QUADRATIC FORMS ON FINITE GROUPS II

C. T. C. WALL

In my paper [1] I showed how a quadratic form on a finitely generated abelian group H led to one on a finite group G, and similarly for symmetric bilinear forms. The prototype for this is the relation between the intersection form on $H_k(M^{2k})$ for a manifold M, and the linking form on $H_{k-1}(\partial M)$. I also showed that any form on G could so arise, but did not discuss uniqueness.

Similar forms had already been considered by various authors [2; 3; 4] (including many of the results of [1] and some not to be found there); in particular, Kneser and Puppe [5] claimed that the symmetric bilinear form on G determined that on H up to stable equivalence, and proved this in the case $|G|$ odd. Complete proofs have since been given by Wilkens [Ph.D. thesis, University of Liverpool, 1971] and Durfee [Ph.D. thesis, Cornell University, 1971]; the former by lengthy matrix manipulations, the latter using a delicate p-adic analysis. Durfee in fact obtains the corresponding result for quadratic forms.

The object of this paper is to present a direct and simple proof of the latter result, which arose out of work on [6; Chapter 8]. The argument can be generalised to replace $\mathbb{Z}$ by any order in a finite algebra over $\mathbb{Q}$ with anti-involution, without essential change.

We adopt the notation of [1], particularly §7. Thus H is a free abelian group, $\lambda : H \times H \to \mathbb{Z}$ a symmetric bilinear form with each $\lambda(x, x)$ even; $\bar{\lambda} : \bar{H} \times \bar{H} \to \mathbb{Q}$ the rational extension of λ, assumed nonsingular, and

$$H' = \{y \in \bar{H} : \bar{\lambda}(x, y) \in \mathbb{Z} \quad \text{for all} \quad x \in H\}$$

the dual module of H. We have $G = H'/H$, and

$$b : G \times G \to S = \mathbb{Q}/\mathbb{Z}, \qquad q : G \to \mathbb{Q}/2\mathbb{Z}$$

are defined by

$$b(x+H, y+H) = \bar{\lambda}(x, y) \qquad (\text{mod } 1).$$

$$q(x+H) = \bar{\lambda}(x, x) \qquad (\text{mod } 2).$$

We wish to show that H is determined by G up to stable equivalence; that is, up to forming direct sums with unimodular even forms. This will be an easy consequence of our main result.

THEOREM *Suppose given even symmetric bilinear forms* $\phi_A : A \times A \to \mathbb{Z}$, $\phi_B : B \times B \to \mathbb{Z}$ *as above, and a homomorphism* $\alpha : A' \to B'$ *inducing an isomorphism*

$$\bar{\alpha} : A'/A \to B'/B$$

Received 29 November, 1971.

[BULL. LONDON MATH. SOC., 4 (1972), 156–160]

of quadratic forms. Then there exists a homomorphism $h : A' \to A$ *such that*

(i) *The map* $i = (h, 1, \alpha) : A' \to A \oplus A' \oplus B' = H(A) \oplus B'$ *is an isometric embedding.*

(ii) *Let* M *be the orthogonal complement of* $i(A')$. *Then the projection* $\pi : M \to A' \oplus B'$ *is injective, with image* $A' \oplus B$.

(iii) $H(A) \oplus B' = M \oplus i(A')$.

(iv) *The induced form on* M *is unimodular and even* $M \times M \to \mathbb{Z}$.

(v) *Let* P *be the inverse image in* $A' \oplus B'$ *of the graph of* $(-\bar{\alpha})$. *If*

$$j = (1, -\alpha) : A' \to A' \oplus B',$$

then $P = j(A') \oplus B$. *The composite* $M \to A' \oplus B \xrightarrow{(j,1)} P$ *is an isometry, where the form on* P *is induced from* $-\phi_A \oplus \phi_B$.

Proof. (i) The function on $A' \times A'$ given by

$$f(x, x') = \phi_A(x, x') - \phi_B(\alpha x, \alpha x')$$

is symmetric and bilinear; also, since $\bar{\alpha}$ is an isomorphism of quadratic forms, the function takes values in $\mathbb{Z}$ and is even on the diagonal. Hence† (e.g. using bases) we can choose a bilinear $g : A' \times A' \to \mathbb{Z}$ with

$$f(x, x') = g(x, x') + g(x', x).$$

Now since A and A' are dually paired by ϕ_A, g determines a homomorphism $h : A' \to A$ with

$$g(x, x') = \phi_A(x, h(x')).$$

Hence,

$$\begin{aligned}\phi_A(x, x') - \phi_B(\alpha x, \alpha x') &= f(x, x') \\ &= \phi_A(x, h(x')) + \phi_A(x', h(x)),\end{aligned}$$

and this is equivalent to the statement that i is an isometry.

