QUADRATIC FORMS INVARIANT UNDER GROUP ACTIONS

BY

JORGE MORALES AND JEAN-MARC PIVETEAU

Introduction

Let K be a field and let G be a finite group. A K-bilinear form β : $V \times V \rightarrow K$ on a K[G]-module V is said to be G-invariant if $\beta(gv, gw) = \beta(v, w)$ for v, w in V and g in G. For simplicity, a symmetric nondegenerate G-invariant bilinear form will be called throughout a G-form.

In this paper we consider two equivalence relations on the set of G-forms on a given K[G]-module V, namely *isometry* and *projective isometry*. Two forms β_1 and β_2 are said to be *isometric* if there exists a K-automorphism f: $V \rightarrow V$ such that $\beta_1(f(v), f(w)) = \beta_2(v, w)$ for all v, w in V (notice that we do not require f to commute with the action of G). The forms β_1 and β_2 are said to be *projectively isometric* if there exists a non-zero constant k in K such that β_1 and $k\beta_2$ are isometric in the previous sense.

W. Feit proved in [2] for the cyclic group C_p of prime order p with $p \equiv 3 \pmod{4}$, that all positive-definite C_p -forms on the irreducible $\mathbb{Q}[C_p]$ -module of dimension p-1 are projectively isometric. He also proved by giving an explicit counterexample that this is false for $p \equiv 1 \pmod{4}$.

Our work originates in an attempt to generalize Feit's result. The question whether all positive-definite G-forms on a given irreducible K[G]-module V are projectively isometric is closely connected with two other problems, interesting for themselves. The first is the classification of all G-forms on V up to (projective) isometry. The second problem is to study the behavior of invariant forms under induction. More precisely, assuming that V is induced from a subgroup H of G, we wish to know which G-forms are obtained, up to isometry, by inducing H-forms (induction of forms is explained in Section 3).

We shall assume throughout this paper that the ground field K is a totally real number field, even though this hypothesis may not be essential for some of our statements.

Here is a summary of the contents of this article:

Section 1 explains the correspondence between symmetric G-invariant bilinear forms on V and G-invariant hermitian forms over the center of the

© 1992 by the Board of Trustees of the University of Illinois Manufactured in the United States of America

Received June 14, 1990.

¹⁹⁸⁰ Mathematics Subject Classification (1985 Revision). Primary 11E12.

endomorphism ring of V. This correspondence is applied repeatedly throughout the paper.

In Section 2 we calculate, under suitable hypotheses, the Hasse-Witt invariant of the difference of two G-forms (Proposition 2.1). We apply this result to obtain explicit criteria for (projective) isometry of G-forms (Theorem 2.2 and Theorem 2.4). We also generalize Feit's theorem [2] to arbitrary p-groups (Corollary 2.6).

Section 3 deals with induction of forms. We prove, under some assumptions, that a positive-definite G-form on an irreducible induced K[G]-module is isometric to a induced form (Theorem 3.1). In particular, for a nilpotent group G of odd order, all positive-definite G-forms on an irreducible K[G] = module are obtained, up to isometry, by inducing forms invariant by a cyclic subgroup (Corollary 3.2).

1. Lifting forms to the endomorphism ring

Let K be a field and let G be a finite group. Let V be an irreducible k[G]-module endowed with a G-form β . Since V is irreducible, the endomorphism ring $\operatorname{End}_{K[G]}(V)$ is a (skew-)field. The form β induces an involution $e \mapsto \overline{e}$ on $\operatorname{End}_{K[G]}(V)$ defined by

$$\beta(ev, w) = \beta(v, \bar{e}w) \text{ for all } v, w \in V.$$

The restriction of this involution to the center E of $\operatorname{End}_{K[G]}(V)$ is independent of the choice of β : Let β' be another G-form on V. The form β' can be written $\beta'(v, w) = \beta(av, w)$ for some K[G]-automorphism a of V. For any z in the center E we have

$$\beta'(zv,w) = \beta(azv,w)$$
$$= \beta(zav,w)$$
$$= \beta(av, \bar{z}w)$$
$$= \beta'(v, \bar{z}w).$$

The above computation shows that β' induces the same involution as β on E as claimed. This involution will be called the *canonical involution* on E.

