Topology Vol. 2, pp. 281–298. Pergamon Press, 1964. Printed in Great Britain

QUADRATIC FORMS ON FINITE GROUPS, AND RELATED TOPICS

C. T. C. WALL

(*Received* 23 *June* 1963)

THE RESULTS of this paper form part of a series of investigations of classification problems in differential topology. Since, however, this part is entirely algebraic (or perhaps, since specific rather than general systems are under consideration, I should say number-theoretic), it has seemed desirable to separate this paper from our other publication [5]. This also permits us to consider the algebra in more detail than we shall actually need for the application.

The plan of the paper is as follows. First we list our terminology, and prove some well-known results in a convenient notation. The one somewhat novel idea is that of a kernel. If λ is a unimodular symmetric bilinear form on a free abelian group R, whose associated quadratic form $\lambda(x, x)$ has zero signature (so that the rank of R is even), a kernel is a pure subgroup K, of half the rank of R, which is isotropic for λ. Equivalently, K is its own annihilator. There is a similar notion if λ is skew-symmetric. The main problem of this paper is to give a complete set of invariants for pairs of kernels; we reduce this to the problem of classifying symmetric or skew nonsingular bilinear forms on a finite group, with values in the circle group, (there are also a number of possible side-conditions). This classification is completely performed, except for the case of symmetric forms on 2-groups, where the results in detail are extremely complicated. In a final section we discuss briefly a more obvious but less simple relation between quadratic forms on finite groups and quadratic forms over the integers.

§1. TERMINOLOGY AND BASIC RESULTS

Throughout this paper the word group shall always mean abelian group. If H, V are two groups, we write $H \pitchfork V$ for the group of homomorphisms of H to V. A bilinear map $\lambda : G \times H \to V$ determines (by linearity in H) for each $g \in G$ a homomorphism from H to V—i.e. an element $A\lambda(g)$ of $H \pitchfork V$. By the linearity of λ in G, $A\lambda : G \to H \pitchfork V$ is a homomorphism. We call it the *homomorphism associated to* λ. Also with λ we have its transpose $\lambda^t : H \times G \to V$ defined by $\lambda^t(h, g) = \lambda(g, h)$. The associated homomorphism of λ^t is denoted unambiguously by $A\lambda^t$.

A *bilinear form* on G to V is a bilinear map $\lambda : G \times G \to V$. If $\varepsilon = \pm 1$, we call λ ε-*symmetric* if $\lambda^t = \varepsilon\lambda$. All the forms of interest to us (as opposed to mere use in constructions)

will be ε-symmetric for one or other value of ε. We abbreviate $(+)$-symmetric to symmetric and $(-)$-symmetric to skew-symmetric, or skew. If, for all $x \in G$, $\lambda(x, x) = 0$, then λ is skew and in this case, we call it *strictly skew*. If V has no 2-torsion and λ is skew, it is strictly skew. We call $g_1, g_2 \in G$ *orthogonal* (with respect to λ) if $\lambda(g_1, g_2) = 0$; if λ is ε-symmetric. orthogonality is a symmetric relation. The *annihilator* H° of a subgroup H of G is the subgroup consisting of all elements of G orthogonal to every element of H. H is *isotropic* if $H \subseteq H^\circ$, or equivalently, if $\lambda|H \times H$ is zero.

The map $\lambda : G \times H \to V$ is *nonsingular*† if $A\lambda$ and $A\lambda^t$ are both isomorphisms. It is clear if $H = G$ and λ is ε-symmetric that if $A\lambda$ is an isomorphism, so is $A\lambda^t$. In general if $A\lambda : G \to H \pitchfork V$ is an isomorphism, so is the dual map from $(H \pitchfork V)\pitchfork V$ to $G \pitchfork V$; if the canonical map from H to $(H \pitchfork V)\pitchfork V$ is an isomorphism, so that we can identify these groups, the dual map is identified with $A\lambda^t$. We shall in fact always work with a group G and a value group V such that the canonical map from G to $(G \pitchfork V)\pitchfork V$ is an isomorphism. The following three cases are of particular interest.

(i) V the field $\mathbf{Q}$ of rationals, G a finite-dimensional vector space over $\mathbf{Q}$.
(ii) V the group $\mathbf{Z}$ of integers, G a free abelian group of finite rank.
(iii) V the quotient group $\mathbf{Q}/\mathbf{Z}$ which we shall write as $\mathbf{S}$ and refer to as the "circle group", G a finite group.

The following lemma is well-known, but we shall use it frequently, and so give a proof.

LEMMA (1). *Let $\lambda : G \times G \to V$ be nonsingular, ε-symmetric, and H a subgroup of G with $\lambda|H \times H$ nonsingular. Then G is the direct sum of H and H°, and $\lambda|H^\circ \times H^\circ$ is nonsingular.*

Proof. Write $\phi = \lambda|G \times H$. The kernel of $A\phi : G \to H \pitchfork V$ is, by definition, H°. By hypothesis, $A\phi|H$ is an isomorphism. Thus H and H° are disjoint, and span G, which is their direct sum. Now $A\lambda : G \to G \pitchfork V$ may be written as $A\lambda : H \oplus H^\circ \to H \pitchfork V \oplus H^\circ \pitchfork V$, and since H and H° are orthogonal, this map preserves the components. Since it is an isomorphism, it induces an isomorphism of H° on $H^\circ \pitchfork V$.

We next consider the following question, (the answer to which is also well-known) since we use the result in the sequel. Let H be free abelian, $\lambda : H \times H \to \mathbf{Z}$ bilinear and ε-symmetric. When is there a bilinear $\psi : H \times H \to \mathbf{Z}$ (without symmetry) such that $\lambda = \psi + \varepsilon\psi^t$? (Of course $\psi + \varepsilon\psi^t$ is always ε-symmetric). Now when $\varepsilon = 1$, a necessary condition is clearly that for $x \in H$, $\lambda(x, x) = 2\psi(x, x)$ must be even. When $\varepsilon = -1$, $\lambda(x, x) = 0$, so there is no such condition. Suppose now that $\{e_i\}$ is a basis for H, with $\lambda(e_i, e_i)$ even for each i. If we set

$$\begin{aligned} \psi(e_i, e_j) &= \lambda(e_i, e_j) && i < j \\ &= \tfrac{1}{2}\lambda(e_i, e_j) && i = j \\ &= 0 && i > j, \end{aligned}$$

and extend ψ to a bilinear map, then we do have $\lambda = \psi + \varepsilon\psi^t$.

† The word "nonsingular" is often used if λ is symmetric and $A\lambda$ a monomorphism. We follow Hirzebruch in preferring to use "nondegenerate" for this case, reserving "nonsingular" for the case of isomorphism.

In the case $\varepsilon = 1$ we call λ *even* if $\lambda(x, x)$ is even for all x, *odd* otherwise. Define $\chi : H \to \mathbf{Z}_2$ by $\chi(x) = \lambda(x, x) \pmod 2$. Then

$$\begin{aligned}\chi(x + y) - \chi(x) - \chi(y) &= \lambda(x + y, x + y) - \lambda(x, x) - \lambda(y, y)\\ &= \lambda(x, y) + \lambda(y, x)\\ &= 2\lambda(x, y) = 0 \pmod 2.\end{aligned}$$

so χ is a homomorphism. If λ is odd, and so χ nonzero, we choose a basis $\{e_i\}$ for H with $\chi(e_1) = 1$, $\chi(e_i) = 0$ for $i > 1$. If the above definition of ψ is now modified by setting

$$\psi(e_1, e_1) = \tfrac{1}{2}(\lambda(e_1, e_1) - 1),$$

we see that $(\lambda - \psi - \varepsilon\psi')(e_i, e_j)$ is zero unless $i = j = 1$ when it equals 1.

Now suppose $\lambda : H \times H \to \mathbf{Z}$ nonsingular and ε-symmetric. We call a subgroup K of H a *kernel* if $K = K^\circ$. Since in this case (V torsion free) if $x \in H$ is orthogonal to K, so is any submultiple of x, K°—i.e. K—is a pure subgroup, and so a direct summand. Hence the projection $\pi : H \to K \oplus \mathbf{Z}$ dual to the inclusion of K in H is onto, and since $A\lambda : H \to H \to \mathbf{Z}$ is an isomorphism, $\pi \circ A\lambda$ is also onto. But its kernel is $K^\circ = K$, hence the rank of H is twice that of K. Conversely, if K is any pure isotropic subgroup with half the rank of H, the rank of K equals that of its annihilator K°; since $K \subseteq K^\circ$ and is pure, it follows that $K = K^\circ$.

