign of f if f is a definite form; otherwise qn may be either positive or negative. These conditions 4.4 will be studied further in §5; meanwhile we define certain groups.

Definition of $\Gamma(f)$, $\Gamma^+(f)$. $\Gamma(f)$ is the subgroup of Γ_d generated by the set of q for which, for suitable integral $n = n(q)$, $\mathbf{t} = \mathbf{t}(q)$, conditions 4.4 can be satisfied. $\Gamma^+(f)$ is the subgroup (of index 1 or 2) of $\Gamma(f)$ generated by the products in Γ of pairs of such q.

There is a connection, which we shall investigate in §5, between conditions 4.4 and

4.51 $\quad p^\delta \| f(\mathbf{t}),$

4.52 $\quad p^\delta | \mathbf{t}'A,$

4.53 $\quad p^\delta | d,$

4.54 $\quad f(\mathbf{t}) \equiv b \pmod{p^{\delta+3}}.$

Definition of $\Gamma(p, f)$. $\Gamma(p, f)$ is the subgroup of Γ generated by the set of v given by

4.6 $\quad b_1 b_2 = u^2 v,\ u$ integral, $v \in \Gamma,$

where b_1, b_2 range independently over the set of b for which, for given p and suitable $\delta = \delta(b) \geqslant 0$, and integral $\mathbf{t} = \mathbf{t}(p)$, 4.5 can be satisfied.

When $p \nmid d$, 4.53 gives $\delta = 0$, while 4.54 is soluble (unless $k = 1$) for every b not divisible by p, as may be seen from 3.1 or 3.2; hence

4.7 $\quad \Gamma(p, f) = \Gamma_p$ if $p \nmid d.$

Here Γ_p (see §2) is the subgroup of Γ defined by $(v, p) = 1$.

All these groups are clearly unaltered if f is replaced

(i) by any equivalent form, or

(ii) by any form congruent to $f \pmod{d^4}$, and with the same signature and discriminant.

(To deduce (ii), note that 4.53 gives $p^{\delta+3} | d^4$ if $p|d$, and use 4.7 if $p \nmid d$.) It follows from the Minkowski definition that the groups are all invariants of the genus of f. We can now state our main result:

https://doi.org/10.4153/CJM-1957-061-4 Published online by Cambridge University Press

THEOREM 1. *Let f be a non-degenerate quadratic form, with integral coefficients, in at least three variables. Then* (i) *the number of classes in the genus of f is not less than the order of the factor group $\Gamma_{d(f)}/\Gamma(f)$ or $\Gamma_{d(f)}/\Gamma^+(f)$, according as improper equivalence is or is not admitted*;

(ii) $\Gamma(f) = \Gamma^+(f)$ *is a necessary condition for f to be improperly equivalent to itself*;

(iii) *if f is indefinite, then there is equality in* (i) *and the necessary condition in* (ii) *is also sufficient.*

It is clear that the value, or lower bound, given by this theorem for the class-number, in either sense, is always a power of 2

5. Relations between the groups. We show first that, for primitive $\mathbf{t}$, 4.41 and 4.42 imply 4.43; whence, if $p \nmid \mathbf{t}$, 4.51 and 4.52 imply 4.53. We may suppose, by an integral unimodular transformation, that $\mathbf{t} = \{1,0, \ldots, 0\}$. Then 4.41, 4.42 reduce to

$$n|a_{11},\ n|\{2a_{11}, a_{12}, \ldots, a_{1k}\}.$$

And the substitution $\mathbf{x} \rightarrow U(\mathbf{t})\mathbf{x}$ reduces to

$$x_1 \rightarrow -x_1 - a_{11}^{-1}(a_{12}x_2 + \ldots).$$

The leading element $2a_{11}$ of A is divisible by $2n$, and its first row and column by n, so $|A|$ is divisible by $(2n, n^2) = n$ or $2n$ according as n is odd or even, giving $n|d = \pm|A|$ or $\pm\frac{1}{2}|A|$.

It follows now that when 4.4 holds $U(\mathbf{t})$ has denominator $n^{-1}f(\mathbf{t}) \equiv q \pmod{d^3}$. For if not, then 4.41, 4.42 would hold also with np, $p^{-1}q$ for n, q, p a prime not dividing d, whence $np \nmid d$. It also follows that the possibilities for q are the same whether or not $\mathbf{t}$ in 4.4 is restricted to be primitive. Similarly, it does not matter whether or not we allow $\mathbf{t}$ in 4.5 to be divisible by p; the possibilities for b are the same in either case, up to a square factor, which in view of 4.6 does not matter.

To reconcile the definition of $\Gamma(p, f)$ with that given, for $k = 3$, in (3), we show that, for odd k, 4.6 may be replaced, in the definition of $\Gamma(p, f)$, by

$$5.1 \qquad (-1)^{\frac{1}{2}(k-1)}db = u^2v,\ u \text{ integral},\ v \in \Gamma.$$

For $p \nmid d$ this is clear from 4.7. If $p \mid d$, we note that the numbers $q_i n_i$ of 3.5 are admissible values of b; the corresponding $\mathbf{t}$ are the vectors making all but one of the squares in 3.5 vanish. It is clear that in 4.6 we may allow b_2 alone to vary, and replace b_1 by a fixed product of an odd number of b. Using the b just found, 3.6 gives the desired result.

Similarly we show that

$$5.2 \qquad \Gamma(f) = \Gamma^+(f), \qquad k \text{ odd}.$$

Since every f is trivially equivalent to itself by $\mathbf{x} \rightarrow -\mathbf{x}$, which is an improper equivalence for odd k, 5.2 shows that the assertions of Theorem 1 simplify

https://doi.org/10.4153/CJM-1957-061-4 Published online by Cambridge University Press

as they should for odd k, the distinction between proper and improper equivalence disappearing.

To prove 5.2, note that the n_i, q_i of 3.5 satisfy 4.4, with the same $\mathbf{t}$ as used in connection with 5.1. Their group product, together with $\Gamma^+(f)$, obviously generates $\Gamma(f)$. Hence 5.2 follows if we show that this group product, which by 3.7 is either a quadratic residue modulo d^3 or the negative of such a residue, is in $\Gamma^+(f)$. Now $\Gamma^+(f)$ contains -1, since we may put $-n$, $-q$ for n, q in 4.4; it also contains all quadratic residues modulo d^3, as we see by keeping n fixed in 4.4 and putting $m\mathbf{t}$ for $\mathbf{t}$, m prime to d, and $q' \equiv m^2q$ modulo d^3 for q. 5.2 follows.

The relation between $\Gamma^+(f)$ and the groups $\Gamma(p, f)$ is given by

LEMMA 1. *q is in $\Gamma^+(f)$ if and only if, for suitable $w = w(q)$ in Γ,*

5.31 $\qquad q \in \Gamma_d,$

5.32 $\qquad w|d,$

5.33 $\qquad wq \in \bigcap_{p|d}{}' \ \Gamma(p,f).$

where the accent denotes the exclusion of negative values of wq in case f is definite.

Proof. We note first that the set of q for which 5.3 can be satisfied is a group, say $\Gamma_+(f)$; for if w_1, q_1 and w_2, q_2 satisfy 5.3 then so do $w_1 \cdot w_2$ and $q_1 \cdot q_2$.

Now note that 4.4 implies 4.5 (with $b = qn$) for every p dividing d. For $p|d$ and $p^\delta|d$ together imply $p^{\delta+3}|d^4$. Hence, writing $n = wc^2$, $w|d$, in 4.4, we see that the "only if" of the lemma, that is, $\Gamma^+(f) \subseteq \Gamma_+(f)$, follows from the definitions of $\Gamma^+(f)$ and $\Gamma(p, f)$. (Note that the product of evenly many qn, or qw, of the same sign is always positive.)

Now to prove the "if," that is, $\Gamma_+(f) \subseteq \Gamma^+(f)$, we consider integers v in Γ with the property that, for each $p|d$ and suitable u_p, $u_p{}^2v$ is an admissible value of b in 4.5, while vf is positive if f is definite. It is clear that products of pairs of such v generate the group on the right of 5.33, while the corresponding products of pairs of values of $\pm(v, d)^{-1}v$ generate $\Gamma_+(f)$. It suffices therefore to show that to each such v there is a u such that 4.4 can be satisfied with $qn = u^2v$. Now the condition that 4.5 can be satisfied with $b = u_p{}^2v$ is obviously satisfied, if at all, with u_p a power of p. So we suppose u_p is a power of p, and write $u = \Pi_p u_p$; clearly u^2v is an admissible value of b in 4.5 for every p dividing d. This is still true, by elementary properties of quadratic residues, if the exponent $\delta + 3$ in 4.54 is replaced by β such that $p^\beta||d^4$. Comparing 4.5, as thus modified, with 4.4 we see easily that, with $q = \pm\ (v, d)^{-1}v$, $qn = n^2\nu$, we can satisfy 4.41 to 4.45. And as 4.46 is satisfied (if applicable) by our choice of the sign of v, the proof is complete.