If K is a totally real number field, then the canonical involution on E is either trivial or it coincides with complex conjugation (see e.g. [1, (50.37)]). The dual vector space $V^* = \text{Hom}_K(V, K)$ can be made into an E-vector space by setting $(e\phi)(v) = \phi(\bar{e}v)$ for e in E and ϕ in V^* . Similarly, the vector space $\text{Hom}_E(V, E)$ has the E-vector space structure given by $(e\Phi)(v)$ $= \Phi(v)\bar{e}$. We leave to the reader to see that the map

$$\operatorname{Hom}_{E}(V, E) \to \operatorname{Hom}_{K}(V, K),$$
$$\Phi \mapsto \operatorname{Tr}_{E/K}(\Phi)$$

is an E-isomorphism. This isomorphism induces a bijection

$$\operatorname{Herm}_{E,G}(V) \xrightarrow{\sim} \operatorname{Symm}_{K,G}(V),$$
$$h \mapsto \operatorname{Tr}_{E/K}(h) \tag{1}$$

between the set $\operatorname{Herm}_{E,G}(V)$ of G-invariant hermitian forms on V (with respect to the canonical involution) and the set $\operatorname{Symm}_{K,G}(V)$ of symmetric G-invariant bilinear forms on V.

We conclude this section by an example. Let C_n be the cyclic group of order *n*. The irreducible $\mathbb{Q}[C_n]$ -module *V* of dimension $\varphi(n)$ can be identified with $\mathbb{Q}(\zeta)$, where ζ is a primitive *n*th root of unity, and a fixed generator of C_n acts on $\mathbb{Q}(\zeta)$ by multiplication by ζ . The canonical involution on $E = \operatorname{End}_{\mathbb{Q}[C_n]}(V) = \mathbb{Q}(\zeta)$ is complex conjugation. Hence the bijection (1) can be written in this case

$$\mathbf{Q}(\zeta + \zeta^{-1}) \to \operatorname{Symm}_{\mathbf{Q},G}(V),$$
$$a \mapsto \beta_a,$$

where β_a is the form give by $\beta_a(v, w) = \text{Tr}_{\mathbf{O}(\zeta)/\mathbf{O}}(av\overline{w})$.

2. The classification of G-forms

We list here for convenience the notation that will be in force from now on:

G	:	a finite group
Κ	:	a totally real number field
V	:	a non-trivial irreducible K G -module
E	:	the center of $\operatorname{End}_{K[G]}(V)$
F	:	the subfield of E fixed by the canonical involution
$d_{E/F}$:	the center of $\operatorname{End}_{K[G]}(V)$ the subfield of <i>E</i> fixed by the canonical involution the determinant of trace form $(x, y) \mapsto \operatorname{Tr}_{E/F}(xy)$ the subgroup of elements of order at most 2 in the Brauer group
$Br_2(L)$:	the subgroup of elements of order at most 2 in the Brauer group
_		of L
N _a	:	the norm of the quaternion algebra $\left(\frac{a, d_{E/F}}{F}\right)$
(,) _n	:	the Hilbert symbol at the prime p
W(L)	:	the Witt ring of L
I(L)	:	the fundamental ideal of $W(L)$
$oldsymbol{\phi}_L$:	the Hilbert symbol at the prime \mathfrak{p} the Witt ring of L the fundamental ideal of $W(L)$ the Hasse-Witt homomorphism $\phi_L: I^2(L) \to Br_2(L)$

We shall assume henceforth the condition

(*) $\operatorname{End}_{K[G]}(V)$ is a commutative field and the canonical involution is non-trivial.

Instances of representations satisfying condition (*) include faithful irreducible representations over K of the following types of groups: abelian groups of order ≥ 3 , nilpotent groups of odd order (see [4], Satz 3).

We shall now calculate explicitly under assumption (*) the difference of two G-forms in the Witt group W(K). The class of a bilinear form β in the Witt ring will be denoted by $[\beta]$.