We next classify triples (H, λ, K) where H, λ, K are as above. Let L be an additive complement to K in H. Then L is complementary to the kernel of $\pi \circ A\lambda$, which thus induces an isomorphism of L on $K \to \mathbf{Z}$. Denote by γ the dual isomorphism of $L \to Z$ on K, so that for $x \in L$, $f : L \to \mathbf{Z}$ we have $f(x) = \lambda(\gamma(f), x)$. Now $\nu = \lambda | L \times L$ is ε-symmetric, so by a result a few lines above we can write $\nu = \psi + \varepsilon\psi^t$ either exactly, or with an error of 1 only on (e_1, e_1) where $\{e_i\}$ is a basis of L. Define $h : L \to H$ by $h(x) = x - \gamma(A\psi(x))$. Clearly h is a homomorphism; since $x - h(x)$ is in K, the image of h is still an additive complement to K in H. Also for $x, y \in L$,

$$\lambda(h(x), h(y)) = \lambda(x, y) - \lambda(x, \gamma(A\psi(y))) - \lambda(\gamma(A\psi(x)), y) + \lambda(\gamma(A\psi(x)), \gamma(A\psi(y))).$$

Here the last term vanishes since $\lambda | K \times K$ is zero, and the second to last term is $-\lambda(\gamma(A\psi(x)), y) = -A\psi(x)(y) = -\psi(x, y)$. Thus we have

$$\lambda(h(x), h(y)) = \lambda(x, y) - \varepsilon\psi(y, x) - \psi(x, y),$$

which, by choice of ψ, vanishes, with perhaps one exception, on all pairs of basis elements. We now pick a basis $\{f_i\}$ of K dual under γ to the chosen basis of L and obtain

LEMMA (2). *Let λ be a nonsingular, ε-symmetric bilinear form on H to $\mathbf{Z}$, K a kernel. Then H has a basis $\{e_i, f_i\}$, such that $\{f_i\}$ is a basis for K, and $\lambda(e_i, f_i) = \varepsilon\lambda(f_i, e_i) = 1$, and λ vanishes on other pairs of basis elements, unless $\varepsilon = 1$ and λ is odd, when $\lambda(e_1, e_1) = 1$.*

We remark that the quadratic forms λ which occur are precisely those of zero signature. Also, for each choice of the rank of H (which must be even), there are three cases: $\varepsilon = -1$, $\varepsilon = 1$ and λ is even, $\varepsilon = 1$ and λ is odd. In particular, no additional invariants arise from the choice of the kernel K.

COROLLARY. *If $\lambda : H \times H \to \mathbf{Z}$ is nonsingular, bilinear and ε-symmetric, and K_1, K_2 are two kernels, then there is an automorphism of H preserving λ which takes K_1 to K_2.*

This result was used in our paper [4].

§2. PAIRS OF KERNELS

For the whole of this section, H is a free abelian group, $\lambda : H \times H \to \mathbf{Z}$ a nonsingular, ε-symmetric, bilinear form, and K_1, K_2 a pair of kernels. We seek a set of invariants for the system. The most natural invariant is the quotient group $G = H/(K_1 + K_2)$. We shall return to this later, but first seek a reduction of the problem which corresponds to the splitting of G as direct sum of its torsion subgroup and a free complement.

Let $K = K_1 \cap K_2$ and T be the pure subgroup of H generated by $K_1 + K_2$. Then $T^\circ = K_1^\circ \cap K_2^\circ = K_1 \cap K_2 = K$. If L is a complement to T in H, it follows that $\lambda' = \lambda | L \times K$ has $A\lambda'$ epimorphic; since K and L have the same rank, $A\lambda'$ must be an isomorphism, i.e. $K + L$ is nonsingular. Write $Y = (K + L)^\circ$; then Y is a complement to K in T. By Lemma (1), $H = Y \oplus Y^\circ$. Now if $X_i = K_i \cap Y (i = 1, 2)$, then $K_i = K \oplus X_i$, and $K \subset Y^\circ$, $X_i \subset Y$. In the summand Y° we have the kernel K; in the summand Y the pair of kernels X_1, X_2—that these are kernels follows since they are pure, isotropic, and of half the rank of the containing group. Moreover, as $K_1 \cap K_2 = K$ follows $X_1 \cap X_2 = 0$.

LEMMA (3). *H splits as $Y \oplus Y^\circ$, and the kernels split also as $X_i \oplus K$. The triple (H, K_1, K_2) determines (Y, X_1, X_2) up to isomorphism $(X_1 \cap X_2 = 0)$ also the rank of (Y°, K). When $\varepsilon = 1$, if H is even, so is Y°; if H is odd and Y even, Y° is odd; if Y is odd, Y° may be chosen with either parity.*

Note. By abuse of language, "Y is odd" means "$\lambda | Y \times Y$ is odd", etc.

Proof. The first clause was proved above. Since K annihilates T, projection parallel to K defines isomorphisms between any two complements to K in T, preserving the form λ and kernels. Thus it only remains to consider parities; here the first two cases are trivial. Now if Y is odd, the homomorphism $\chi : H \to \mathbf{Z}_2$ defined above is nonzero; in fact $T \not\subset \operatorname{Ker} \chi$. Thus we can choose complements L_0, L_1 to T in H with $\chi(L_0) = 0$, $\chi(L_1) \neq 0$. Setting $Y_i = T \cap L_i^\circ$, we obtain two complements to K in T, and $Y_i^\circ = K + L_i$ has the same parity as i.

Now for (Y, X_1, X_2) we have $X_1 \cap X_2 = 0$, so the pure subgroup spanned by $X_1 + X_2$ is the whole of Y, and the quotient $Y/(X_1 + X_2)$ is a torsion group, and so finite. Since, by Lemma (3), the general problem is reduced to this case—for (Y°, K), having only a single kernel, was classified in Lemma (2)—we now revert to our original notation with the extra hypothesis that $K_1 \cap K_2 = 0$.

We first extend the problem from the integers to the rationals by taking tensor products with $\mathbf{Q}$; we shall denote the rational extension by adding a bar. Then $\bar{\lambda} : \bar{H} \times \bar{H} \to \mathbf{Q}$ is nonsingular, and $\bar{K}_1, \bar{K}_2$ are subspaces of $\bar{H}$, isotropic, of half its dimension, with $\bar{K}_1 \cap \bar{K}_2 = 0$. Hence $\bar{H} = \bar{K}_1 \oplus \bar{K}_2$. The associated homomorphism of $\bar{\lambda} | \bar{H} \times \bar{K}_1$ is a map of $\bar{H}$ onto $\bar{K}_1^\wedge \mathbf{Q}$, with kernel $\bar{K}_1$, so induces an isomorphism of $\bar{K}_2$. Thus $\bar{\mu} = \bar{\lambda} | \bar{K}_1 \times \bar{K}_2$ is nonsingular. Choosing dual bases in $\bar{K}_1$ and $\bar{K}_2$ we see that the classification problem over $\mathbf{Q}$ is trivial.

We must now return from rationals to integers. We can regard H as contained in $\bar{H}$; since K_i is a pure subgroup, we have $K_i = H \cap \bar{K}_i (i = 1, 2)$. Note that $K_2 \otimes \mathbf{Q} = \bar{K}_2 \otimes \mathbf{Q}$, so that we can write $A\bar{\mu} : \bar{K}_1 \to K_2 \otimes \mathbf{Q}$. Define $K_1' = (A\bar{\mu})^{-1}(K_2 \otimes \mathbf{Z})$. Similarly define K_2' as the inverse image for the isomorphism $A\bar{\mu}^t$ of $K_1 \otimes \mathbf{Z}$. Now $H \subset \bar{H} = \bar{K}_1 \oplus \bar{K}_2$, and the associated homomorphism of any element of H takes H, hence also K_1 and K_2, to $\mathbf{Z}$. So $H \subset K_1' \oplus K_2'$. As K_2 is a direct summand of H, the projection of $H \otimes \mathbf{Z}$ to $K_2 \otimes \mathbf{Z}$ is onto, hence also that of H (in $K_1' \oplus K_2'$) to K_1'. The kernel of this is K_2. So there is an induced isomorphism of $G = H/(K_1 + K_2)$ on K_1'/K_1. Write $g_1 : K_1' \to G$ for the projection. Similarly we have $g_2 : K_2' \to G$ inducing an isomorphism on K_2'/K_2 on G. We observe that $K_1' \oplus K_2'/K_1 \oplus K_2 \cong G \oplus G$, and H consists of those elements $x_1' + x_2'$ of $K_1' \oplus K_2'$ with $g_1(x_1') = g_2(x_2')$.