From 5.1 and Lemma 1 it follows that the group $\gamma(f)$ of **(3)** coincides with $\Gamma(f)$ and with $\Gamma^+(f)$ when $k = 3$ and f is indefinite.

Theorem 1 is true for imprimitive forms, and we shall later need to be free to exclude such forms or not, as convenient. So we prove that *the factor groups*

https://doi.org/10.4153/CJM-1957-061-4 Published online by Cambridge University Press

of Theorem 1 *are unaltered up to isomorphism if* f *is replaced by* mf, $m \neq 0$. We do this by showing that on so doing each of $\Gamma(f)$, $\Gamma^+(f)$, $\Gamma_{d(f)}$ is replaced by a subgroup of itself of index 2^σ, σ being the number of primes dividing m but not d. As far as $\Gamma_{d(f)}$ is concerned this is clear. For the other two groups it suffices to show that on the one hand q can satisfy 4.4 and have all or any of these p as divisors (which is trivial), while on the other hand if 4.4 holds with $(q, m) = 1$ it also holds with mn, q, mf for n, q, f. This last assertion depends on modifying the choice of $\mathbf{t}$ so as to satisfy 4.45 to a higher modulus; this is done as in the proof of Lemma 2 below, and is straightforward.

A similar argument gives

$$\Gamma(p, mf) = \Gamma(p, f) \text{ for } m \neq 0. \tag{5.6}$$

6. Construction of automorphs. To obtain an upper bound for the class-number, we need to construct automorphs, of the special type 4.1, with convenient properties; in particular, with equality in 4.45. We prove:

LEMMA 2. *Suppose that* f *is indefinite,* $k \geqslant 4$, 4.4 *holds, and also* $f(\mathbf{t}) \equiv qn \pmod{q^2}$. *Then there exists* $\mathbf{z}$ *satisfying*

$$\mathbf{z} \equiv \mathbf{t} \pmod{dq^2}, f(\mathbf{z}) = qn. \tag{6.1}$$

Proof. With the present hypotheses, and $d \neq 0$, it suffices, by the result proved in **(7)**, to show that a solution of 6.1 is not excluded by congruence considerations. In other words, we need only show that

$$\mathbf{z} \equiv \mathbf{t} \pmod{dq^2}, f(\mathbf{z}) \equiv qn \pmod{m} \tag{6.2}$$

can be satisfied for any prescribed $m \neq 0$, and suitable $\mathbf{z}$.

Suppose first $(m, dq) = 1$; then since $k > 2$ there is at least one product term in 3.1 or 3.2 (for any prime power factor of m) and so 6.2 is trivial. Next suppose $m = d^s$, $s \geqslant 5$. We can find $r \equiv 1 \pmod{d^3}$ so that $qn \equiv rf(\mathbf{t}) \pmod{d^s}$. Then we can solve $h^2 \equiv r \pmod{d^s}$; and it suffices to put $\mathbf{z} = h\mathbf{t}$. We may therefore suppose $m = q^s$, $s \geqslant 3$. Proceeding by induction on s, suppose $\mathbf{z} = \mathbf{x}$ satisfies 6.2 with $m = q^{s-1}$. Put $\mathbf{z} = \mathbf{x} + q^{s-1}\mathbf{y}$; then 6.21 holds, and 6.22 with $m = q^s$ reduces to

$$f(\mathbf{z}) \equiv f(\mathbf{x}) + q^{s-1}\mathbf{x}'A\mathbf{y} \equiv f(\mathbf{x}) + q^{s-1}\mathbf{t}'A\mathbf{y} \equiv qn \pmod{q^s}$$

This reduces to a linear congruence of the type $\mathbf{t}'A\mathbf{y} \equiv l \pmod{q}$, which is soluble for $\mathbf{y}$ unless some p dividing q, hence not dividing d, by 4.44, divides $\mathbf{t}'A$, and also, by hypothesis, $f(\mathbf{t})$. If so, then with $n = p$ 4.41 and 4.42 hold and 4.43 fails, which as shown at the beginning of §5 is impossible.

We deduce the

COROLLARY. *Suppose* f *is indefinite,* $k \geqslant 4$, *and* 4.4 *holds. Then there exists* $\mathbf{z}$ *with* $f(\mathbf{z}) = qn$ *such that* $U(\mathbf{z})$ *has denominator* q *and satisfies*

$$qnU(\mathbf{z}) = (p^2\xi_2, p\xi_2, \ldots, p\xi_{k-1}, \xi_k) \tag{6.3}$$

https://doi.org/10.4153/CJM-1957-061-4 Published online by Cambridge University Press

with integral ξ_i, for every p dividing q for which

$$p^2 | a_{11},\ p | a_{1j}, \qquad 1 < j < k. \tag{6.4}$$

Proof. We apply the lemma with a suitable $\mathbf{t}$. If p divides q but does not satisfy 6.4, any solution of $f(\mathbf{t}) \equiv qn \pmod{p^2}$ will do, and some solution clearly exists, by 3.1 or 3.2. If p divides q and satisfies 6.4, we require a solution of $f(\mathbf{t}) \equiv qn \pmod{p^2}$ which also satisfies

$$\mathbf{t} \equiv \{1, 0, \ldots, 0, q\theta\} \pmod{p^2}, \tag{6.5}$$

for some θ. The congruence $f(\mathbf{t}) \equiv qn \pmod{p^2}$ reduces, by 6.4, 6.5, to $a_{1k} q\theta \equiv qn \pmod{p^2}$, which is soluble since $p \nmid a_{1k}$. For $p | a_{1k}$ would with 6.4 give $p | d$, $(q, d) > 1$, contradicting 4.4.

Now 6.3 follows from 4.1, 6.4, 6.5 by a simple calculation.

7. Rational transformations. Denote by R a matrix, with determinant ± 1 and denominator prime to $d(f)$, which takes f into $f^R = f(R\mathbf{x})$ with integral coefficients. Impose for the moment, in case $d(f)$ is odd, the additional restriction that the denominator of R be odd. Then it is well known that every form in the genus of f is expressible as f^R, and conversely. (This is equivalent to saying that the Eisenstein-Smith definition of the genus by rational transformations is equivalent to that of Minkowski, which we have used.) The additional restriction on the denominator of R is easily removed, as we shall see.

Among the matrices R are included all automorphs S of f whose denominators are prime to $d(f)$, and also all products SR, since $f^{SR} = f^R$. For given R, we shall construct S so that if possible SR is simpler, in a sense to be defined, than R. The construction requires f to be indefinite, and $k \geqslant 4$.

It is not difficult to express R as

$$R = T[r_1 s_1^{-1}, \ldots, r_k s_k^{-1}]X, \quad |T| = 1, \quad |X| = |R|, \tag{7.1}$$

where the matrices T, X are integral, and the positive integers r_i, s_i satisfy $(r_i, s_i) = 1$ and

$$1 = r_1 | r_2 | \ldots | r_k, \quad 1 = s_k | s_{k-1} | \ldots | s_1. \tag{7.2}$$

The proof that this is possible is similar to the proof that 7.3, below, is possible, and so we omit it; but we note that the r_i, s_i depend only on R and not on T, X. For firstly, $r_1 s_1^{-1}$ is the largest positive rational fraction such that $r_1^{-1} s_1 R$ has integral elements. Next, $r_1 r_2 s_1^{-1} s_2^{-1}$ is the largest fraction such that all the 2×2 submatrices of R have determinants which are integral multiples of $r_1 r_2 / s_1 s_2$; and so on.

Similarly, we can for any p express R as

$$R = M[p^{\theta_1}, \ldots, p^{\theta_k}]N, \quad |M| = 1, \quad |N| = |R|, \quad \theta_1 \leqslant \theta_2 \leqslant \ldots \leqslant \theta_k, \tag{7.3}$$

where M, N have denominators prime to p, and the integers $\theta_i = \theta_i(R, p)$ depend only on i, R, p and not on M, N. The sum of these integers is obviously

https://doi.org/10.4153/CJM-1957-061-4 Published online by Cambridge University Press

zero, and they all vanish if p does not divide the denominator of R. To prove that R can be expressed in the form 7.3, suppose for the moment that M satisfying 7.32 has been suitably chosen. Then $\theta_1, \ldots, \theta_k$ and N may be chosen so that 7.31 holds, by simply taking out from each row vector of $M^{-1}R$ the highest possible power of p so as to leave a vector with denominator prime to p. If now 7.33 fails, then p must divide $|N|$, and we see that a higher power of p can be taken out from one of the rows after a suitable row operation on $M^{-1}R$, equivalent to a suitable modification of the choice of M.