(ii) M is the set of $(x, y, z) \in (A \oplus A' \oplus B')$ which are orthogonal to $(h(w), w, \alpha(w))$ for all $w \in A'$; i.e.

$$0 = \phi_A(x, w) + \phi_A(y, h(w)) + \phi_B(z, \alpha(w)). \tag{2}$$

If $y = z = 0$, then $\phi_A(x, w) = 0$ for all w, so $x = 0$ since ϕ_A is nondegenerate. Hence π is injective.

†This does not work with symmetric bilinear forms. However, we can simply take $h = 0$ and define a metabolic structure on $A \oplus A'$ by $\phi((a, f), (a', f')) = \phi_A(f, a') + \phi_A(a, f') + \phi_A(f, f') - \phi_B(\alpha' f, \alpha' f')$. Later details then need alteration, but this is the essential step.

The first two terms on the right-hand side of (2) are integers. Hence the image of z in B'/B is orthogonal to all $\bar{\alpha}(w)$, hence to all of B'/B. But this form is nonsingular, hence z has zero image. Thus $z \in B$.

Conversely, given any $y \in A'$, $z \in B$,

$$w \mapsto \phi_A(y, h(w)) + \phi_B(z, \alpha(w))$$

gives a linear map $A' \to \mathbb{Z}$; and any such map is given by $w \mapsto -\phi_A(x, w)$ for some $x \in A$.

(v) Let (x_1, y_1, z_1) and $(x_2, y_2, z_2) \in M$. Then their product is

$$\begin{aligned}
&\phi_A(x_1, y_2) + \phi_A(x_2, y_1) + \phi_B(z_1, z_2) \\
&= -\phi_A(y_1, h(y_2)) - \phi_B(z_1, \alpha(y_2)) - \phi_A(y_2, h(y_1)) - \phi_B(z_2, \alpha(y_1)) + \phi_B(z_1, z_2) \qquad \text{(by (2))} \\
&= -f(y_1, y_2) - \phi_B(z_1, \alpha(y_2)) - \phi_B(z_2, \alpha(y_1)) + \phi_B(z_1, z_2) \\
&= \phi_B(\alpha(y_1), \alpha(y_2)) - \phi_A(y_1, y_2) - \phi_B(z_1, \alpha(y_2)) - \phi_B(z_2, \alpha(y_1)) + \phi_B(z_1, z_2) \\
&= \phi_B(z_1 - \alpha(y_1), z_2 - \alpha(y_2)) - \phi_A(y_1, y_2).
\end{aligned}$$

Now the given map $M \to P$ takes $(x, y, z) \in M$ to $(y, z) \in A' \oplus B$ and thence to $(y, z - \alpha(y)) \in A' \oplus B'$. It follows at once that, indeed, we have an isometry.

(iv) By (v), it suffices to show that P is unimodular. Now the form on P is integral, for if (x_1, y_1) and (x_2, y_2) are in P, their product is

$$-\phi_A(x_1, x_2) + \phi_B(y_1, y_2).$$

Reducing x_1, x_2 mod A, etc., we see that modulo integers, this is

$$\begin{aligned}
\bar{y}_1 . \bar{y}_2 - \bar{x}_1 . \bar{x}_2 &= \bar{\alpha}\bar{x}_1 . \bar{\alpha}\bar{x}_2 - \bar{x}_1 . \bar{x}_2 \qquad &&\text{(definition of } P) \\
&= 0 &&(\bar{\alpha} \text{ an isometry}).
\end{aligned}$$