We shall now obtain a bilinear form on G induced by λ. Since the same argument will be needed twice later, we give it here in a form which will cover all the cases we need.

LEMMA (4). *Let K_1', K_2' be free abelian groups of rank r, and $\lambda' : K_1' \times K_2' \to \mathbf{Q}$ a bilinear pairing. Let $K_1 \subset K_1'$, $K_2 \subset K_2'$ be subgroups also of rank r, and suppose that λ' has non-singular restrictions $\phi_1 : K_1 \times K_2' \to \mathbf{Z}$, $\phi_2 : K_1' \times K_2 \to \mathbf{Z}$. Then λ' induces a nonsingular pairing $\omega : K_1'/K_1 \times K_2'/K_2 \to \mathbf{S}$.*

Proof. Write G_i for K_i'/K_i, $g_i : K_i' \to G_i$ for the projection $(i = 1, 2)$. Define

$$\omega(g_1(x_1), g_2(x_2)) = \lambda'(x_1, x_2) \pmod 1.$$

If $g_i(x_i') = g_i(x_i)$, then $x_i' - x_i \in K_i (i = 1, 2)$ and so

$$\lambda'(x_1', x_2') - \lambda'(x_1, x_2) = \phi_1(x_1' - x_1, x_2') + \phi_2(x_1, x_2' - x_2)$$

is an integer; thus ω is well defined.

Suppose $A\omega(u_1) = 0$. Write $u_1 = g_1(x_1)$. Then for all x_2 in K_2', $\omega(u_1, g_2(x_2)) = 0$, i.e. $\lambda'(x_1, x_2)$ is an integer. So $A\lambda'(x_1) \in K_2' \otimes \mathbf{Z}$, and since ϕ_1 is nonsingular, $x_1 \in K_1$. Then $u_1 = g_1(x_1) = 0$. Thus $A\omega$ is $(1 - 1)$. Similarly, so is the Pontrjagin dual map $A\omega^t$, so $A\omega$ is also onto, and ω is nonsingular.

In the case above, $G = G_1 = G_2$, and we write b for ω.

LEMMA (5). *The pair of kernels K_1, K_2 with $K_1 \cap K_2 = 0$ has as complete set of invariants (r, G, b) where r is the rank of K_1; G, b are as above. Moreover (r, G, b) is a set of invariants if and only if G is a finite group which admits r generators, and $b : G \times G \to \mathbf{S}$ is a nonsingular, $(-\varepsilon)$-symmetric bilinear form.*

Proof. It is clear from their definitions that r, G and b are indeed invariant. Also $G = H/(K_1 + K_2)$ is a quotient of H/K_2, a free group of rank r, so admits r generators. Now for $g, h \in G$, write $g = g_1(x_1) = g_2(x_2)$, $h = g_1(y_1) = g_2(y_2)$. Then

$$\begin{aligned} b(g, h) + \varepsilon b(h, g) &= \bar{\lambda}(x_1, y_2) + \varepsilon\bar{\lambda}(y_1, x_2) \\ &= \bar{\lambda}(x_1, y_2) + \bar{\lambda}(x_2, y_1) \\ &= \bar{\lambda}(x_1, y_1) + \bar{\lambda}(x_1, y_2) + \bar{\lambda}(x_2, y_1) + \bar{\lambda}(x_2, y_2) \\ &= \bar{\lambda}(x_1 + x_2, y_1 + y_2) \end{aligned}$$

(we have used the fact that K_1', K_2' are isotropic), and this is an integer since, by a remark above, $x_1 + x_2$ and $y_1 + y_2$ are in H.

So b is $(-\varepsilon)$-symmetric; it is very amusing, the way b has symmetry of the opposite kind to λ.

To prove the converse we start from (r, G, b) and show how to build up (H, K_1, K_2) in an essentially unique way, which is forced on us by the definitions above. Let K_1' be a free group of rank r, $g_1 : K_1' \to G$ an epimorphism; by a well-known result, this is unique up to automorphisms of K_1'. Put $K_1 = \operatorname{Ker} g_1$. Let $K_2' = K_1 \pitchfork \mathbf{Z}$, and extend the non-singular pairing $K_1 \times K_2' \to \mathbf{Z}$ defined by evaluation to $\mu : K_1' \times K_2' \to \mathbf{Q}$; this can be done uniquely since each element of K_1' is a submultiple of an element of K_1. Then μ defines $A\mu' : K_2' \to K_1' \pitchfork \mathbf{Q}$, whose image contains $K_1' \pitchfork \mathbf{Z}$ since each homomorphism of K_1' to $\mathbf{Z}$ induces one of K_1 which corresponds to some element of K_2'. Define $K_2 = (A\mu')^{-1}(K_1' \pitchfork \mathbf{Z})$. Then all the conditions of Lemma (4) are satisfied, and μ induces a nonsingular pairing $\omega : G \times (K_2'/K_2) \to \mathbf{S}$.

Identify K_2'/K_2 with G by the isomorphism $(Ab')^{-1}(A\omega')$; then ω is identified with b. Define an ε-symmetric bilinear map $\lambda' : (K_1' \oplus K_2') \times (K_1' \oplus K_2') \to \mathbf{Q}$ by

$$\lambda'(x_1 + x_2, y_1 + y_2) = \mu(x_1, y_2) + \varepsilon\mu(y_1, x_2).$$

Let H be the set of elements $x_1 + x_2$ of $K_1' \oplus K_2'$ with $g_1(x_1) = g_2(x_2)$. This completes our construction, for $H \cap K_i' = K_i$, so if we can show that λ' induces a nonsingular $\lambda : H \times H \to \mathbf{Z}$, we have the pair of kernels K_1, K_2 and since the construction here is parallel to that of Lemma (4) it will follow that the corresponding set of invariants is (r, G, b). Also, the construction involved no arbitrary choices, and each step was forced on us by the parallelism with Lemma (4).

So it only remains to prove $\lambda : H \times H \to \mathbf{Z}$ defined and nonsingular. That it is defined follows, reckoning modulo 1, from

$$\begin{aligned}\lambda'(x_1 + x_2, y_1 + y_2) &= \mu(x_1, y_2) + \varepsilon\mu(y_1, x_2)\\ &= b(g_1(x_1), g_2(y_2)) + \varepsilon b(g_1(y_1), g_2(x_2))\\ &= b(g_2(x_2), g_1(y_1)) - b(g_2(x_2), g_1(y_1)) = 0,\end{aligned}$$

using the definition of H and symmetry of b at the last stage. So λ takes only integer values. Since the rational extension of λ' is clearly nonsingular, $A\lambda$ is a monomorphism. To prove $A\lambda$ onto, take any homomorphism $H \to \mathbf{Z}$. This induces a homomorphism of $K_2 \oplus K_1$ to $\mathbf{Z}$ and so, by duality, an element $x_1 + x_2$ of $K_1' \oplus K_2'$. This has the property that for $y_1 + y_2 \in H$, $\lambda'(x_1 + x_2, y_1 + y_2)$ is an integer. Hence, reckoning again modulo 1,

$$\begin{aligned}0 = \lambda'(x_1 + x_2, y_1 + y_2) &= b(g_1(x_1), g_2(y_2)) + \varepsilon b(g_1(y_1), g_2(x_2))\\ &= b(g_1(x_1), g) - b(g_2(x_2), g)\end{aligned}$$

if $g = g_1(y_1) = g_2(y_2)$. But now, since g is arbitrary and b nonsingular, $g_1(x_1) = g_2(x_2)$, and so $x_1 + x_2$ is in H.

We can now prove

THEOREM (1). *A complete system of invariants of a pair (K_1, K_2) of kernels in H is given by (r, G, b, χ), where r is the rank of K_1, $G = H/(K_1 + K_2)$, $b : G^* \times G^* \to \mathbf{S}$ is a non-*

singular, $(-\varepsilon)$-symmetric bilinear form on the torsion subgroup G^* of G and, if $\varepsilon = 1$, $\chi : G \to \mathbf{Z}_2$ is a homomorphism.
The invariants (r, G, b, χ) appear, provided that G admits r generators, and (if $\varepsilon = 1$) for $g \in G^*$, $b(g, g) = \frac{1}{2}\chi(g) \pmod 1$.