Definition. We define $q(R)$ to be the product of all primes p for which the sum of the positive ones among the numbers $\theta_i(R, p)$ is odd.

LEMMA 3. *The integers* $\theta_i = \theta_i(R, p)$ *of* 7.33 *satisfy*

$$\theta_i = -\theta_{k+1-i}, \qquad 1 \leqslant i \leqslant k \tag{7.4}$$

and the r_i, s_i *of* 7.1 *satisfy* $r_i = s_{k+1-i}$, *whence* $r_i = 1$ *for* $i \leqslant \frac{1}{2}k$, *and* 7.1 *may be rewritten*

$$R = T[s_1^{-1}, \ldots s_l^{-1}, 1, s_l, \ldots, s_1]X, \tag{7.5}$$

where T, X *are integral,* $l = [\frac{1}{2}k]$, *and the* 1 *is to be omitted for even* k.

Proof. We use for the first time the hypothesis that f^R is integral. We suppose $p \nmid d$; otherwise the θ_i are all zero and 7.4 is trivial. It suffices to prove 7.4 since the remaining assertions follow easily. Suppose 7.4 false and let h ($\leqslant \frac{1}{2}k$) be the least i for which it fails. Suppose also $\theta_h + \theta_{k+1-h} < 0$; for otherwise we may replace f, R, θ_i by f^R, R^{-1}, $-\theta_{k+1-i}$.

Suppose further that $T = I$ in 7.1; for if not we may replace f, R by f^T, $T^{-1}R$. Then it easily follows that we can take $M = I$ in 7.3. It is easily seen that

$$f^{RN^{-1}}$$

is also integral, so we may suppose

$$R = [p^{\theta_1}, \ldots, p^{\theta_k}].$$

The coefficient of $x_i x_j$ in f^R is now $p^{\theta_i+\theta_j} a_{ij}$; so we must have

$$p|a_{ij} \text{ if } \theta_i + \theta_j < 0.$$

By 7.34 and our hypotheses regarding the θ_i, this gives

$$p|a_{ij} \text{ for } i \leqslant h, j \leqslant k + 1 - h.$$

This shows that the matrix A_0 derived from A by replacing by zero every element $2a_{ii}$ or a_{ij} ($i \neq j$) with $p|a_{ij}$ has rank $< k$. For the submatrix of A_0 consisting of its first h rows has rank $< h$.

Thus $|A_0| = 0$. If $p \neq 2$, this gives the contradiction $|A| \equiv |A_0| \equiv 0 \pmod{p}$, $p|d$. If $p = 2$, we may have $|A| = \pm 2d$, so we need to prove $|A| \equiv |A_0| \pmod 4$. If we consider the terms in the expansion of $|A|$ that vanish in that of $|A_0|$, we see that they are all even, and either occur in pairs

https://doi.org/10.4153/CJM-1957-061-4 Published online by Cambridge University Press

(because of the symmetry of A) or contain factors $2a_{ii}$ or $a_{ij}a_{ji} = a_{ij}^2 \equiv 0 \pmod 4$. This completes the proof.

COROLLARY. *We may assume* $T = I$ *in* 7.5 *and simultaneously that* 6.4 *holds for every* p *dividing the denominator of* R.

Proof. We have seen in the proof of the lemma that we may assume $T = I$, and that then 6.41 holds since by hypothesis $\theta_1 < 0$. Further, we have 6.42 for every j for which $\theta_1 + \theta_j < 0$. This is true by 7.34 and 7.5 unless $j \geqslant \frac{1}{2}(k+2)$.

We consider for simplicity the case in which $a_{1,k-1}$ and $a_{1,k}$ are the only a_{1j} not divisible by p; in this case, $\theta_1 = \theta_2 = -\theta_{k-1} = -\theta_k$. We can transform f so that 6.4 holds by a suitable matrix V^{-1}, where

$$V = \begin{pmatrix} I_{k-2} & 0 \\ 0 & W \end{pmatrix},$$

W being a 2×2 matrix. But then we have to put $T = V$ instead of $T = I$ in 7.5. We thus have $R = VDX$, where D denotes the diagonal matrix in 7.5. We may write instead $R = D(D^{-1}VD)X$ if $D^{-1}VD$ is integral. Now

$$D^{-1}VD = \begin{pmatrix} I_{k-2} & 0 \\ 0 & W_1 \end{pmatrix},$$

where W_1 is derived from W by multiplying the second row, and dividing the second column, by s_1/s_2. s_1/s_2 is an integer by 7.22, divisible exactly by

$$p^{-\theta_1+\theta_2} = p^{\theta_{k-1}-\theta_k} = p^0.$$

Hence W_1 can be integral, and $W \equiv I \pmod m$ for any assigned m prime to p, without restricting W in any way modulo p. The result follows.

When R is an automorph $U(\mathbf{z})$, the numbers s_i are easily found. By 4.3, with a suitable integral unimodular matrix in place of R, we may suppose $\mathbf{z} = \{1,0,\ldots,0\}$. The positive and zero θ_i are determined by 7.4 when the negative ones are known, and the latter are clearly the same for $U(\mathbf{z})$ as for $I - U(\mathbf{z}) = \mathbf{z}\mathbf{z}'A/f(\mathbf{z})$, which has only one non-zero row. Thus θ_i is zero for $1 < i < k$, $s_i = 1$ for $i \neq 1$, s_1 is the denominator of $U(\mathbf{t})$, and $p^{-\theta_1} || s_1$, as is easily seen.

Now we consider the effect on the θ_i of replacing R by $U(\mathbf{z})R$, with suitable $\mathbf{z}$. It is convenient to write

$$\theta_i = \theta_i(R,p),\ \theta_i' = \theta_i(U(\mathbf{z}),p),\ \theta_i'' = \theta_i(U(\mathbf{z})R,p),$$

and desirable to choose $\mathbf{z}$ so that

$$q(U(\mathbf{z})R) = q(U(\mathbf{z})).q(R). \tag{7.6}$$

We prove:

LEMMA 4. (i) *For suitable* $\mathbf{z}$, $U(\mathbf{z})$ *has denominator prime to* d, 7.6 *holds, and for each* p *dividing the denominator of* R *we may as we choose have either*

https://doi.org/10.4153/CJM-1957-061-4 Published online by Cambridge University Press

(a) $\theta_i' = 0$, $\theta_i'' = \theta_i$ $(1 \leqslant i \leqslant k)$ *or*

(b) $(\theta_1', \ldots, \theta_k') = (-1,0,\ldots,0,1)$ *and* $(\theta_1'', \ldots, \theta_k'')$ *is a permutation of* $(\theta_1 + 1, \theta_2, \ldots, \theta_{k-1}, \theta_k - 1)$.

(ii) *If* f *is indefinite and* $k \geqslant 4$ *we may further have any positive* q *for which* 4.4 *can be satisfied as the denominator of* $U(\mathbf{z})$, *provided only that if* p *divides the denominator of* R *then* $p|q$ *if and only if alternative* (b) *is chosen in* (i).

Proof. It is convenient to assume throughout that f is indefinite and $k \geqslant 4$, and use the Corollary to Lemma 2. In other cases, when only (i) is to be proved, a suitable congruence condition may replace the Diophantine equation 6.12.

Suitable congruence conditions modulo d^4, and modulo p for every p for which we wish to satisfy (a), will clearly give $U(\mathbf{z})$ with denominator prime to d and to every such p, so that for each such p all the θ_i' vanish. Then $\theta_i'' = \theta_i$ for each such p, as we see on premultiplying 7.3 by $U(\mathbf{z})$.

For the p for which we have to satisfy (b), we use the corollaries to Lemmas 2, 3. Multiplying 6.3 and 7.31, with $T = I$, the result easily follows.

For the p which divide the denominator of $U(\mathbf{z})$ but not that of R, we have all the θ_i zero, and $\theta_i'' = \theta_i'$ is proved just like (a). Thus for every p to be considered we see that the sum of the positive θ_i'' is congruent modulo 2 to the sum of the positive θ_i and θ_i'. Plainly this gives 7.6.

Assertion (ii) is now trivial on choosing q suitably in the corollary to Lemma 2.

8. Upper bound for the class-number. We prove:

THEOREM 2. *Every form* f^R, *with* R *satisfying the conditions of the last section, is in the genus of* f.

If f *is indefinite and* $k \geqslant 4$, *then the class of* f^R, *in the wide sense, depends only on the coset of* $\Gamma(f)$, *in* Γ_d, *to which* $q(R)$ *belongs; thus in particular* f^R *is equivalent to* f *if* $q(R)$ *is in* $\Gamma(f)$.