Conversely, let $u : P \to \mathbb{Z}$ be any homomorphism. Since A', B' are dual to A, B there exist $x_0 \in A'$, $y_0 \in B'$ such that for all $(x', y') \in A + B \subset P$,

$$u(x', y') = -\phi_A(x_0, x') + \phi_B(y_0, y'). \tag{3}$$

This also must hold for all $(x', y') \in A' \oplus B'$; hence in particular on P. It remains to show that $(x_0, y_0) \in P$, i.e. that $\bar{y}_0 = -\bar{\alpha}\bar{x}_0$. But (3) takes integer values on P: and for all $x \in A'$, $(x, -\alpha x) \in P$, so

$$\begin{aligned}
0 \equiv u(x, -\alpha x) &= \phi_B(y_0, -\alpha x) - \phi_A(x_0, x) \\
&\equiv \bar{y}_0 . (-\bar{\alpha}\bar{x}) - \bar{x}_0 . \bar{x} = -\bar{\alpha}\bar{x} . (\bar{y}_0 + \bar{\alpha}\bar{x}_0);
\end{aligned}$$

since B'/B is nonsingular, and $\bar{y}_0 + \bar{\alpha}\bar{x}_0$ is orthogonal to everything, it is zero.

Finally, the form is even since if $(x, y) \in P$,

$$\begin{aligned} \phi_B(y, y) - \phi_A(x, x) &\equiv q(\bar{y}) - q(\bar{x}) \pmod 2 && \text{(Def. of } q) \\ &= q(-\bar{\alpha}\bar{x}) - q(\bar{x}) && \text{(Def. of } P) \\ &\equiv 0 \pmod 2 && (\pm\bar{\alpha} \text{ preserve } q). \end{aligned}$$

(iii) Since $i(A')$ is nondegenerate, $i(A') \cap M = 0$ and $i(A') + M$ has finite index in $H(A) \oplus B'$. Now the forms on $H(A)$ and M are unimodular, and on A' and B' have determinant $\pm 1/N$, where N is the order of G. Thus $M \oplus i(A')$ and $H(A) \oplus B'$ have the same discriminant (up to sign), so the index is 1. (It is also not difficult to verify (iii) directly.)

COROLLARY 1. *There is an isometry $H(A) \oplus B \cong M \oplus A$. Hence A and B are stably equivalent.*

Take dual modules in (iii) above.

COROLLARY 2. *The signature of A is determined* mod 8 *by the quadratic form on G.*

For the signature of a unimodular even form is divisible by 8. This argument is due to Durfee, but in fact we have the following.

THEOREM 2.
$$\sum\{\exp[i\pi q(g)] : g \in G\} = \sqrt{|G|}\, \exp(i\pi\sigma/4).$$

This result appears as [7; Theorem 3.6]: the authors' proof is not given there, but one is included in an appendix to lecture notes on Symmetric Bilinear Forms by John Milnor and Dale Husemoller (issued from Haverford College, 1971) and a much simpler one in a revised form of these notes. It was discovered independently about the same time by D. Sullivan, but his proof is not yet available either. It was also announced earlier by van der Blij [8], in a more general form, with an outline proof which seems to have a serious gap in it. (I rediscovered this argument: the snag is that the multiple integral $\int \exp[i\pi f(u, u)]\, du$, where f is bilinear, does not converge for any known—to me—theory of integration.) The most important special case goes back to Gauss [9], and a great number of proofs have appeared since.

References

1. C. T. C. Wall, " Quadratic forms on finite groups and related topics ", *Topology* 2 (1964), 281–298.
2. H. Seifert, " Verschlingungsinvarianten ", *Sitz. Preuss. Akad. Wiss. Berlin* 26 (1933), 811–828.
3. H. van Kampen, " Invariants derived from looping coefficients ", *Amer. J. Math.*, 60 (1938), 595–610.
4. E. Burger, " Über gruppen mit Verschlingungen ", *J. reine angew, math.*, 188 (1950), 193–200.
5. M. Kneser and D. Puppe, " Quadratische Formen und Verschlingungsinvarianten von Knoten ", *Math. Z.*, 58 (1953), 376–384.

6. C. T. C. Wall, *Surgery on compact manifolds* (Academic Press, 1970).
7. G. Brumfiel, I. Madsen and J. Milgram, " Surgery, BPL, B TOP and the PL bordism rings ", Springer Lecture notes no. 249, 54–74.
8. F. van der Blij, " An invariant of quadratic forms mod 8 ", *Kon. ned. Akad. van Wet. Ser. A* 62 (1959), 291–293.
9. C. F. Gauss, " Summatio quarundarum serierum singularium," *Comm. Soc. reg. Gottingen rec.* 1 (1811).

University of Liverpool,
Liverpool L69 3BX.