Proof. We observe that the decomposition of Lemma (3) induces a decomposition of $G = Y/(X_1 + X_2) \oplus Y^\circ/K$ into torsion subgroup and a free part, and by that lemma, apart from questions of parity when $\varepsilon = 1$, the invariants just reduce to those of (Y, X_1, X_2) which, by Lemma (5), are determined by rank, G^* and b. So the theorem is already proved if $\varepsilon = -1$ and it remains only to consider parity.

We recall that when $\varepsilon = 1$, $\lambda(x, x) = \chi(x) \pmod 2$ defines a homomorphism $\chi : H \to \mathbf{Z}_2$. χ clearly vanishes on kernels, and so defines another homomorphism $\chi : G = H/(K_1 + K_2) \to \mathbf{Z}_2$. We call G even if $\chi(G) = 0$, odd otherwise. If G is even, so is any complement to G^*; if G is odd and G^* even, any complement to G^* must be odd; if G^* is odd, it has complements of both types. These cases correspond exactly to those in Lemma (3). Hence it remains only to describe $\chi|G^*$ in terms of b (which must be possible, since we then have a complete set of invariants which omits χ). Now b is skew-symmetric, so each $c(x) = b(x, x)$ has order 2, and

$$\begin{aligned} c(x + y) - c(x) - c(y) &= b(x + y, x + y) - b(x, x) - b(y, y) \\ &= b(x, y) + b(y, x) = 0, \end{aligned}$$

so c is a homomorphism. We assert $c = \frac{1}{2}\chi$ (recall that values of c are multiples of $\frac{1}{2}$ modulo 1, values of χ are integers modulo 2; the $\frac{1}{2}$ is simply an isomorphism). Let $x \in H$, $x = x_1 + x_2$ $(x_i \in K_i')$, $g_i(x_i) = g \in G$. Then $c(g) = b(g, g) = \tilde{\lambda}(x_1, x_2) \pmod 1$, so

$$\begin{aligned} 2c(g) = 2\tilde{\lambda}(x_1, x_2) &= \tilde{\lambda}(x_1, x_2) + \tilde{\lambda}(x_2, x_1) \\ &= \tilde{\lambda}(x_1, x_1) + \tilde{\lambda}(x_1, x_2) + \tilde{\lambda}(x_2, x_1) + \tilde{\lambda}(x_2, x_2) \\ &= \tilde{\lambda}(x_1 + x_2, x_1 + x_2) = \lambda(x, x) = \chi(x) \pmod 2. \end{aligned}$$

This completes the proof of Theorem (1).

The direct sum of two systems (H, K_1, K_2) and (H', K_1', K_2') is the system $(H \oplus H', K_1 \oplus K_1', K_2 \oplus K_2')$, where $H \oplus H'$ is the orthogonal direct sum. The direct sum of two sets of invariants (r, G, b, χ) and (r', G', b', χ') is the set $(r + r', G \oplus G', b + b', \chi + \chi')$ where of course G^* and G'^* are orthogonal for $b + b'$. From our definitions, without further discussion, follows

COMPLEMENT TO THEOREM (1). *The set of invariants of the direct sum of two systems is the direct sum of their separate sets of invariants.*

§3. PAIRS OF Φ-KERNELS

We now have to consider a slight extension of the problem of the preceding paragraph (this is demanded by the application). Here $\lambda : H \times H \to \mathbf{Z}$ is, as before, a nonsingular, skew-symmetric bilinear form (we take only the case $\varepsilon = -1$) and $\phi : H \to \mathbf{Z}_2$ satisfies the identity

$$\phi(x + y) = \phi(x) + \phi(y) + \lambda(x, y) \pmod 2.$$

Thus ϕ is really a nonsingular quadratic form mod 2, with associated symmetric (mod 2!) bilinear map λ. It is known that the structure of (H, λ, ϕ) is determined by the (even) rank of H, and the Arf invariant Φ; however, we do not need this result.

A kernel K in H is called a *ϕ-kernel* if ϕ vanishes identically on K (note that since λ vanishes on $K \times K$, ϕ would in any case reduce to a homomorphism of K, so it is sufficient for ϕ to vanish on a set of basis elements of K). If a basis $\{e_i, f_i\}$ of H is chosen as in Lemma (1), we have $\phi(f_i) = 0$. For each i, either $\phi(e_i) = 0$ or we can replace e_i by $e_i + f_i$, and thus obtain $\phi(e_i) = 0$ also. Thus the only invariant of the system (H, λ, ϕ, K) is the rank of K.

We are now ready to consider the classification problem for pairs of ϕ-kernels (K_1, K_2). Of course, the results of §2 remain valid, but do not determine ϕ from the invariants. Again we use the splitting of Lemma (3); by the last paragraph, the only invariant of (Y°, K) is the rank of K, and (Y, X_1, X_2) is determined up to isomorphism as before. So it is enough to consider the case $K_1 \cap K_2 = 0$. Here a new invariant appears.

LEMMA (6). *With the notation of Lemma* (4), *for $g \in G$ with $g = g_1(x_1) = g_2(x_2)$ define* $q(g) = \tilde{\lambda}(x_1, x_2) + \phi(x_1 + x_2)$ (mod 2). *Then q is well-defined, and*

$$q(g + h) - q(g) - q(h) = 2b(g, h) \text{ (mod 2).}$$

Proof. Since $g_1(x_1) = g_2(x_2)$, $x_1 + x_2$ is in H, so $\phi(x_1 + x_2)$ is defined. If also $g = g_1(x_1') = g_2(x_2')$, then $k_1 = x_1' - x_1 \in K_1$, $k_2 = x_2' - x_2 \in K_2$. The difference between the two values of $q(g)$ is (modulo 2)

$$\begin{aligned}
&\tilde{\lambda}(x_1 + k_1, x_2 + k_2) + \phi(x_1 + k_1 + x_2 + k_2) - \tilde{\lambda}(x_1, x_2) - \phi(x_1 + x_2) \\
&\quad = \tilde{\lambda}(x_1, k_2) + \tilde{\lambda}(k_1, x_2) + \lambda(k_1, k_2) + \phi(k_1 + k_2) + \lambda(x_1 + x_2, k_1 + k_2) \\
&\quad = \tilde{\lambda}(x_1, k_2) + \tilde{\lambda}(k_1, x_2) + \lambda(k_1, k_2) + \phi(k_1) + \phi(k_2) + \lambda(k_1, k_2) + \tilde{\lambda}(x_1, k_2) + \tilde{\lambda}(x_2, k_1) \\
&\quad = 2\tilde{\lambda}(x_1, k_2) + 2\lambda(k_1, k_2) = 0 \quad \text{(mod 2).}
\end{aligned}$$

Hence $q(g)$ is well-defined. Now let $g = g_1(x_1) = g_2(x_2)$, $h = g_1(y_1) = g_2(y_2)$. Again reckoning modulo 2, we have

$$\begin{aligned}
&q(g + h) - q(g) - q(h) \\
&\quad = \tilde{\lambda}(x_1 + y_1, x_2 + y_2) + \phi(x_1 + y_1 + x_2 + y_2) \\
&\qquad\qquad - \tilde{\lambda}(x_1, x_2) - \phi(x_1 + x_2) - \tilde{\lambda}(y_1, y_2) - \phi(y_1 + y_2) \\
&\quad = \tilde{\lambda}(x_1, y_2) + \tilde{\lambda}(y_1, x_2) + \lambda(x_1 + x_2, y_1 + y_2) \\
&\quad = \tilde{\lambda}(x_1, y_2) + \tilde{\lambda}(y_1, x_2) + \tilde{\lambda}(x_1, y_2) + \tilde{\lambda}(x_2, y_1) \\
&\quad = 2\tilde{\lambda}(x_1, y_2) = 2b(g, h).
\end{aligned}$$

Thus q is a quadratic form on G—by a quadratic form $Q : G \to V$ we understand a mapping such that $B : G \times G \to V$, defined by $B(x, y) = Q(x + y) - Q(x) - Q(y)$, is bilinear. When B is nonsingular, we call Q nonsingular. We note that putting $y = 0$ shows that $Q(0) = 0$. If $Q(-x) = Q(x)$, we call Q homogeneous. It is clear that q is nonsingular and homogeneous.