If $|R| = 1$ *similar results, but with* $\Gamma^+(f)$ *for* $\Gamma(f)$, *hold for proper equivalence.*

Proof. The first assertion is classical for R with odd denominator. If R has an even denominator (which is possible only if d is odd) then the following argument gives $f^R = f^V$ for some V with denominator odd and prime to d.

Now let f be indefinite, and $k \geqslant 4$. Note that, since the square of every element of Γ is 1, q_1 and q_2 are in the same coset of $\Gamma(f)$ in Γ_d if and only if $q_1.q_2$ is in $\Gamma(f)$.

Denote by Q a matrix satisfying the conditions imposed in §7 on R, and in addition

8.1 $$s_1(Q) = q \in \Gamma_d,\ s_i(Q) = 1 \text{ if } i \neq 1.$$

8.1 is equivalent, by 7.4, 7.5, to

8.2 $$\theta_1(Q,p), \ldots, \theta_k(Q,p) = -1,0,\ldots,0,1,$$

https://doi.org/10.4153/CJM-1957-061-4 Published online by Cambridge University Press

for each p dividing the denominator of Q. We have seen in the proof of Lemma 4 that every $U(\mathbf{z})$ with denominator q in Γ_d is a Q with $q(U(\mathbf{z})) = q$.

Now apply Lemma 4 repeatedly. At each step the sum of the positive θ_i may be made to decrease for any p for which it exceeds 1; and since we always take $U(\mathbf{z})$ to be a Q, the sum in question does not exceed 1 for any prime factor newly introduced into the denominator. Thus after sufficiently many steps we see that we have $SR = Q$, for some $S = \ldots U(\mathbf{z}_2)U(\mathbf{z}_1)$ which is an automorph of f. We have by 7.6

$$q(Q) = q(SR) = \ldots q_2 \cdot q_1 \cdot q(R),$$

where $q_1 = q(U(\mathbf{z}_1)), \ldots$. The numbers $q_1, q_2, \ldots$ may after a certain stage, when we have already cancelled out all unwanted factors from the denominator of R, be arbitrary positive numbers that are admissible values of q in 4.4. Their product in Γ may thus, by the definition of $\Gamma(f)$, be any element of $\Gamma(f)$. We thus have $SR = Q$ with any $q(Q)$ in the coset of $\Gamma(f)$, in Γ_d, to which $q(R)$ belongs.

Now if $q(R)$ is in $\Gamma(f)$ we take $q(Q) = 1$, which by 8.1 makes Q integral, so that $f^R = f^{SR} = f^Q$ is equivalent to f. This proves the third assertion.

To prove the second assertion, take any two forms

$$f^{R_1}, f^{R_2}$$

which have $q(R^1) \cdot q(R^2)$ in $\Gamma(f)$, which are to be proved equivalent. Express them, by the foregoing construction, as

$$f^{Q_1}, f^{Q_2}$$

where $q(Q_1) \cdot q(R_1)$ and $q(Q_2) \cdot q(R_2)$ are in $\Gamma(f)$, whence $q(Q_1) \cdot q(Q_2)$ is in $\Gamma(f)$. We prove the second assertion by applying the third with f^{Q_1}, $Q_1^{-1}Q_2$ for f, R. Since f^{Q_1} is in the genus of f, it has the same groups as f, and we need only show that $q(Q_1^{-1}Q_2)$ is in $\Gamma(f)$.

It is easily seen that we may take $q(Q_2)$ to be prime to $q(Q_1)$; for $q(Q_2)$ can be any positive integer in the same coset of $\Gamma(f)$ in Γ_d as $q(R_2)$. 8.1 with 7.5 shows that Q_1^{-1} is also a Q, with denominator $q(Q_1^{-1}) = q(Q_1)$ prime to $q(Q_2)$. Hence as in the proof of Lemma 4 we see that

$$q(Q_1^{-1} Q_2) = q(Q_1^{-1}) \cdot q(Q_2) = q(Q_1) \cdot q(Q_2),$$

which is in $\Gamma(f)$, as was to be proved.

To prove the result for proper equivalence we proceed in the same way. But since the matrices $U(\mathbf{z})$ have determinant -1 by 4.23, we must pre-multiply by evenly many of them; the corresponding products of evenly many q given 4.4 generate $\Gamma^+(f)$.

If $k \geqslant 3$, transform f so that 3.1 or 3.2 holds, with $\beta = 2$, for each $p|q$, for suitable q in Γ_d. Then

$$Q = [q, q^{-1}, 1, \ldots, 1]$$

https://doi.org/10.4153/CJM-1957-061-4 Published online by Cambridge University Press

takes f into f^Q in the genus of f, and in a class determined by the coset of $\Gamma(f)$ or $\Gamma^+(f)$ in Γ_d to which $q(Q) = q$ belongs. Theorem 2 shows that this construction, with q ranging over a set of representatives of the cosets in question, yields a representative of each class in the genus of f, provided $k \geqslant 4$ and f is indefinite.

9. Lower bound for the class-number (preliminary). We shall deduce Theorem 1 from Theorem 2 and

THEOREM 3. *Let S by an automorph of f with denominator prime to $d(f)$. Then $q(S)$, defined in §7, is in $\Gamma(f)$ in any case, and in $\Gamma^+(f)$ if and only if either $\Gamma(f) = \Gamma^+(f)$ or $|S| = +1$.*

It is difficult to prove this theorem directly. We shall deduce it for $|S| = +1$ from Lemma 7; and we note here that the result for $|S| = -1$ then follows on considering $U(\mathbf{z})S$, for suitable $\mathbf{z}$, and using 7.6.

Deduction of Theorem 1 *from Theorems* 2,3. We consider first assertion (ii). Suppose f has an integral automorph S with $|S| = -1$. Then obviously $q(S) = 1 \in \Gamma^+(f)$. So by Theorem 3 we have $\Gamma(f) = \Gamma^+(f)$. This shows that assertion (i) need only be proved for unrestricted equivalence.

Now consider the forms f^Q constructed in §8, with q ranging over a set of representatives of the cosets in Γ_d of $\Gamma(f)$. Theorem 1(i) follows if we prove that these forms are all inequivalent. As in the proof of Theorem 2 this can be reduced to proving that f^Q, with $q(Q) = q$, is not equivalent to f unless q is in $\Gamma(f)$. Now if $f^{QT} = f$, T integral, then QT is an automorph of f and so $q(QT) \in \Gamma(f)$, by Theorem 3. But clearly $q(QT) = q(Q)$.

Theorem 1(iii) now follows for $k \geqslant 4$ (and f indefinite), as far as unrestricted equivalence is concerned, since by Theorem 2 every form in the genus is equivalent to one of the f^Q. For proper equivalence, we modify the construction of the set of forms f^Q by making q range over a set of representatives of the cosets of $\Gamma^+(f)$. (For $k = 3$, see **3**, Theorem 1.)

10. The groups $\Gamma(p, f)$. We shall see, in Theorem 4, that Theorem 2 is in most cases (when f is indefinite) sufficient to prove that the class number is 1. Theorem 2 also tells us whether two given forms in the same genus are equivalent, provided that we can find an R by which they are related (which is not very difficult) and determine the groups $\Gamma(f)$, $\Gamma^+(f)$. In §5 we have seen how to find a q in $\Gamma(f)$ which, adjoined to $\Gamma^+(f)$, generates $\Gamma(f)$. Lemma 1 then determines $\Gamma^+(f)$, if we can determine the groups $\Gamma(p, f)$. In so doing, we shall throughout this section assume 3.3 or 3.4, with a suitable sufficiently large β.

We may thus replace the A in 4.52 by

$$[p^{\lambda_1}, \ldots, p^{\lambda_k}]$$

if $p \neq 2$, and by

$$[2^{\mu_1}, 2^{\mu_1}, \ldots, 2^{\mu_\nu}, 2^{\mu_\nu}, 2^{\lambda_{\nu+1}}, \ldots, 2^{\lambda_{k+1}}]$$

https://doi.org/10.4153/CJM-1957-061-4 Published online by Cambridge University Press

if $p = 2$. For the matrix of a form ϕ_ρ has odd determinant, and so may be replaced by the 2×2 identity matrix without affecting 4.52; and the a_i, prime to p, may be cancelled out in any case. 4.52 thus reduces for $p \neq 2$ to

10.1 $$p^\delta | p^{\lambda_i} t_i, \text{ implying } p^{\delta+1} | p^{\lambda_i} t_i^2 \text{ if } \lambda_i \neq \delta,$$

for $i = 1, \ldots, k$. And for $p = 2$ 4.52 reduces to

10.2 $$2^\delta | 2^{\mu_\rho} t_{2\rho-1}, 2^{\mu_\rho} t_{2\rho}, \text{ implying } 2^{\delta+1} | 2^{\mu_\rho} \phi_\rho \text{ if } \mu_\rho \neq \delta,$$

for $\rho = 1, \ldots, \nu$, and

10.3 $$2^\delta | 2^{\lambda_i+1} t_i, \text{ implying } 2^{\delta-1+|\delta-\lambda_i-1|} | 2^{\lambda_i} t_i^2,$$

for $i = 2\nu + 1, \ldots, k$.