(2.1) PROPOSITION. Assume condition (*). Let β_1 and β_2 be two G-forms on V and let a be the unique element in F such that $\beta_1(x, y) = \beta_2(ax, y)$ for all x, y in V. Then the difference $[\beta_1] - [\beta_2]$ lies in $I^2(K)$ and its Hasse-Witt invariant is given by

$$\phi_K([\beta_1] - [\beta_2]) = \dim_E(V) \operatorname{Cor}_{F/K}\left(\frac{a, d_{E/F}}{F}\right).$$
(2)

Proof. Let $h: V \times V \to E$ be the hermitian form over E such that $\beta_1 = \operatorname{Tr}_{E/K}(h)$ (see (1)). Obviously we have $\beta_2 = \operatorname{Tr}_{E/K}(ah)$. We first compute the class of the form

$$X_a := \operatorname{Tr}_{E/F}(h) \perp \left(-\operatorname{Tr}_{E/F}(ah)\right)$$

in W(F). Choosing a diagonalization we write $h = \langle c_1, \ldots, c_n \rangle$, where the coefficients c_i are in the fixed field F and n is the dimension of V over E. On the one hand we have

$$\begin{split} X_a &= \langle 1, -a \rangle \otimes \operatorname{Tr}_{E/F}(h) \\ &= \langle 1, -a \rangle \otimes \langle 1, -d_{E/F} \rangle \otimes \langle 2c_1, \dots, 2c_n \rangle \\ &= \langle 1, -a, -d_{E/F}, ad_{E/F} \rangle \otimes \langle 2c_1, \dots, 2c_n \rangle \\ &= N_a \otimes \langle 2c_1, \dots, 2c_n \rangle. \end{split}$$

On the other hand, the forms N_a and cN_a are isometric over F for any c in F^* . Thus $[X_a] = n[N_a]$ in W(F). In particular $[X_a]$ belongs to $I^2(F)$. Using the commutativity of the diagram

(see e.g. [3, Section 6]) we obtain

$$\phi_{K}([\beta_{1}] - [\beta_{2}]) = \phi_{k} \operatorname{Tr}_{F/K}([X_{a}])$$
$$= n\phi_{K} \operatorname{Tr}_{F/K}([N_{a}])$$
$$= n \operatorname{Cor}_{F/K}\phi_{F}([N_{a}])$$
$$= n \operatorname{Cor}_{F/K}\left(\frac{a, d_{E/F}}{F}\right). \quad \Box$$

We are now able to formulate the main result of this section.

(2.2) THEOREM. Let V be a K[G]-module satisfying condition (*). Let β_1 and β_2 be two G-forms on V. Let $a \in F$ be such that $\beta_1(x, y) = \beta_2(ax, y)$.

- (I) Suppose that $\dim_E(V)$ is even. Then β_1 and β_2 are isometric if and only if they have the same signature.
- (II) Suppose that $\dim_E(V)$ is odd. Then β_1 and β_2 are isometric if and only if they have the same signature and

$$\prod_{\mathfrak{B}|\mathfrak{p}} \left(a, d_{E/F} \right)_{\mathfrak{B}} = 1 \tag{3}$$

for all primes \mathfrak{P} of K.

Proof. Recall that forms over number fields are classified by rank, discriminant, Hasse invariant, and signature. Evidently β_1 and β_2 have the same rank and discriminant, and by hypothesis they have the same signature. Hence we need only to test the vanishing of the Hasse-Witt homomorphism ϕ_K on the difference $[\beta_1] - [\beta_2]$.