THEOREM (2). *A complete set of invariants of a pair (K_1, K_2) of ϕ-kernels in H is given by (r, G, q), where r is the rank of K_1, $G = H/(K_1 + K_2)$ and q is a nonsingular homogeneous quadratic form on G^* with values rationals modulo* 2. *The set (r, G, q) appears if and only if G admits r generators.*

Proof. As remarked above, it is sufficient to consider the case $K_1 \cap K_2 = 0$. We have seen that the invariants are defined, and have the given properties. Conversely, suppose them given. We define the nonsingular symmetric bilinear form b by the relation

$$b(g, h) = \tfrac{1}{2}\{q(g + h) - q(g) - q(h)\} \pmod 1$$

Since q is homogeneous,

$$b(g, -g) = \tfrac{1}{2}\{q(0) - q(g) - q(-g)\} = -q(g) \pmod 1,$$

so $b(g, g) = q(g) \pmod 1$. By Theorem (1), we can use (r, G, b) to construct (H, K_1, K_2) in a unique way. Now for $x \in H$, write as usual $x = x_1 + x_2$, $g_1(x_1) = g_2(x_2) = g$; then we must define $\phi(x) = q(g) - \tilde{\lambda}(x_1, x_2) \pmod 2$. Since $b(g, g) = q(g) \pmod 1$, this is certainly an integer. The calculation given in Lemma (6) can now be reversed to deduce the formula $\phi(x + y) = \phi(x) + \phi(y) + \lambda(x, y)$ from the formula $q(g + h) = q(g) + q(h) + 2b(g, h) \pmod 2$. Finally if $x \in K_1$, $x_2 = 0$ so clearly $\phi(x) = 0$. Thus K_1 (similarly, also K_2) is a ϕ-kernel. It is evident from the definition of ϕ that (H, K_1, K_2) has (r, G, q) as its set of invariants.

As before, we define the direct sums of sets of invariants in the natural way, and Theorem (2) has a complement verbally identical with that of Theorem (1).

We need one further complement to Theorem (1); this, however, is fairly trivial.

PROPOSITION. *Let the hypotheses of Theorem* (1) *or* (2) *be modified by giving a homomorphism* $\alpha : H \to P$ *(for some group* P*) and calling a kernel* K *an* α*-kernel if* $\alpha(K) = 0$. *Then the conclusion is modified by including a homomorphism* $\alpha' : G \to P$.

Proof. Since the homomorphism α of H annihilates K_1 and K_2, it factors through $G = H/(K_1 + K_2)$, thus inducing the invariant α'. Conversely, α' determines α: we simply compose with the natural projection of H on G.

This concludes the first half of this paper; from now on we concern ourselves with a more detailed examination of the nature of ε-symmetric or quadratic forms on a finite group.

§4. NONSINGULAR SKEW FORMS ON FINITE GROUPS

In this section we shall classify up to isomorphism pairs (G, b), where G is a finite group, $b : G \times G \to \mathbf{S}$ a nonsingular skew-symmetric bilinear form. This problem was already discussed in [3]. However, since our previous results were incomplete, we shall make no use of them here.

G splits as the direct sum of its Sylow subgroups G_p. Since these are clearly orthogonal, the whole problem splits accordingly. We shall continue (using Lemma (1)) to split (G, b) as a direct sum. It is thus convenient to extend our problem to determine not merely the set of isomorphism classes of (G, b), but also their behaviour under direct sums. Write $\mathfrak{M}$ for the set of isomorphism classes of pairs (G, b); then direct sum induces an addition on $\mathfrak{M}$ which is evidently commutative and associative. Thus $\mathfrak{M}$ is an abelian monoid (taking G as the zero group gives a zero for $\mathfrak{M}$).

Recall from the proof of Theorem (1) that if $c(x) = b(x, x)$, then $c : G \to \mathbf{Y}_2$ is a homomorphism (where $\mathbf{Y}_2$ denotes the group of multiples of $\frac{1}{2}$, mod 1). Suppose G a p-group

with $c = 0$ (if $p \neq 2$, of course c must vanish anyway). Let $x \in G$ have maximal order p^r. Then the subgroup $\{x\}$ of G generated by x is additively a direct summand. Projecting G onto it, and then mapping x to p^{-r} defines a homomorphism of G to $\mathbf{S}$. Since b is non-singular, this determines by duality an element y of G, such that $b(x, y) = p^{-r}$. The order of y is p^{-r}, since p^{-r} generates the image of the homomorphism, and since $b(x, x) = c(x) = 0$, $\{x\}$ and $\{y\}$ do not meet, so form a direct sum (not orthogonal) H in G. By inspection, we see that $b|H \times H$ is nonsingular, so by Lemma (1), $G \cong H \oplus H^\circ$.

Define $W_{p^r} \in \mathfrak{M}$ as the isomorphism class of $(H, b|H \times H)$: since H is the direct sum of cyclic groups of order p^r generated by x and y, and $b(x, x) = b(y, y) = 0$, $b(x, y) = p^{-r}$, this is well determined.

LEMMA (7). *Let $\mathfrak{M}_s$ be the submonoid of $\mathfrak{M}$ defined by (G, b) such that $c = 0$. Then $\mathfrak{M}_s$ is the free monoid generated by the W_{p^r} (one for each prime power).*

Proof. We observed above that G splits as the direct sum of its Sylow subgroups; it is therefore sufficient to consider the case when G is a p-group. The argument above, with induction on the order of G, now shows that the W_{p^r} generate $\mathfrak{M}_s$. If $\mathfrak{M}_s$ were not free, there would be a relation

$$\sum \lambda_r W_{p^r} = \sum \mu_r W_{p^r}.$$

But since W_{p^r} is the direct sum of two cyclic groups of order p^r, unless each $\lambda_r = \mu_r$ the two sides of this equation are not even isomorphic as abelian groups.

We must now consider the case when G is a 2-group and $c \neq 0$. Since $c : G \to \mathbf{Y}_2 \subset \mathbf{S}$ is a homomorphism, and b nonsingular, there is a well-defined element $\hat{c} \in G$, of order 2, such that for $y \in G$, $b(\hat{c}, y) = c(y) = b(y, y)$. First suppose $b(\hat{c}, \hat{c}) = c(\hat{c})$ non-zero; then it must be $\frac{1}{2}$. We observe that the restriction of b defines a nonsingular form on $H = \{\hat{c}\}$, so by Lemma (1), we have $G = H \oplus H^\circ$. Moreover H° is orthogonal to $\hat{c}$, i.e. c vanishes on it, so we can use Lemma (7) to describe H°. We write Y_2 for the element of $\mathfrak{M}$ defined by H: it is generated by an element x of order 2, and $b(x, x) = \frac{1}{2}$.

Now suppose $b(\hat{c}, \hat{c}) = 0$. Let $\hat{c}$ have height r in the finite 2-group G: then we can write $\hat{c} = 2^{r-1}x$, with $\{x\}$ a direct summand of G. If $r = 1$, $x = \hat{c}$ and so $b(x, x) = 0$; if $r > 1$, $b(x, x) = c(x) = b(x, \hat{c}) = 2^{r-1}b(x, x)$ so as $b(x, x)$ has order 2, it must vanish. Now as in the proof of Lemma (7), since $\{x\}$ is a direct summand, we can find $y \in G$ with $b(x, y) = 2^{-r}$, and y of order 2^r. Again $\{x\}$ and $\{y\}$ form a direct sum H in G, we can verify that the restriction of b to H is nonsingular, so by Lemma (1), $G \cong H \oplus H^\circ$, and since $\hat{c} \in H$ is orthogonal to H°, c vanishes on H°. We write X_{2^r} for the class of H in $\mathfrak{M}$; this is the direct sum of cyclic groups of order 2^r generated by x and y, $b(x, x) = 0$, $b(x, y) = 2^{-r}$, and finally $b(y, y) = c(y) = b(\hat{c}, y) = 2^{r-1}b(x, y) = \frac{1}{2}$. So X_{2^r} is well-defined. This completes the proof of

THEOREM (3). *$\mathfrak{M}$ is generated by the W_{p^r}, Y_2 and X_{2^r}. More precisely, if for (G, b), c vanishes, (G, b) can be expressed uniquely as a sum of W_{p^r}. If $c(\hat{c}) \neq 0$, (G, b) is the sum of Y_2 and an element of $\mathfrak{M}_s$. If $c(\hat{c}) = 0$ and $\hat{c}$ has height r, (G, b) is the sum of X_{2^r} and an element of $\mathfrak{M}_s$.*

Using the uniqueness up to isomorphism of direct sum decompositions of abelian groups, we see that in each case, the element of $\mathfrak{M}_s$ is well-defined.

COROLLARY. $Y_2 + Y_2 = X_2$, $Y_2 + X_{2^r} = Y_2 + W_{2^r}$, *and if* $r \leq s$,
$$X_{2^r} + X_{2^s} = X_{2^r} + W_{2^s}.$$

These relations follow on applying the theorem to the expressions on the left hand sides of the equations. They show that the generator X_2 is unnecessary, and also how to express any sum of the generators of $\mathfrak{M}$ in standard form.