We now prove (see **3**, Lemma 3, 598 for the case $k = 3$):

LEMMA 5. (a) *If $p \neq 2$ then $\Gamma(p, f)$ is generated by adjoining the integers*

$$a_i a_j p^{\lambda_i + \lambda_i}, \qquad i, j = 1, \ldots, k.$$

each with its square factor removed, to the group of quadratic residues given by $(v|p) = 1$ or to the group Γ_p given by $(v, p) = 1$ according as $\lambda_i = \lambda_i$ does or does not imply $i = j$.

(b) *In case $\nu \neq 0$, $\Gamma(2, f) = \Gamma$ if the exponents λ_i, μ_ρ are not all of the same parity, or if for any i, j we have*

10.4 $$\lambda_i = \lambda_j, a_i \equiv a_j \pmod 4, 2\nu < i < j \leqslant k;$$

Otherwise $\Gamma(2, f) = \Gamma_2$.

(c) *If $\nu = 0$, then $\Gamma(2, f)$ is generated by the subgroup of Γ with $v \equiv 1 \pmod 8$, together with the integers*

$$a_i a_j 2^{\lambda_i + \lambda_j},$$

each with its square factor removed, and also, if the stated conditions hold, the following integers, each with square factor removed:

(i) $1 + a_i a_j$, *if* 10.4 *holds for any i, j;*
(ii) -3, *if any two exponents differ by* 0, 2 or 4;
(iii) $1 + 2a_i a_j$, *if $\lambda_j - \lambda_i = 1$ or 3;*
(iv) -1, *if there are three exponents no two of which differ by more than* 3.

Proof. It is convenient to write

$$b = p^\delta b', p \nmid b';$$

and to note that we are concerned only with the parity of δ and the value of $(b'|p)$, or the residue ± 1 or ± 3 of b' modulo 8 if $p = 2$. For if $(v|p) = 1$, or $v \equiv 1 \pmod 8$, it is obviously possible to take $b_2 = b_1 v$ in 4.6; and so all such v are in $\Gamma(p, f)$.

(a) Using 10.1, we write 4.54 as

$$b' \equiv \sum_{\lambda_i = \delta} a_i t_i^2 \pmod p.$$

https://doi.org/10.4153/CJM-1957-061-4 Published online by Cambridge University Press

The sum must not be empty, or $p|b'$, so δ is equal to some λ_i. If the sum contains two terms or more we can have $(b'|p) = \pm 1$ as we choose; but otherwise $(b'|p) = (a_i|p)$. Putting in 4.6 the values of b so found, we clearly obtain the stated result.

(b) We can choose t_1, t_2 so that $\phi_1(t_1, t_2)$ has any desired odd residue modulo 8; then with $t_3 = \ldots = t_k = 0$ we have $\delta = \mu_1$ and any desired b'. Similarly, δ can be taken equal to any of the μ_1, or, as shown below, to any of the λ_i. It is therefore sufficient to consider whether, if the μ_ρ, λ_i are all of the same parity, δ can be of the opposite parity. If so, then 10.2, 10.3, 4.54 give

$$10.5 \qquad \sum_{\delta-2\leqslant\lambda_i\leqslant\delta} 2^{\lambda_i} a_i t_i^{\,2} \equiv 2^{\delta} \pmod{2^{\delta+1}},$$

and this sum contains only terms with $\lambda_i = \delta - 1$. This is easily seen to be impossible unless 10.4 holds.

(c) Putting $t_i = 1$ and $t_j = 0$ for $j \neq 1$, we see that we can satisfy 4.54, which by 10.2, 10.3 reduces to

$$10.6 \qquad \sum_{\delta-4\leqslant\lambda_i\leqslant\delta+2} 2^{\lambda_i} a_i t_i^{\,2} \equiv 2^{\delta} b' \pmod{2^{\delta+3}},$$

with $\delta = \lambda_i$, $b' = a_i$. Thus we can have $b_1 b_2 = a_i a_j 2^{\lambda_i+\lambda_j}$ in 4.6.

If 10.4 holds, we take $i, j = 1, 2$ for convenience, and put $t_1 = 1$, $t_2 = 1, 2$, $t_3 = \ldots = t_k = 0$. 10.6 is satisfied with

$$\delta = \lambda_1 + 1, \lambda_1; \; b' = \tfrac{1}{2}(a_1 + a_2), a_1 + 4a_2.$$

Putting these values of b, and also $2^{\lambda_1} a_1$, in 4.6, we find that $\Gamma(2, f)$ contains v congruent to $1 + a_1 a_2, -3 \pmod{16}$, as asserted in clauses (i), (ii) of part (c) of the lemma; and for clause (ii) 10.42 is not needed.

To prove that $\Gamma(2, f)$ contains -3, if $\lambda_2 - \lambda_1 = 2$ or 4, or -1 or $3 \equiv 1 + 2a_1 a_2 \pmod 8$, if $\lambda_2 - \lambda_1 = 1$ or 3, write

$$\lambda_2 - \lambda_1 = 1 + \epsilon + 2\eta, \quad \epsilon = 0 \text{ or } 1, \quad \eta = 0 \text{ or } 1.$$

Put $t_1 = 2^{\eta}$, $t_2 = 1$, and all other $t_i = 0$. We find that 10.6 holds with $\delta = \lambda_1 + 2\eta$, $b' = a_1 + 2^{1+\epsilon} a_2$. Using this b and $2^{\lambda_1} a_1$ in 4.6, we have $v \equiv 1 + 2^{1+\epsilon} a_1 a_2 \pmod 8$ in $\Gamma(2, f)$.

Clause (iv) of part (c) is easily seen to be redundant unless the three exponents in question, which for convenience we take to be $\lambda_1, \lambda_2, \lambda_3$, are all of the same parity. If so, clause (ii) applies and we need only find a v with $v \equiv -1 \pmod 4$. This is trivial if the a_i have not all the same residue (mod 4). Taking therefore

$$\lambda_1 = \lambda_3 - 2\epsilon, \; \lambda_2 = \lambda_3 - 2\eta, \; \epsilon = 0 \text{ or } 1, \; \eta = 0 \text{ or } 1,$$

and

$$t_1 = 2^{\epsilon}, \; t_2 = 2^{\eta}, \; t_3 = 1, \; t_4 = \ldots = t_k = 0,$$

we see that 10.6 holds with

$$\delta = \lambda_3, \; b' = a_1 + a_2 + a_3 \equiv -a_3 \pmod 4,$$

which gives the desired result.

https://doi.org/10.4153/CJM-1957-061-4 Published online by Cambridge University Press

It remains to be seen whether we have missed any of the possibilities for $\delta \pmod 2$ or for $b' \pmod 8$. As far as δ is concerned, the argument of (b) still holds. Considering the residue of b' modulo 8, suppose first that no two of the exponents λ_i differ by 0, 2, or 4. Then if the sum in 10.6 contains three or more terms, that in 10.5 is either empty or contains a single term with exponent $\delta - 1$; in either case 10.5 is impossible. If on the other hand the sum in 10.6 contains at most two terms then the number of possibilities to be considered is very small, and it can easily be seen that b' has always a residue modulo 8 previously obtained with the same $\delta \pmod 2$.

Suppose now that there are two exponents whose difference is 0, 2, or 4. Then we have already proved $-3 \in \Gamma(2, f)$, and so need only consider $b' \pmod 4$, that is, we may reduce 10.6 $\pmod{2^{\delta+2}}$. This means, using 10.3, that the terms with exponents $\delta - 4$, $\delta + 2$, go out. We may now suppose that no two exponents differ by 1 or 3; for if such a difference occurs we already know that a v in $\Gamma(2, f)$ can be $\equiv -1 \pmod 4$, so that the residue of b' modulo 4 need not be considered. For a similar reason, we assume that no three exponents have differences all $\leqslant 2$, by (c) (iv) of the lemma. Now the number of possibilities to be considered is again very small, and we omit the remaining details.

COROLLARY. *If $p \neq 2$ and Γ_p is not included in $\Gamma(p, f)$ then $p^{\frac{1}{2}k(k-1)} | d$.*
If Γ_2 is not included in $\Gamma(2, f)$ then $4^{\frac{1}{2}k(k-1)} | d$; and if -3 is not in $\Gamma(2, f)$, then $8^{\frac{1}{2}k(k-1)} | d$.