- (I) If dim_E(V) is even then $\phi_K([\beta_1] [\beta_2]) = 0$ by Proposition 2.1.
- (II) If $\dim_E(V)$ is odd then identity (2) becomes

$$\phi_K([\beta_1]-[\beta_2])=\operatorname{Cor}_{F/K}\left(\frac{a,d_{E/F}}{F}\right).$$

Let now \mathfrak{p} be a prime of K and let \mathfrak{B} be a prime of F above \mathfrak{p} . Using the commutativity of the diagram

(see e.g. [5, Section 1]), and taking the sum over all primes \mathfrak{B} lying above \mathfrak{p} ,

we obtain the commutative diagram

which shows immediately that the p-component of $\operatorname{Cor}_{F/K}(a, d_{E/F}/F)$ is given by the product of Hilbert symbols

$$\prod_{\mathfrak{B}|\mathfrak{p}} (a, d_{E/F})_{\mathfrak{B}}.$$

This completes the proof of the theorem. \Box

(2.3) Remark. If \mathfrak{B} is inert in E then $Br_2(F_{\mathfrak{B}})$ can be identified with $F_{\mathfrak{B}}^*/N_{E/F}(E_{\mathfrak{B}}^*)$. With this identification, the natural map $Br_2(F_{\mathfrak{B}}) \to \mathbb{Z}/2\mathbb{Z}$ is given by $x \mapsto \operatorname{ord}_{\mathfrak{B}}(x) \pmod{2}$. Thus, in this case, condition (3) becomes

$$\sum_{\mathfrak{B}|\mathfrak{p}} \operatorname{ord}_{\mathfrak{B}}(a) \equiv 0 \; (\operatorname{mod} 2),$$

or equivalently,

$$\operatorname{ord}_{\mathfrak{p}}(N_{F/K}(a)) \equiv 0 \pmod{2f_{\mathfrak{p}}},$$

where $f_{\mathfrak{p}}$ is the inertial degree of \mathfrak{p} in F. With the same notation, we have:

- (2.4) THEOREM. Let V be a irreducible K[G]-module satisfying (*).
- (I) If $\dim_E(V)$ is even, then all positive-definite invariant bilinear forms are isometric.
- (II) If dim_E(V) is odd, then the following statements are equivalent:
 (a) [F:K] is odd;
 (b) All positive-definite G-forms are projectively isometric.

Proof. (I). Direct consequence of Theorem 2.2. (II). Assume now that $\dim_E(V)$ is odd.

(a) \Rightarrow (b). Since [F: K] is odd and E/K is normal, we can choose $d_{E/F}$ in K^* . Let β_1 and β_2 be positive-definite G-forms. Let a be in F such that $\beta_1(x, y) = \beta_2(ax, y)$ for all x, y in V. Let \mathfrak{p} be a prime of K and fix a prime

150

 \mathfrak{B}_0 of F above \mathfrak{p} . Let $\Gamma = \operatorname{Gal}(F/K)$. With this notation we have

$$\begin{split} \prod_{\mathfrak{B}|\mathfrak{p}} (a, d_{E/F})_{\mathfrak{B}} &= \prod_{\sigma \in \Gamma/\Gamma_{\mathfrak{B}_0}} (\sigma(a), d_{E/F})_{\mathfrak{B}_0} \\ &= (N_{F/K}(a), d_{E/F})_{\mathfrak{B}_0} \\ &= \prod_{\mathfrak{B}|\mathfrak{p}} (N_{F/K}(a), d_{E/F})_{\mathfrak{B}} \end{split}$$

(note that the order of $\Gamma_{\mathfrak{B}_0}$ is odd). Applying Theorem 2.2 we conclude that β_1 and $N_{F/K}(a)\beta_2$ are isometric.

(b) \Rightarrow (a). Let β_1 be a positive-definite G-invariant form on V. Choose a prime \mathfrak{p} of K such that $\mathfrak{p}O_F$ is the product of [F:K] distinct primes of F which are inert in E (such a prime exists by Tchebotarev's Density Theorem). Let $\mathfrak{B}_1, \ldots, \mathfrak{B}_{[F:K]}$ be the primes of F lying above \mathfrak{p} and let a be a totally positive element in F satisfying

$$\operatorname{ord}_{\mathfrak{B}_i}(a) = \begin{cases} 1 & \text{if } i = 1, \\ 0 & \text{if } i > 1. \end{cases}$$

Let $\beta_2(v, w) = \beta_1(av, w)$. By hypothesis, there exists k in K^* such that $k\beta_1$ and β_2 are isometric. By Theorem 2.2 part II (and Remark 2.3), we must have

$$\sum_{\mathfrak{B}|\mathfrak{p}} \operatorname{ord}_{\mathfrak{B}}(a) \equiv \sum_{\mathfrak{B}|\mathfrak{p}} \operatorname{ord}_{\mathfrak{B}}(k) \pmod{2}.$$
(4)