The monoid $\mathfrak{M}$ is intimately related to the classification of simply-connected 5-manifolds; we refer the reader to [2] (for $\mathfrak{M}_s$) and [1] (for the general case).

§5. NONSINGULAR SYMMETRIC FORMS ON FINITE GROUPS

This section aims to do the same for symmetric forms as the previous one accomplished for skew forms. However, considerable extra complications arise in the case of 2-groups, and as we do not yet possess a complete description, we shall omit here all discussion of relations between the generators of the monoid in that case.

We write $\mathfrak{N}$ for the monoid of isomorphism classes of finite groups with nonsingular symmetric bilinear form, where addition is defined by orthogonal sum. We shall frequently refer simply to a group, and leave the corresponding form understood. If G is expressed as an (orthogonal) direct sum, we shall call it *split*, and refer to such an expression as a *splitting*.

As in §4, any G splits as the sum of its Sylow subgroups; this is a characteristic splitting, and the monoid $\mathfrak{N}$ is the direct sum of monoids $\mathfrak{N}_p$ corresponding to p-primary groups for various primes p. A *homogeneous* group is a direct sum of cyclic groups of the same order p^r. Now if G is any p-group write G_k for the set of elements of G of order dividing p^k (clearly a subgroup) and
$$\rho_k(G) = G_k/(G_{k-1} + pG_{k+1});$$
this has exponent p, and if G is a (non-orthogonal!) direct sum of r_k cyclic groups of each order p^k, then $\rho_k(G)$ has rank r_k. Any form b on G determines a form b' on $\rho_k(G)$: writing $[x]$ for the coset containing x, we can put, for $x, y \in G_k$,
$$b'([x], [y]) = p^{k-1}b(x, y);$$
this is well-defined.

LEMMA (8). (i). *If H is homogeneous, exponent p^k, b a symmetric bilinear form on H, then (H, b) is nonsingular if and only if $(\rho_k(H), b')$ is;*

(ii). *A splitting of H determines one of $\rho_k(H)$, and all splittings of $\rho_k(H)$ arise in this way;*

(iii). *G splits into homogeneous groups H_k, and $\rho_k(H_k) = \rho_k(G)$;*

(iv). *Each $\rho_k(G)$ is nonsingular.*

Proof. (i). Let $\{e_i\}$ be a basis for H, and $b(e_i, e_j) = p^{-k}a_{ij}$ (mod 1). Then b is nonsingular if and only if the determinant $|a_{ij}|$ is prime to p. Since for $\rho_k(H)$ we have the same

a_{ij}, the result follows. For the rest of the proof, in accordance with our convention, each group is associated with a nonsingular symmetric form.

(ii). It is clear, from the description above, that a splitting of H determines one of $\rho_k(H)$. Conversely, given a splitting of $\rho_k(H)$, choose a basis $\{e_i : 1 \leqslant i \leqslant n\}$ of H such that the cosets $\{[e_i] : 1 \leqslant i \leqslant r\}$ generate one of the summands. Then by (i), the subgroup K of H with basis $\{e_i : 1 \leqslant i \leqslant r\}$ is nonsingular, so by Lemma (1), H splits as $K \oplus K^\circ$. This determines the given splitting of $\rho_k(H)$.

(iii). Let G have exponent p^r. We deduce, as in (i), that $\rho_r(G)$ is nonsingular. Write G as a (non-orthogonal) direct sum of a homogeneous group H_r of exponent p^r and a group of smaller exponent. Then $\rho_r(H_r) = \rho_r(G)$ is nonsingular, so by (i), H_r is nonsingular, and by Lemma (1), $G \cong H_r \oplus H_r^\circ$. By induction on r, it follows that G can be split into homogeneous groups H_n. Since ρ_k is additive for direct sums, and $\rho_k(H_n) = 0$ for $k \neq n$ it follows that $\rho_k(G) = \rho_k(H_k)$.

(iv). This follows from the induction in (iii).

This lemma is the key to our discussion, particularly when p is odd (for p even, a refinement of ρ_k would be useful for a more detailed discussion, which we do not give). Since the $\rho_k(G)$ are of exponent p, we classify these next (of course this result is well-known). Let H have exponent p. If $x \in H$ and $b(x, x) \neq 0$, then b is nonsingular on $\{x\}$, so H splits (unless it is cyclic). But if $b(x, x) = 0$ for all x,

$$2b(x, y) = b(x, y) + b(y, x) = b(x + y, x + y) - b(x, x) - b(y, y) = 0$$

for all x, y so, if $p \neq 2$, b is zero, contradicting nonsingularity. Thus for $p \neq 2$, H splits into cyclic subgroups. Now $b(x, x) = a/p$ with a prime to p; if x is replaced by cx we obtain $b(cx, cx) = ac^2/p$. There are two essentially different cases; when a is a residue or a non-residue—denote the corresponding elements of $\mathfrak{N}$ by A_p and B_p.

Since a non-residue can be found which is a sum of two residues (e.g. the lowest positive non-residue), if $\{x\} + \{y\} = H$ represents $2A_p$, we can find an element z of H with $b(z, z)$ a non-residue, so by Lemma (1) $H = \{z\} \oplus \{z\}^\circ$, and $2A_p = B_p + C_p$ say. Now (c.f. (i) of Lemma (8)) the determinant $|a_{ij}|$ does give an invariant for groups of exponent p, and it follows that $C_p \neq A_p$. Then C_p must be B_p, and $2A_p = 2B_p$. Any group of exponent p and rank r has isomorphism class rA_p or $(r-1)A_p + B_p$, the determinant shows these to be different, thus there are no more relations.

We continue to suppose p odd, and determine the structure of $\mathfrak{N}_p$. Any group splits (Lemma (8(iv))) into homogeneous parts H_k. By the above, $\rho_k(H_k)$ splits into cyclic summands; by Lemma (8(ii)), so does H_k. But for a cyclic group of order p^k, with generator x, we still have $p^k b(x, x)$ prime to p, and by Hensel's lemma, if this is a quadratic residue modulo p, it also is modulo p^k. Thus if $\rho_k(H_k) = A_p$, H_k can be generated by x of order p^k with $b(x, x) = 1$; write A_{p^k} for this group. Similarly, B_p "lifts" to a well-defined B_{p^k}. Now $2A_p = 2B_p$, and $\rho_k(2A_{p^k}) = 2A_p = 2B_p$. By Lemma (8(ii)), we can "lift" the splitting on the right-hand side, and deduce that $2A_{p^k} = 2B_{p^k}$.

We have shown that $\mathfrak{N}_p$ is generated by the A_{p^k} and B_{p^k}, and that for each k, $2A_{p^k} = 2B_{p^k}$. We now say there are no further relations. For suppose

$$\Sigma_k(\alpha_k A_{p^k} + \beta_k B_{p^k}) = \Sigma_k(\gamma_k A_{p^k} + \delta_k B_{p^k}) \tag{1}$$

Apply ρ_k to each side; then

$$\alpha_k A_p + \beta_k B_p = \gamma_k A_p + \delta_k B_p.$$

But we proved above that a relation of this kind must be a consequence of $2A_p = 2B_p$; hence (1) is a consequence of the relations $2A_{p^k} = 2B_{p^k}$. The structure of $\mathfrak{N}_p$ for odd p is thus completely determined.

For the case $p = 2$ we shall only go far enough to find generators of $\mathfrak{N}_2$. As above, first consider groups of exponent 2. In this case the concepts "symmetric" and "skew-symmetric" coincide, and by Theorem (3) we have generators W_2, X_2 and Y_2, with relations $2Y_2 = X_2$, $Y_2 + X_2 = Y_2 + W_2$. We change notation and write A_2 for Y_2, E_2 for W_2: these are generators, and satisfy only $3A_2 = A_2 + E_2$.

Next we must determine homogeneous groups H with $\rho_k(H) = A_2$ or $= E_2$; by the same argument as above, these will be generators of $\mathfrak{N}_2$. In the first case, H is cyclic of order 2^k, and we must classify integers (modulo 2^k) up to multiplication by perfect squares. We can again use Hensel's lemma, but this now reduces the case $k > 3$ to the case $k = 3$. We obtain

$k = 2$	A_4	$b(x, x) = \frac{1}{4}$	B_4	$b(x, x) = -\frac{1}{4}$
$k \geqslant 3$	A_{2^k}	$b(x, x) = 2^{-k}$	B_{2^k}	$b(x, x) = -2^{-k}$
	C_{2^k}	$b(x, x) = 5.2^{-k}$	D_{2^k}	$b(x, x) = -5.2^{-k}$.