Proof. For odd p, the present hypothesis, with part (a) of the lemma, shows that the exponents λ_i are all unequal. Their sum, say θ, is thus at least $\frac{1}{2}k(k-1)$; and obviously $p^\theta | d$.

For $p = 2$, either hypothesis, with part (b) of the lemma, gives $\nu = 0$. Now with θ as above we have

$$2^{\theta'} | d, \quad \theta' = \theta + 2\,[\tfrac{1}{2}k].$$

If $\Gamma(2, f)$ contains no $v \equiv -1 \pmod 4$, or no $v \equiv -3 \pmod 8$, then clauses (iii) and (iv), or (ii), of part (c) of the lemma show that

$$\theta \geqslant 0 + 0 + 4 + \ldots, \text{ or } \theta \geqslant 0 + 1 + 6 + \ldots .$$

By a simple calculation, this gives $\frac{1}{2}\theta'$ or $\frac{1}{3}\theta' \geqslant \frac{1}{2}k(k-1)$, which completes the proof.

We deduce:

THEOREM 4. *Suppose that f is indefinite, $k \geqslant 3$, and let d_1 be the greatest integer whose $\frac{1}{2}k(k-1)$th power divides d. Suppose also that $d_1 = 1,2,4$, p or $2p$, $p \equiv -1 \pmod 4$. Then the class-number of f, in the strict sense, is 1.*

Proof. It is sufficient, by Theorem 1(iii), to show that $\Gamma^+(f) = \Gamma_d$. We know (since n, q in 4.4 may be replaced by $-n$, $-q$) that -1 is in $\Gamma^+(f)$. So it suffices to find a subgroup of $\Gamma^+(f)$ which either coincides with Γ_d or is a

https://doi.org/10.4153/CJM-1957-061-4 Published online by Cambridge University Press

subgroup of index 2 of Γ_d, not containing -1. We obtain such a subgroup by putting $w = 1$ in 5.3, dropping the accent since f is indefinite. This subgroup is

$$\bigcap_{p|d} \{\Gamma(p,f) \cap \Gamma_p\} = \Big\{\bigcap_{2p|d_1} \Gamma(p,f)\Big\} \cap \Gamma_d,$$

by Lemma 5, Corollary. By the present hypotheses this reduces to Γ_d if $d_1 = 1$ or 2, and if $d_1 = 4$ to $\Gamma(2,f) \cap \Gamma_d$, including, by the corollary, all $q \equiv 1 \pmod 4$ in Γ_d. If $d_1 = p$ or $2p$, $p \equiv -1 \pmod 4$, then the subgroup in question is $\Gamma(p, f) \cap \Gamma_d$, with $(-1|p) = -1$, whence it does not include -1, if it is proper.

11. Factorization of automorphs. We prove:

LEMMA 6. *Every automorph S of f is expressible as a product of automorphs of the special type* 4.1; *that is, we may write*

$$S = U(\mathbf{t}_1) \ldots U(\mathbf{t}_h),\ |S| = (-1)^h,\ h \geqslant 0, \tag{11.1}$$

for suitable $\mathbf{t}_i$, $i = 1, \ldots, h$, with $f(\mathbf{t}_i)$ not zero. If p is odd and does not divide the denominator of S, then we may choose the $\mathbf{t}_i$ so that p does not divide the denominator of any of the $U(\mathbf{t}_i)$.

Proof. It suffices to prove the second part; the first is well known. We proceed by induction on k; for $k = 1$ the lemma is trivial since S can only be $\pm I$, and $U(\mathbf{t})$ can only be $-I$.

Consider first, for $k \geqslant 2$, the special case

$$f = a_{11}x_1 + g, \tag{11.21}$$

$$A = [2a_{11}, B], \tag{11.22}$$

$$S = [1, T], \tag{11.23}$$

T being necessarily an automorph of the $(k-1)$-ary form $g = g(x_2, \ldots, x_k)$. For such f, consider the $U(\mathbf{t})$ with $t_1 = 0$; we see from 4.1 that

$$U(\mathbf{t}, A) = [1, U(\boldsymbol{\zeta},B)], \text{ if } \mathbf{t} = \{0,\boldsymbol{\zeta}\} \tag{11.3}$$

and 11.2 holds. The inductive argument thus gives the result at once. Note that if 11.21 holds and the first column of S is $\{1,0, \ldots, 0\}$, then the first row of S must be $(1,0, \ldots, 0)$, so that 11.23 holds for suitable T.

Now make the weaker hypothesis that S has first column $\{1,0, \ldots, 0\}$ and $p \nmid a_{11}$. The substitution

$$x_1 \to x_1 - a_{12}x_2 - \ldots - a_{1k}x_k,\ x_i \to 2a_{11}x_i \qquad (i > 1),$$

has a matrix P with determinant $(2a_{11})^{k-1}$ prime to p. It takes f into a form f^P of the type 11.21, with an automorph $P^{-1}SP$ which has denominator prime to p and first column $\{1,0, \ldots, 0\}$. So by 4.3 with $R = P$ we have the desired result in this less special case.

Now in the general case (using 4.3 again, with suitable integral R with determinant 1) we may suppose $p \nmid a_{11}$ (since f may be taken to be primitive).

https://doi.org/10.4153/CJM-1957-061-4 Published online by Cambridge University Press

The result will follow from what we have already proved if we can find $\mathbf{t}$ such that $U(\mathbf{t})$ has denominator prime to p and $U(\mathbf{t})S$ has first column $\{1,0,\ldots,0\}$; that is, if

$$U(\mathbf{t})S\mathbf{y} = \mathbf{y} \quad \text{where} \quad \mathbf{y} = \{1,0,\ldots,0\}.$$

For if so, we have $U(\mathbf{t})S = S_1$, $S = U^{-1}(\mathbf{t})S_1 = U(\mathbf{t})S_1$, for an S_1 for which the result has been proved. It will also suffice if we can make $U(\mathbf{t})S\mathbf{y} = -\mathbf{y}$; for the denominator of $U(\mathbf{y})$ is a divisor of $a_{11} = f(\mathbf{y})$, and so we may introduce a factor $U(\mathbf{y})$ (see 4.21).

It suffices therefore to find $\mathbf{t}$ such that

$$U(\mathbf{t})S\mathbf{y} = \pm\mathbf{y}, \mathbf{y} = \{1,0,\ldots,0\}, p \nmid f(\mathbf{t});$$

for the last of these conditions ensures that p does not divide the denominator of $U(\mathbf{t})$. We take $\mathbf{t} = \mathbf{y} \pm S\mathbf{y}$, and it suffices to prove that, with proper choice of the ambiguous sign, we have

11.41 $$U(\mathbf{y} \pm S\mathbf{y})S\mathbf{y} = \pm S\mathbf{y},$$

11.42 $$f(\mathbf{y} \pm S\mathbf{y}) \not\equiv 0 \pmod{p},$$

for $\mathbf{y}$ such that $p \nmid f(\mathbf{y})$. 11.42 is clear from

$$f(\mathbf{y} \pm S\mathbf{y}) = \tfrac{1}{2}(\mathbf{y}' \pm \mathbf{y}'S')A(\mathbf{y} \pm S\mathbf{y}) = f(\mathbf{y}) + f(S\mathbf{y}) \pm \mathbf{y}'AS\mathbf{y} = 2f(\mathbf{y}) \pm \mathbf{y}'AS\mathbf{y}.$$

For if 11.42 fails for both choices of the sign, then $p|4f(\mathbf{y})$. Now (with either sign) $U(\mathbf{y} \pm S\mathbf{y})$ takes $\mathbf{y} \pm S\mathbf{y}$ into $-(\mathbf{y} \pm S\mathbf{y})$ by 4.21, and leaves $\mathbf{y} \mp S\mathbf{y}$ invariant, by 4.22; for

$$(\mathbf{y}' \pm \mathbf{y}'S')A(\mathbf{y} \pm S\mathbf{y}) = 2f(\mathbf{y}) - 2f(S\mathbf{y}) = 0.$$

Hence 11.41 holds; and this completes the proof. It is of interest to note that we cannot always take the $U(\mathbf{t}_i)$ in 11.1 to have odd denominators when the denominator of S is odd. That is, the second part of the lemma fails for $p = 2$. To show this, take $k = 4$,

$$f = x_1^2 + x_1x_2 + x_2^2 + x_3^2 + x_3x_4 + x_4^2,$$

and let S be the matrix interchanging x_1 and x_3, x_2 and x_4. If $U(\mathbf{t})$ has odd denominator, then, by 4.1, 4.5 must hold, with $\delta = 0$ since $d = 9$ is odd. That is, $f(\mathbf{t})$ must be odd. This gives that t_1, t_2 are both even and t_3, t_4 not both even, or vice versa. Then a simple calculation shows that the (i, j) element of $U(\mathbf{t})$ must be even for $i \leqslant 2, j > 2$ or vice versa. Any product of matrices with this property has the same property; but S has not.