The left hand side of (4) is equal to 1 by the construction of a, and, since p is totally decomposed in F, the right hand side of (4) is given by

$$\sum_{\mathfrak{B}|\mathfrak{p}} \operatorname{ord}_{\mathfrak{B}}(k) = [F:K] \operatorname{ord}_{\mathfrak{p}}(k).$$

Therefore [F:K] must be odd. \Box

(2.5) COROLLARY. Let $K = \mathbf{Q}$ and assume condition (*). Suppose that G acts faithfully on V and that $\dim_E(V)$ is odd. If all positive-definite G-forms on V are projectively isometric, then the center Z(G) of G is cyclic and its order is either 2^{ν} with $0 \le \nu \le 2$, or of the form p^{ν} or $2p^{\nu}$ with p prime and $p \equiv 3 \pmod{4}$.

Proof. Let n = |Z(G)|. The statement being trivial for $n \le 2$ we may assume n > 2. Since G acts faithfully, the center Z(G) is mapped injectively into E^* , therefore Z(G) is cyclic and E contains the cyclotomic field $\mathbf{Q}(\zeta_n)$.

By Theorem 2.4 Part II the degree $[\mathbf{Q}(\zeta_n + \overline{\zeta_n}): \mathbf{Q}]$ must be odd, or equivalently, $\varphi(n)/2$ must be odd. This is true only for n = 4 or of the form p^{α} or $2p^{\alpha}$ with $p \equiv 3 \pmod{4}$. \Box

We also have a generalization of Feit's result.

(2.6) COROLLARY. Let G be a p-group (p > 2). Let V be a simple non-trivial Q[G]-module. The following statements are equivalent:

(a) $p \equiv 3 \pmod{4};$

(b) All positive-definite G-forms on V are projectively isometric.

Proof. Evident consequence of Theorem 2.4, since in this case E contains $\mathbf{Q}(\zeta_p)$ and is contained in $\mathbf{Q}(\zeta_{|G|})$. Notice also that condition (*) is automatically satisfied. \Box

3. Induction of forms

We keep the conventions and the notation from the previous section. Let H be a subgroup of G and let U be a K[H]-module. We write the induced K[G]-module $\operatorname{Ind}_{H}^{G}(U) = K[G] \otimes_{K[H]} U$ in the form

$$\operatorname{Ind}_{H}^{G}(U) = \bigoplus_{i=1}^{r} x_{i} \otimes U,$$

where $\{x_1, \ldots, x_r\}$ is a system of representatives of the left cosets of G (mod H). Let β be an H-form on U. The induced module $\operatorname{Ind}_{H}^{G}(U)$ inherits naturally the G-form $\tilde{\beta}$ defined by

$$\tilde{\beta}(x_i \otimes v, x_i \otimes w) = \delta_{ii}\beta(v, w),$$

which will be called the form induced from β . We have the following result.

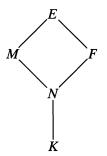
(3.1) THEOREM. Let H be a normal subgroup of prime index p in G (p > 2) and let U be a K[H]-module. Suppose that $V = \text{Ind}_{H}^{G}(U)$ is irreducible and satisfies condition (*) of the previous section. Then any positive-definite G-form on V is isometric to a G-form induced from a positive-definite H-form on U.

Proof. The induction functor $\operatorname{Ind}_{H}^{G}$ provides an injection of $M := \operatorname{End}_{K[H]}(U)$ into $E = \operatorname{End}_{K[G]}(V)$. Two cases have to be distinguished.

(a) M = E. In this case $\operatorname{Res}_{H}^{G}(V)$ is the orthogonal sum of non-isomorphic K[H]-submodules $x_i \otimes U$, where $\{x_1 = 1, x_2, \ldots, x_p\}$ is a system of representatives of G/H. Any G-form β on V is in this case the orthogonal sum of p copies of $\overline{\beta}: U \times U \to K$, where $\overline{\beta}$ is given by $\overline{\beta}(u, v) := \beta(1 \otimes u, 1 \otimes v)$.