For lifting E_2, we proceed inductively. Let x, y be generators. For $k = 2$ we have $b(x, x)$ and $b(y, y) = 0$ or $\frac{1}{2}$; $b(x, y)$ is $\pm\frac{1}{4}$. If $b(x, x) \neq b(y, y)$, say $b(x, x) = 0$, $b(y, y) = \frac{1}{2}$, we replace y by $x + y$ and change $b(y, y)$ to zero. Then if $b(x, y) = -\frac{1}{4}$, replace y by $-y$. We obtain groups E_4, F_4 with

$$b(x, x) = b(y, y) = 0 \text{ or } \tfrac{1}{2}, \qquad b(x, y) = \tfrac{1}{4}.$$

It may be seen without much trouble that these are inequivalent. Now a similar argument can be used inductively (or perhaps we could again apply Hensel's lemma) to show that these have unique liftings for $k \geqslant 2$,

$$E_{2^k}, F_{2^k} \quad b(x, x) = b(y, y) = 0 \text{ or } 2^{1-k}, \qquad b(x, y) = 2^{-k}.$$

THEOREM (4). *The monoid $\mathfrak{N}$ is the direct product of the $\mathfrak{N}_p$. For p odd, $\mathfrak{N}_p$ has generators A_{p^k}, B_{p^k} $(k \geqslant 1)$, and sole relations $2A_{p^k} = 2B_{p^k}$.*

Generators of $\mathfrak{N}_2$ are A_{2^k}, E_{2^k} $(k \geqslant 1)$, B_{2^k}, F_{2^k} $(k \geqslant 2)$, C_{2^k}, D_{2^k} $(k \geqslant 3)$.

It turns out that for $\mathfrak{N}_2$ we have 4 kinds of relation between homogeneous groups of fixed exponent, (which we have classified), but also several more when we allow mixed types; the detailed description will be very complicated.

The reader may have noticed that our classification is close to that of quadratic forms (not unimodular) over the p-adic integers; our use of ρ_k in Lemma (8) resembles that of the

lattice L^a [6, §82I], and the result on $\mathfrak{R}_p$ parallels [6, Theorem (92.2)]. In fact the construction of §7 gives a very close relation between the two problems. In the case $p = 2$, the relation is less close, as the groups of exponent 2 and 4 are special.

§6. QUADRATIC FORMS ON FINITE GROUPS

We now come to the problem which gives a title to this paper. It turns out, however' that it is possible to reduce this problem to the one considered in §5. We use quadratic form in the sense of §3—i.e., G is a finite group, q a function on G whose values are rational numbers modulo 2 such that $q(-x) = q(x)$ and $b(x, y) = \frac{1}{2}\{q(x + y) - q(x) - q(y)\}$ (mod 1) is a nonsingular symmetric bilinear map of $G \times G$ to $\mathbf{S}$.

If direct sums are defined in the natural way, then (G, q) splits if and only if the corresponding (G, b) does, so we have the usual decomposition into p-primary components. There are now two very different cases to consider, according as p is even or odd.

Now we proved in §3 that $b(x, x) = q(x)$ (mod 1), and so $2b(x, x) = 2q(x)$ (mod 2). Hence

$$q((N + 1)x) - q(Nx) - q(x) = 2b(Nx, x) = 2Nq(x),$$

so by induction on N, $q(Nx) = N^2q(x)$. If now G has odd order, for any $x \in G$, $Nx = 0$ for some odd N, and $N^2q(x) = 0$, so the denominator of $q(x)$ is odd, and numerator even. We now say that q is determined by b, and in fact every nonsingular b corresponds to exactly one q. For, first, $b(x, x)$ has odd denominator, hence, second, for just one of the two classes modulo 2 which give $b(x, x)$ modulo 1, the numerator is even; so we must (and do) take $q(x)$ as this one. But now

$$q(x + y) - q(x) - q(y) = 2b(x, y)$$

holds modulo 1; since each side has odd denominator and even numerator, it also holds mod. 2. Thus b does determine q.

Now suppose G a 2-group, with no direct summands of order 2, G_2 the subgroup of elements of order 2, $G' = G/G_2$. Let b be a nonsingular symmetric bilinear form on G. Then we define a quadratic form q on G' by:

$$q([x]) = 2b(x, x) \pmod 2.$$

This is well-defined, for if $[x] = [x + z]$, then z has order 2, so by our hypotheses on G, $z = 2a$ for some a, and

$$\begin{aligned} b(x + z, x + z) - b(x, x) &= 2b(x, z) + b(z, z) \\ &= b(x, 2z) + b(a, 2z) = 0. \end{aligned}$$

Now

$$\begin{aligned} \tfrac{1}{2}\{q([x]\} + \{[y]) - q([x]) - q([y])\} &= b(x + y, x + y) - b(x, x) - b(y, y) \\ &= 2b(x, y) \end{aligned}$$

and this is clearly bilinear, so q is quadratic; evidently q is homogeneous. Since b is nonsingular on G, its associated homomorphism is an isomorphism, thus the associated homomorphism of $2b$ has kernel G_2, and induces an isomorphism of G', so that $2b$ induces a nonsingular form on G', and q is also nonsingular.

THEOREM (5). *Let q be a nonsingular homogeneous quadratic form on the finite 2-group G'. Then there is a group G with no direct summand of order 2, and a nonsingular symmetric bilinear form b on G such that (G, b) gives rise to (G', q) as above; moreover (G, b) is unique up to isomorphism.*

Proof. First choose a basis $\{e_i'\}$ of G'—i.e., generators of a set of cyclic subgroups of which G' is the direct sum. Take a corresponding set $\{e_i\}$, form a cyclic group on e_i of twice the order of that on e_i', and let G be their direct sum. Then $e_i \to e_i'$ induces a homomorphism $G \to G'$ with kernel G_2; also, each e_i has order at least 4.

Now if $b : G \times G \to \mathbf{S}$ is to give rise to q, we must have

$$\begin{aligned} b(e_i, e_i) &= \tfrac{1}{2}q(e_i') && \pmod 1 \\ 2b(e_i, e_j) &= \tfrac{1}{2}\{q(e_i' + e_j') - q(e_i') - q(e_j')\} && \pmod 1. \end{aligned}$$

Choose the $b(e_i, e_j)$ for $i \leqslant j$ to satisfy these relations, and extend to a symmetric bilinear map. To see that this can be done, we need only check that if e_i has order 2^r, $2^r b(e_i, e_j) = 0$; but this is 2^{r-1} times

$$\tfrac{1}{2}\{q(e_i' + e_j') - q(e_i') - q(e_j')\} = b'(e_i', e_j'),$$

where b' is the bilinear form which goes with q, and

$$2^{r-1}b'(e_i', e_j') = b'(2^{r-1}e_i', e_j') = b'(0, e_j') = 0.$$

Now since b' is nonsingular, so is each $\rho_{k-1}(b') = \rho_k(b)$, so by Lemma (8), b is nonsingular. Now b gives rise to a quadratic form q'' with bilinear form b'' (as described above) on G'; we have

$$b''(e_i', e_j') = 2b(e_i, e_j) = b'(e_i', e_j'),$$

so $b'' = b'$, and now since $q''(e_i') = 2b(e_i, e_i) = q(e_i')$, it follows that $q'' = q$. Thus (G, b) does indeed give rise to (G', q).

We must now prove uniqueness. Let b_1, b_2 be two forms on G, each giving rise to q on G'. Then $b_2 - b_1$ has order 2 everywhere, and vanishes on diagonal pairs. As in §1, we set

$$\begin{aligned} \gamma(e_i, e_j) &= b_2(e_i, e_j) - b_1(e_i, e_j) && i < j \\ &= 0 && i \geqslant j, \end{aligned}$$

and have $b_2 - b_1 = \gamma + \gamma^t$. Define $f : G \to G$ as $1 + (Ab_1)^{-1} \circ A\gamma$. Since this leaves elements of order 2 fixed, and adds to every element one of order 2, $f \circ f = 1$, so f is an involutory automorphism. And

$$\begin{aligned} b_1(f(x), f(y)) &= b_1(x, y) + b_1(x, (Ab_1)^{-1}(A\gamma)y) + b_1((Ab_1)^{-1}(A\gamma)x, y) + \\ &\qquad + b_1((Ab_1)^{-1}(A\gamma)x, (Ab_1)^{-1}(A\gamma)y) \\ &= b_1(x, y) + \gamma(y, x) + \gamma(x, y) + 0 = b_2(x, y), \end{aligned}$$

so the automorphism f carries b_1 into b_2. Thus (G, b_1) and (G, b_2) are isomorphic, and in fact the isomorphism f induces the identity on G'.