12. Definition and properties of $v(A, S)$. We define $v(S) = v(A, S)$ by 11.1 and

12.1 $$u^2v(S) = \prod_{i=1}^{h} f(\mathbf{t}_i), \; u \text{ integral}, \; v(S) \in \Gamma.$$

Although the factorization 11.1 is not unique, it is known (see **2**, Sätze 4.4,

https://doi.org/10.4153/CJM-1957-061-4 Published online by Cambridge University Press

4.5; and **4**) that $v(A, S)$ depends only on A and S. It is essentially the *spinor norm* of S as defined by Eichler **(2)**. Clearly

12.2 $$v(S_1S_2) = v(S_2S_1) = v(S_1)\cdot v(S_2).$$

From 4.3 (with $|R| \neq 0$),

12.3 $$v(R'AR, R^{-1}SR) = v(A, S).$$

In case 11.2 holds, we take the factors in 11.1 to be of the type 11.3, and so

12.4 $$v(A, S) = v(B, T).$$

The property of $v(S)$ that we need to prove Theorem 3 is given in the first assertion of the following lemma; the second assertion is put in to simplify the proof.

LEMMA 7. *Let S be any automorph of f with denominator prime to p. Let v_1 be any element of Γ such that, for suitable u, 4.5 can be satisfied with $b = u^2v_1$. Then $v(S)$ is in $\Gamma(p, f)$ if $|S| = 1$, in v_1. $\Gamma(p, f)$ if $|S| = -1$.*

Proof for $p \neq 2$. First suppose $S = U(\mathbf{t})$. The hypothesis that p does not divide the denominator of S shows, using 4.1, that $\mathbf{t}$ must satisfy 4.51, 4.52, implying as we have seen 4.53, for some δ; whence $b = f(\mathbf{t})$ satisfies 4.54. Taking in 4.6 $b_1 = f(\mathbf{t})$, $b_2 = u^2v_1$, we find an element of $\Gamma(p, f)$ which is clearly $v_1\cdot v(U(\mathbf{t}))$. Hence $v(U(\mathbf{t}))$ is in v_1. $\Gamma(\mathrm{p}, f)$, since $v_1\cdot v_1 = 1$. This gives the result in the special case when $h = 1$ in 11.1; it follows generally by Lemma 6.

The case $p = 2$ is much more difficult since we cannot use Lemma 6. We shall proceed by induction on k; the case $k = 1$ is trivial as noted in the proof of Lemma 6. We shall also assume (see 5.6) that f is primitive; but an imprimitive $(k-1)$ary form may have to be considered in the induction. The argument used in the case $p \neq 2$ shows that the hypotheses and conclusion of the lemma are unaltered, except for interchange of the two cases, if S is replaced by $SU(\mathbf{t})$ or by $U(\mathbf{t})S$, the denominator of $U(\mathbf{t})$ being odd. We devote the next section to a preliminary simplification of the problem.

13. Proof of Lemma 7 for $p = 2$ (preliminary). We prove first:

LEMMA 8. *Write for brevity $\mathbf{y} = \{1,0, \ldots, 0\}$. Then Lemma 7 (with $p = 2$) is true in the following three cases (assuming the inductive hypothesis):*

(i) $f(\mathbf{y}) \equiv 1 \pmod 2$, $2 \mid \mathbf{y}'A$, $S\mathbf{y} = \pm \mathbf{y}$;
(ii) $f(\mathbf{y}) \equiv 1 \pmod 2$, $2 \nmid \mathbf{y}'A$, $S\mathbf{y} = \pm \mathbf{y}$;
(iii) $f(\mathbf{y}) \equiv 4 \pmod 8$, $2 \nmid \mathbf{y}'A$, $S\mathbf{y} = \pm \mathbf{y}$.

Proof. (i) We begin with the still more special case 11.2. Taking $t_1 = 0$ in 4.5, we see that all the values of b that are possible with g in place of f are also possible with f; hence $\Gamma(2, g) \subseteq \Gamma(2, f)$. Moreover, the v_1 of Lemma 7

https://doi.org/10.4153/CJM-1957-061-4 Published online by Cambridge University Press

may be taken to be a value of b arising from 4.5 with $t_1 = 0$. Hence this special case can be dealt with as in Lemma 6, using 12.4, instead of factorizing the matrix T, to apply the inductive hypothesis.

In the general case, we have a_{11} odd and $a_{12}, \ldots, a_{1k}$ all even. As in the proof of Lemma 6, it suffices to remove the product terms involving x_1 by a transformation with integral coefficients and odd determinant, and then apply 12.3. The required transformation is

$$x_1 \to x - \tfrac{1}{2}a_{12}x_2 - \ldots - \tfrac{1}{2}{}_{1k}x_k, \qquad x_1 \to a_{11}x_i \quad (i > 1).$$

(ii) The transformations needed to make f satisfy 3.4 can be chosen so as to leave a_{11} and $\mathbf{y}$ invariant. We may therefore assume 3.4, with $\mu_1 = 0$ since $2 \nmid \mathbf{y}'A$ means that one of $a_{12}, \ldots, a_{1k}$ (necessarily a_{12} in 3.4) is odd; and we write 3.4 for brevity as

13.1 $$f \equiv a_{11}x_1^{\,2} + a_{12}x_1x_2 + a_{22}x_2^{\,2} + \psi \pmod{2^\beta} \quad (a_{11} \text{ odd}).$$

Write $M = [1,4, \ldots, 4]$.
It is clear that $M^{-1}SM$, which is

$$\begin{pmatrix} \pm 1 & 4\mathbf{a}' \\ 0 & S_{22} \end{pmatrix}$$

if S is

$$\begin{pmatrix} \pm 1 & \mathbf{a}' \\ 0 & S_{22} \end{pmatrix},$$

has the same odd denominator as S and satisfies $M^{-1}SM\mathbf{y} = \mathbf{y}$ (that is, has $\mathbf{y} = \{1,0, \ldots, 0\}$ as its first column). $M^{-1}\,SM$ is an automorph of

13.2 $$f^M \equiv a_{11}x_1^{\,2} + 4a_{12}x_1x_2 + 16a_{22}x_2^{\,2} + 16\psi \pmod{2^\beta}.$$

f^M satisfies the conditions of part (i) of the lemma, and so Lemma 7 is true with f^M, $M^{-1}SM$ for f, S. It follows also for f, S, using 12.3 with $R = M$, if we can prove that $\Gamma(2, f^M) = \Gamma(2, f)$.

Now from 13.2 we see that f^M goes, by a trivial unimodular transformation, into a form congruent modulo 2^β to

13.3 $$a_{11}x_1^{\,2} + 4a_{22}'x_2^{\,2} + 16\psi, a_{22}' \equiv -a_{11} \pmod 4.$$

$\Gamma(2,f)$ includes Γ_2 by Lemma 5(b); as does $\Gamma(2,f^M)$, by Lemma 5(b) if applicable, or by Lemma 5(c), which shows that $\Gamma(2, f^M)$ contains -3 (clause (ii)) and also an integer congruent to $a_{11}a_{22}' \equiv -1 \pmod 4$. To prove $\Gamma(2, f^M) = \Gamma(2, f)$ we therefore need only show that both or neither of these groups contains even v. Comparing 13.1 and 13.3, with ψ in each case written out in full, we see that both or neither contain two exponents of opposite parity, and both or neither contain terms satisfying 10.4. This gives the result.

(iii) This case can be reduced to case (ii). We use the same M, and cancel a divisor 4 from f^M. The argument is similar but a little simpler.

https://doi.org/10.4153/CJM-1957-061-4 Published online by Cambridge University Press

We deduce

LEMMA 9. *Lemma 7 is true for $p = 2$ (assuming the inductive hypothesis) if there exist either* $\mathbf{y}$, δ *satisfying*

$$f(\mathbf{y}) \equiv 1 \pmod 2,\ 2|\mathbf{y}'A,\ 2^{\delta}|f(\mathbf{y} \pm S\mathbf{y}),\ 2^{\delta}|(\mathbf{y}' \pm \mathbf{y}'S')A, \tag{13.4}$$

(with either sign) or $\mathbf{z}$ *satisfying*

$$\mathbf{z}'AS\mathbf{z} \equiv 1 \pmod 2. \tag{13.5}$$

Note that 13.4 can be satisfied, if at all, with primitive $\mathbf{y}$, so we may suppose $\mathbf{y} = \{1,0, \ldots, 0\}$.