152

(b) $M \subseteq E$. In this case $\operatorname{Res}_{H}^{G}(V)$ is isomorphic to $U \oplus \cdots \oplus U$; therefore $E \cong \mathbf{M}_{p}(M)^{G/H}$. Comparing the dimensions over M, we see that E/M is an extension of degree p. Note that complex conjugation is non-trivial on M (since [E:M] is odd, M cannot be contained in the subfield F of E fixed by complex conjugation). Let N be the intersection $M \cap F$. We sketch here for clarity the related tower of fields:



Let β_1 and β_2 be positive definite G-forms on V and assume that β_1 is a form induced from H, that is

$$\beta_1(x_i \otimes u, x_j \otimes v) = \delta_{ij}\overline{\beta}_1(u, v),$$

where $\overline{\beta}_1$ is a positive-definite *H*-form on *U*. Let $B_i: V \times V \to N$ be such that

$$\beta_i(x, y) = \operatorname{Tr}_{E/K}(B_i(x, y)) \quad \text{for } i = 1, 2.$$

Since [F:N] = p is odd, by Theorem 2.4 Part II, the forms B_1 and B_2 are projectively isometric, that is there exists a in N such that aB_1 and B_2 are isometric. Applying the trace $\operatorname{Tr}_{N/K}$ we see that the forms $\beta_3 := \operatorname{Tr}_{N/K}(aB_1)$ and $\beta_2 = \operatorname{Tr}_{N/K}(B_2)$ are isometric. We finish the proof by showing that β_3 is an induced form as well

$$\beta_{3}(x_{1} \otimes u, x_{j} \otimes v) = \operatorname{Tr}_{N/K}B_{3}(x_{i} \otimes u, x_{j} \otimes v)$$
$$= \operatorname{Tr}_{N/K}B_{1}(x_{i} \otimes au, x_{j} \otimes v)$$
$$= \overline{\beta}_{1}(au, v)\delta_{ii}. \quad \Box$$

(3.2) COROLLARY. Let G be a nilpotent group of odd order and let V be an irreducible K[G]-module. Let β be a positive-definite G-form on V. Then there exists a divisor n of |G| and a totally positive element a in the cyclotomic field $K(\zeta_n)$ such that β is isometric to an orthogonal sum

$$\beta_0 \perp \cdots \perp \beta_0,$$

where $\beta_0(x, y) = Tr_{K(\zeta_n)/K}(ax\overline{y})$.

Proof. We may assume that G acts faithfully on V. We prove the corollary by induction on the order of G. For |G| = 1 the statement is trivial. For |G| > 1 we have two possible cases.

- (1) If $V = \text{Ind}_{H}^{G}(U)$, where H is a subgroup of index p, then we apply Theorem 3.1 and the induction hypothesis.
- (2) If V is not induced, then, by [4, Section 3], the group G must be cyclic. \Box

(3.3) *Remark*. Corollary 3.2 together with Feit's theorem [2] give an alternative proof for Corollary 2.6.

Acknowledgement. The authors are grateful to the referee for her/his useful comments.

REFERENCES

- 1. C. CURTIS and I. REINER, Methods of representation theory, vol. II, Wiley, New York 1987.
- 2. W. FEIT, On certain rational quadratic forms, Linear and Multilinear Algebra, vol. 3 (1975), pp. 25-32.
- 3. C. RIEHM, The corestriction of algebraic structures, Invent. Math., vol. 11 (1970), pp. 73-98.
- P. ROQUETTE, Realisierung von Darstellungen endlicher nilpotenten Gruppen, Arch. Math., vol. 9 (1958), pp. 241–250.
- 5. J.-P. SERRE, "Local class field theory" in *Algebraic number theory*, J.W.S. Cassels & A. Fröhlich, editors, Academic Press, New York, 1967.

Louisiana State University Bâton Rouge, Louisiana Eidgen Technische Hochschule Zurich, Switzerland