Theorem (5) completes the reduction of the classification problem for quadratic forms to that for symmetric bilinear forms; it also (for the author, at least) clarifies the nature of both kinds in characteristic 2 or whenever 2-torsion arises.

§7. AN INVARIANT OF SOME SINGULAR FORMS

Let H be a free abelian group, $\lambda : H \times H \to \mathbf{Z}$ an ε-symmetric bilinear form. We shall not assume λ nonsingular, but assume instead that $A\lambda$ is a monomorphism; then it is precisely the fact that $A\lambda$ is not onto which interests us. The cokernel is finite and we shall call it G. Now let $\bar{\lambda} : \bar{H} \times \bar{H} \to \mathbf{Q}$ be the rational extension of λ, which *is* nonsingular. So $A\bar{\lambda}$ is an isomorphism of $\bar{H}$ on $\bar{H} \otimes \mathbf{Q} = H \otimes \mathbf{Q}$; we let H' correspond to $H \otimes \mathbf{Z}$. Then $\bar{\lambda}$ induces $\lambda' : H' \times H' \to \mathbf{Q}$, and we see that the conditions of Lemma (4) are all satisfied, with $H' = K_1' = K_2'$ and $H = K_1 = K_2$ (recall that λ is ε-symmetric, so ϕ_1 and ϕ_2 are—up to sign-transposes). Thus λ induces a nonsingular pairing $b : G \times G \to \mathbf{S}$. Since λ is ε-symmetric, so is b.

As usual, various particular features must be observed. If $\varepsilon = -1$, then $\bar{\lambda}$ satisfies not merely $\bar{\lambda}(y, x) = -\bar{\lambda}(x, y)$ but also (as $\mathbf{Q}$ is torsion free) $\bar{\lambda}(x, x) = 0$. Thus for $g \in G$, $b(g, g) = 0$—or with a notation used earlier $c = 0$. Now suppose $\varepsilon = 1$ and λ even. Then we can find a quadratic form q on G (with our usual convention) with associated bilinear form b. For if $g \in G$ is the coset of x in H', write $q(g) = \lambda'(x, x) \pmod 2$. Any other element over g is of the form $x + y$ for $y \in H$, and

$$\lambda'(x + y, x + y) - \lambda'(x, x) = 2\lambda'(x, y) + \lambda(y, y);$$

since the right hand side is always an even integer, q is well-defined; it is evident that q is quadratic homogeneous, with associated bilinear map b. The above equation also shows that q is only well-defined if λ is even.

Unlike the situation in §2, the arguments here can by no means be reversed—quadratic forms over the integers are much more complicated than ones on finite groups. So perhaps it is surprising that we can prove

THEOREM (6). *Any nonsingular ε-symmetric or quadratic form on a finite group can be obtained as above, provided, if $\varepsilon = -1$, that $c = 0$.*

Proof. We do not know of any general construction which will proceed from G to H in this situation, so treat each case on its merits. Observe, however, that the direct sum of forms H gives rise to the direct sum of the corresponding forms G. It is therefore sufficient to prove the results for the generators of $\mathfrak{M}_s$ and $\mathfrak{N}$ given by Lemma (7) and Theorem (4), and by Theorem (5), a similar reduction is valid in the case of quadratic forms.

In each case we shall give the matrix of λ': that of λ will then be the inverse. If N is the order of G, i.e. the index of H in H', then the determinant of a matrix for λ is $\pm N$; hence for λ' is $\pm 1/N$. Also if the terms in the matrix of λ' are taken modulo 1, we get a matrix which represents b. Conversely if we have a matrix, whose determinant is $\pm 1/N$, and which, modulo 1, represents b it is easy to check that the inverse must be an integral matrix, and so represent an integral form λ, and then λ gives rise to b. For a quadratic form, the diagonal elements of the matrix are determined modulo 2. Since it is then clear that λ' does determine q, it follows from a remark above that the inverse integral matrix will have even diagonal elements.

The case $\varepsilon = -1$ is easy: for W_{p^r} we take the matrix

$$\begin{pmatrix} 0 & p^{-r} \\ -p^{-r} & 0 \end{pmatrix}.$$

Next consider symmetric forms: for A_{p^r} we can take (p^{-r}) and for E_{2^r} take

$$\begin{pmatrix} 0 & 2^{-r} \\ 2^{-r} & 0 \end{pmatrix}.$$

The remaining cases are less easy. In fact, for F_{2^r} we take

$$\begin{pmatrix} 2^{1-r} & 2^{-r} & 0 \\ 2^{-r} & 2^{1-r} & 1 \\ 0 & 1 & b \end{pmatrix},$$

where b is determined by

$$3b = 2^{r+1} + (-1)^r.$$

The other cases are all cyclic of order p^r, with a generator x and $b(x, x) = n \cdot p^{-r}$, where n is prime to p. We take the Euclidean algorithm, using this fact,

$$1 = nd_1 - p^r d_2$$

$$d_1 = a_1 d_2 - d_3 \qquad \text{(we can suppose } 0 < n < p^r$$

$$\vdots \qquad \text{and so } 0 < d_2 < d_1)$$

$$d_{k-1} = a_{k-1} d_k - 1$$

$$d_k = a_k$$

and then use the matrix

$$\begin{pmatrix} np^{-r} & 1 & 0 & \dots & 0 & 0 \\ 1 & a_1 & 1 & \dots & 0 & 0 \\ 0 & 1 & a_2 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & a_{k-1} & 1 \\ 0 & 0 & 0 & \dots & 1 & a_k \end{pmatrix}.$$

For by induction on i, we see that d_{k+1-i} is the determinant of the last i rows and columns, and hence p^{-r} is the determinant of the whole matrix.

Finally, we must consider quadratic forms. For groups of odd order, these are essentially the same as symmetric bilinear forms; we have A_{p^r} and B_{p^r} to consider. The quick method for A_{p^r} will not now work. We use the algorithmic method instead. Now the fact that n is prescribed modulo $2p^r$ is no embarrassment, since we can choose $|n|$ less than p^r, but we must have a_i even (since $q(0) = 0$). Now as p^r is odd, we may suppose d_1 even. Then just take (for each i) $a_{i-1}d_i$ as the closest even multiple of d_i to d_{i-1}: the remainder d_{i+1} has $|d_{i+1}| < |d_i|$ unless d_i divides d_{i-1}, so is the H.C.F. of d_1, d_2 and is ± 1. But since d_1 is even and d_2 odd, it is clear by induction that d_{2j+1} is even and d_{2j} odd, so if $d_i = \pm 1$, d_{i-1} is even, and $d_{i-1} = a_{i-1}d_i$ with a_{i-1} even. Hence we can find an algorithm with each a_i even, as required.

For quadratic forms on a cyclic 2-group, we can use the same algorithm, except that now n (and not p^r) is odd, so we take d_1 odd and d_2 even at the first stage; the argument is now essentially the same as before. The matrix given above for E_{2^r} is still all right; it

remains to consider F_{2r} where now $r \geqslant 1$. It suffices to take

$$\begin{pmatrix} 2^{1-r} & 2^{-r} & 0 & 0 \\ 2^{-r} & 2^{1-r} & 1 & 0 \\ 0 & 1 & 2a & 1 \\ 0 & 0 & 1 & 2b \end{pmatrix},$$

where

$$a = \tfrac{1}{3}(2^r - (-1)^r), \qquad b = (-1)^{r-1}.$$

This completes the proof of the theorem.

REFERENCES

1. D. BARDEN: On simply-connected 5-manifolds, to be published.
2. S. SMALE: On the structure of 5-manifolds, *Ann. Math., Princeton* **75** (1962), 38–46.
3. C. T. C. WALL: Killing the middle homotopy group of odd dimensional manifolds, *Trans. Amer. Math. Soc.* **103** (1962), 421–433.
4. C. T. C. WALL: On simply-connected 4-manifolds, *J. Lond. Math. Soc.*, to be published.
5. C. T. C. WALL: Classification problems in differential topology, *Topology* **2** (1963), 253–272, etc.
6. O. T. O'MEARA: *Introduction to quadratic forms*, Springer Verlag, Berlin (1963).

Trinity College,
Cambridge.