Proof. From 4.1, 13.43, 13.44 we see that the denominator of $U(\mathbf{y} \pm S\mathbf{y})$ is odd. Hence we may, as noted at the end of § 12, replace S by $U(\mathbf{y} \pm S\mathbf{y})S = S_1$, say. As we saw in the proof of Lemma 6, $S_1\mathbf{y} = \pm \mathbf{y}$. Thus by assertion (i) of Lemma 8, 13.4 implies Lemma 7.

Now assume 13.5, with $f(\mathbf{z})$ odd. We have

$$f(\mathbf{z} + S\mathbf{z}) = 2f(\mathbf{z}) + \mathbf{z}'AS\mathbf{z} \equiv 1 \pmod 2,$$

so the denominator of $U(\mathbf{z} + S\mathbf{z})$ is odd. Replacing S by $U(\mathbf{z} + S\mathbf{z})S$, Lemma 8(ii) with $\mathbf{y} = \mathbf{z}$ gives the result. If $f(\mathbf{z}) \equiv 4 \pmod 8$, we similarly apply Lemma 8 (iii).

If 13.5 holds with $f(\mathbf{z}) \equiv 2 \pmod 4$ or $0 \pmod 8$, we need only show that there exists $\mathbf{y}$ with $\mathbf{y}'AS\mathbf{y}$ odd and $f(\mathbf{y})$ odd or congruent to 4 modulo 8. We can find $\boldsymbol{\zeta}$ with $\mathbf{z}'A\boldsymbol{\zeta}$ odd, since 13.5 gives $2 \nmid \mathbf{z}'A$. We put $\mathbf{y} = \mathbf{z} + 2a\boldsymbol{\zeta}$, with suitable a. Clearly

$$\mathbf{y}'AS\mathbf{y} \equiv \mathbf{z}'AS\mathbf{z} \equiv 1 \pmod 2,$$
$$f(\mathbf{y}) = f(\mathbf{z}) + 2a\mathbf{z}'A\boldsymbol{\zeta} + 4a^2f(\boldsymbol{\zeta}),$$

whence $f(\mathbf{y}) = f(\mathbf{z}) \pm 2, f(\mathbf{z}) + 4 \pmod 8$ for $a = \pm 1, 2$. Hence the result.

14. Completion of proof of Lemma 7; proof of Theorem 3. Suppose first that $\mu_1 = 0$ in 3.4. Then Lemma 7 is true for $p = 2$ if we can satisfy 13.5. This is possible unless AS is congruent (mod 2) to a skew matrix. We suppose therefore that this is so; and further, since we may replace S by $SU(\mathbf{t})$ if $f(\mathbf{t})$ is odd, making the denominator of $U(\mathbf{t})$ odd, that $ASU(\mathbf{t})$ has the same property for every such $\mathbf{t}$. We shall show that this leads to a contradiction by assuming 3.4, with $\mu_1 = 0$ and a_{11} odd, as we may since ϕ_1 represents odd integers. We take $\mathbf{t} = \{1,0, \ldots, 0\}$, so that $f(\mathbf{t}) = a_{11}$ is odd. A simple calculation shows that $U(\mathbf{t})$ is congruent (mod 2) to the matrix with 1's on its diagonal and in the (1, 2) position and 0's elsewhere. Then if $\mathbf{s}_1$, $\mathbf{s}_2$ are the first two column vectors of S, those of AS are, by 3.4, congruent modulo 2 to $\mathbf{s}_2$, $\mathbf{s}_1$; and those of $ASU(\mathbf{t})$ to $\mathbf{s}_2, \mathbf{s}_1 + \mathbf{s}_2$. With AS and $ASU(\mathbf{t})$ both skew modulo 2 we must have $\mathbf{s}_2 \equiv 0$, $|S| \equiv 0 \pmod 2$, which is impossible.

https://doi.org/10.4153/CJM-1957-061-4 Published online by Cambridge University Press

We may therefore suppose, since f is assumed primitive, that in 3.4 we have $\lambda_1 = 0$ and all the μ_ρ positive. We may also suppose that no μ_ρ is 1, since otherwise Lemma 5(b) gives $\Gamma(2, f) = \Gamma$, and we have nothing to prove.

If three or more of the λ_i are 0, then 10.4 holds, and by Lemma 5(b) or (c)(i), (ii), (iv), we again have $\Gamma(2, f) = \Gamma$. We therefore assume that at most two of the λ_i vanish, and so rearranging the terms of 3.4 we may suppose

14.1 $$A \equiv [2, 2^{\lambda_2+1}, 0, \ldots, 0] \pmod 4.$$

It suffices now to deduce from 14.1 that 13.4 can be satisfied with $\mathbf{y} = \{1, 0, \ldots, 0\}$. This choice of $\mathbf{y}$ certainly satisfies 13.41 and 13.42. We choose the sign in 13.43 so that this condition holds with $\delta = 1$ or 2; for the sum of the two numbers

$$f(\mathbf{y} \pm S\mathbf{y}) = 2f(\mathbf{y}) + \mathbf{y}'AS\mathbf{y} \text{ is } 4f(\mathbf{y}) \equiv 4 \pmod 8.$$

Now 13.44 is certainly satisfied if $\delta = 1$. 13.43 holds with $\delta = 1$ if $\mathbf{y}'AS\mathbf{y} \equiv 0 \pmod 4$. If this is not so, then with $S\mathbf{y} = \boldsymbol{\xi} = \{\xi_1, \ldots, \xi_k\}$ we have ξ_1 odd. If so, then by 14.1 we have

$$1 \equiv f(\mathbf{y}) \equiv f(S\mathbf{y}) \equiv 1 + 2^{\lambda_2}\xi_2 \pmod 2.$$

Thus $2^{\lambda_2}\xi_2$ is even, and this with 14.1 gives 13.44 with $\delta = 2$.

Proof of Theorem 3. For the reason noted in §9, we may suppose $|S| = 1$. Since no p dividing d divides the denominator of S, we have $v(S) \in \Gamma(p, f)$ for each such p, by Lemma 7. If f is definite, then by 11.1 with h even since $|S| = 1$, we have $v(S) > 0$. Hence if we write

$$v(S) = wq_1,\ w|d,\ q_1 > 0,\ q_1 \in \Gamma_d,$$

we have by Lemma 1 $q_1 \in \Gamma^+(f)$. It suffices to prove $q_1 = q(S)$.

This is equivalent to showing that if $p \nmid d$ then $p|v(S)$ if and only if $p|q(S)$. We shall prove this for all S with denominators prime to d (without the restriction $|S| = 1$). For simplicity we shall assume that either p does not divide the denominator of S, or the numbers $\theta_i(S,p)$ defined in §7 are $-1, 0, \ldots, 0, 1$ (see 7.3, with $R = S$). It is clear from §9 that these are the only cases of Theorem 3 that are needed to prove Theorem 1. Other cases can however be dealt with similarly. In the second case, Lemma 4 shows that we can write $S = U(\mathbf{z})S_1$, where $p||f(\mathbf{z})$ and S_1 has denominator prime to p.

Now in the first case, when p does not divide the denominator of S, we have from Lemma 7, $v(S) \in \Gamma(p, f)$; that is, by 4.7, $p \nmid v(S)$, and clearly $p \nmid q(S)$. In the other case p divides $q(S)$, and using 12.2 we have $v(S) = v(U(\mathbf{z}))$. $v(S_1)$, that is, $v(S)$ is $f(\mathbf{z})v(S_1)$ with its square factor removed. Since $p||f(\mathbf{z})$ and, by what we have just proved, $p \nmid v(S_1)$, this gives $p|v(S)$, and the proof is complete.

https://doi.org/10.4153/CJM-1957-061-4 Published online by Cambridge University Press

References

1. H. Brandt, *Über quadratische Kern- und Stamm-formen*, Festschrift zum 60. Geburstag von Professor Andreas Speiser (Zürich, 1945).

2. M. Eichler, *Quadratische Formen und orthogonale Gruppen* (Berlin, 1952).

3. B. W. Jones and G. L. Watson, *On indefinite ternary quadratic forms*, Can. J. Math., *8* (1956), 592–608.

4. R. Lipschitz, *Untersuchungen über die Summen von Quadraten* (Bonn, 1886).

5. A. Meyer, *Ueber indefinite quadratische Formen*, Viertelschr. Naturforsch. Ges. Zürich, *36* (1891), 241–250.

6. G. Pall, *On the order invariants of integral quadratic forms*, Quart. J. Math. (Oxford), *6* (1935), 30–51.

7. G. L. Watson, *Representation of integers by indefinite quadratic forms*, Mathematika, *2* (1955), 32–38.

University College,
London

https://doi.org/10.4153/CJM-1957-061-4 Published online by Cambridge University Press