Linear and Multilinear Algebra, Vol. 54, No. 6, December 2006, 391–396

Taylor & Francis
Taylor & Francis Group

A note on orthogonal similitude groups

C. RYAN VINROOT*

Department of Mathematics, Tata Institute of Fundamental Research,
Homi Bhabha Road, Mumbai – 400 005, India

Communicated by R. Guralnick

(*Received 18 October 2004; in final form 24 March 2005*)

Let V be a vector space over the field F such that $\mathrm{char}(F) \neq 2$, and let V have a symmetric nondegenerate bilinear form. Let $\mathrm{GO}(V)$ be the orthogonal similitude group for this symmetric form, with similitude character μ. We prove that if $g \in \mathrm{GO}(V)$ with $\mu(g) = \beta$, then $g = t_1 t_2$ where t_1 is an orthogonal involution, and t_2 is such that $t_2^2 = \beta I$ and $\mu(t_2) = \beta$. As an application, we obtain an expression for the sum of the degrees of the irreducible characters of $\mathrm{GO}(n, \mathbb{F}_q)$ for odd q.

Keywords: Similitude group; Orthogonal group; Factorization of matrices; Characters of the similitude group over a finite field

2000 AMS Subject Classifications: 15A23; 20G40

1. Introduction

This note is an addendum to [1], where we obtain a factorization in the symplectic similitude group. In Theorem 1 below, we obtain a factorization in the group of orthogonal similitudes $\mathrm{GO}(V)$, where V is an F-vector space with $\mathrm{char}(F) \neq 2$, and the similitude character is μ. The method is the same as in [1], and the notation established there is freely used. In the proof of Theorem 1, we refer to [1] to all parts that immediately apply to the orthogonal case, while any changes that are needed in the proof are given specifically.

As an application of Theorem 1, we use a result of Gow [2] on the orthogonal group over a finite field to obtain information on the characters of the orthogonal similitude group over a finite field, as given in Theorem 2 and Corollary 2. In a paper to appear by Adler and Prasad [3], Corollary 1 is used to prove a theorem on p-adic groups. In particular, if V is a vector space over a p-adic field, Adler and Prasad prove that any irreducible admissible representation of $\mathrm{GO}(V)$ restricted to $\mathrm{O}(V)$ is multiplicity free, and they also prove the corresponding statement for the symplectic similitude group.

*Email: vinroot@math.tifr.res.in

Linear and Multilinear Algebra
ISSN 0308-1087 print: ISSN 1563-5139 online
http://www.tandf.co.uk/journals
DOI: 10.1080/03081080500209588

2. The main theorem

Let V be an F-vector space, with $\mathrm{char}(F) \neq 2$, equipped with a nondegenerate bilinear symmetric form $\langle \cdot, \cdot \rangle : V \times V \to F$. Then the *orthogonal group of similitudes* of V with respect to this form is the group $\mathrm{GO}(V) = \{g \in \mathrm{GL}(V)\colon \langle gv, gw \rangle = \mu(g)\langle v, w \rangle$ for some $\mu(g) \in F^\times$ for all $v, w \in V\}$. Then $\mu : \mathrm{GO}(V) \to F^\times$ is a multiplicative character called the *similitude character*, and the *orthogonal group* is $\mathrm{O}(V) = \ker(\mu)$.

Theorem 1 *Let g be an element of $\mathrm{GO}(V)$ satisfying $\mu(g) = \beta$. Then we may factor g as $g = t_1 t_2$, where t_1 is an orthogonal involution and t_2 satisfies $t_2^2 = \beta I$ and $\mu(t_2) = \beta$.*

Proof Wonenburger [4] proved that any element of $\mathrm{O}(V)$ is the product of two orthogonal involutions. So if $\mu(g) = \beta$ is a square in F, then the theorem follows directly from Wonenburger's result. So we assume β is not a square.

As in [1], for any monic polynomial $f \in F[x]$ of degree d, define the *β-adjoint* of f to be

$$\hat{f}(x) = f(0)^{-1} x^d f(\beta/x),$$

and define a monic polynomial to be *self-β-adjoint* if $\hat{f} = f$. Then, for any $g \in \mathrm{GO}(V)$, the minimal polynomial of g is self-β-adjoint. All of the results in sections 2 and 3 of [1] are valid for transformations g which are self-β-adjoint, as the proofs only use this fact. These results reduce us to looking at the case that either g is a cyclic transformation for V, that is V is generated by vectors of the form $g^i v$ for some $v \in V$, or the case that g has minimal polynomial of the form $q(x)^s$, where $q(x)$ is an irreducible self-β-adjoint polynomial.

We deal with the cyclic case first. In [1, Proposition 3(i)], we prove that if $g \in \mathrm{GL}(V)$ is a cyclic transformation with self-β-adjoint minimal polynomial, ignoring any inner product structure, then we can factor $g = t_1 t_2$ such that $t_1^2 = I$ and $t_2^2 = \beta I$. This is proven as follows. If V is cyclic for the vector v, then we let P be the space spanned by vectors of the form $(g^i + \beta^i g^i)v$ and let Q be the space spanned by the vectors of the form $(g^i - \beta^i g^i)v$. Then $V = P \oplus Q$, and the transformation having P as its $+1$ eigenspace and Q as its -1 eigenspace is exactly the involution t_1 that we seek. For the case that $g \in \mathrm{GO}(V)$, we must show that this t_1 is orthogonal. Let $(g^i + \beta^i g^i)v \in P$ and $(g^j - \beta^j g^j)v \in Q$. Then we have:

$$\begin{aligned}
&\left\langle (g^i + \beta^i g^{-i})v,\ (g^j - \beta^j g^{-j})v \right\rangle \\
&\quad = \left\langle (g^i + \beta^i g^{-i})v,\ g^j v \right\rangle - \left\langle g^i v,\ \beta^j g^{-j} v \right\rangle - \left\langle \beta^i g^{-i} v,\ \beta^j g^{-j} v \right\rangle \\
&\quad = \left\langle (g^i + \beta^i g^{-i})v,\ g^j v \right\rangle - \left\langle g^j v,\ \beta^i g^{-i} v \right\rangle - \left\langle g^j v,\ g^i v \right\rangle \\
&\quad = \left\langle (g^i + \beta^i g^{-i})v,\ g^j v \right\rangle - \left\langle g^j v,\ (g^i + \beta^i g^{-i})v \right\rangle \\
&\quad = 0.
\end{aligned}$$

So P and Q are mutually orthogonal. Now let u and u' be any two vectors in $V = P \oplus Q$. Write $u = w + y$, $u' = w' + y'$, where $w, w' \in P$ and $y, y' \in Q$. We compute $\langle t_1 u, t_1 u' \rangle$:

$$\begin{aligned}
\left\langle t_1 u, t_1 u' \right\rangle &= \left\langle t_1(w + y),\ t_1(w' + y') \right\rangle = \left\langle w - y,\ w' - y' \right\rangle \\
&= \left\langle w, w' \right\rangle + \left\langle y, y' \right\rangle - \left\langle y, w' \right\rangle - \left\langle w, y' \right\rangle \\
&= \left\langle w, w' \right\rangle + \left\langle y, y' \right\rangle.
\end{aligned}$$

While computing $\langle u, u' \rangle$ gives us:

$$\begin{aligned}\langle u, u' \rangle &= \langle w + y,\ w' + y' \rangle \\ &= \langle w, w' \rangle + \langle y, y' \rangle + \langle y, w' \rangle + \langle w, y' \rangle \\ &= \langle w, w' \rangle + \langle y, y' \rangle.\end{aligned}$$

Therefore, we have $\langle t_1 u,\ t_1 u' \rangle = \langle u, u' \rangle$, and t_1 is orthogonal. Since g satisfies $\mu(g) = \beta$, then $t_2 = t_1 g$ satisfies $\mu(t_2) = \beta$.

We now deal with the case that the minimal polynomial of g is of the form $q(x)^s$, where $q(x)$ is irreducible and self-β-adjoint. It follows from [1, Lemmas 4 and 5] and the cyclic case above that we may assume that V is the sum of two cyclic spaces, and further we may assume that for any $u_1 \in V$ satisfying $q(g)^{s-1} u_1 \neq 0$, the cyclic space U_1 generated by u_1 is degenerate, and for an appropriate $u_2 \in V$, we have $V = U_1 \oplus U_2$ where U_2 is the cyclic space generated by u_2. We follow the proof of [1, Proposition 3(iii)]. We may write $U_1 = P_1 \oplus Q_1$ where P_1 is spanned by vectors of the form $(g^k + \beta^k g^{-k}) u_1$ and Q_1 is spanned by vectors of the form $(g^k - \beta^k g^{-k}) u_1$.

There are two different cases, the first is when either $q(x)$ is relatively prime to $x^2 - \beta$ or $q(x) = x^2 - \beta$ and s is odd. In this case, we find a $u_2 \in Q_1^{\perp}$, and $V = U_1 \oplus U_2$ where U_2 is cyclically generated by u_2. Then $U_2 = P_2 \oplus Q_2$, where P_2 is spanned by vectors of the form $(g^k + \beta^k g^{-k}) u_2$ and Q_2 is spanned by vectors of the form $(g^k - \beta^k g^{-k}) u_2$. Letting $P = P_1 \oplus P_2$ and $Q = Q_1 \oplus Q_2$, we are able to show that if t_1 is the involution with P as its $+1$ eigenspace and Q as its -1 eigenspace, then $(t_1 g)^2 = \beta I$ (for the symplectic group, we actually show this in the second case of Proposition 3(iii)). We need to show that t_1 is orthogonal. From the cyclic case above, we have $P_i \perp Q_i$ for $i = 1, 2$. In the proof of [1, Proposition 3(iii)], we show that $P_i \perp Q_j$ for $i \neq j$. So now $P \perp Q$, and from the argument in the cyclic case above, we have that t_1 is orthogonal, and so $t_2 = t_1 g$ satisfies $\mu(t_2) = \beta$.

In the case that $q(x) = x^2 - \beta$ and s is even, we are able to find a $u_2 \in P_1^{\perp}$ such that $V = U_1 \oplus U_2$, where U_2 is the space cyclically generated by u_2. We define P_2 and Q_2 as before. We let $P = P_1 \oplus Q_2$ be the $+1$ eigenspace and $Q = P_2 \oplus Q_1$ be the -1 eigenspace of an involution t_1, and this satisfies $(t_1 g)^2 = \beta I$. To show t_1 is orthogonal, we need only show that $P \perp Q$ and appeal to the cyclic case above. We have already shown $P_i \perp Q_i$ for $i = 1, 2$, so now we need $P_1 \perp P_2$ and $Q_1 \perp Q_2$. We have:

$$\begin{aligned}&\left\langle \left(g^k \pm \beta^k g^{-k}\right) u_1,\ \left(g^l \pm \beta^l g^{-l}\right) u_2 \right\rangle \\ &\quad = \left\langle \left(g^k \pm \beta^k g^{-k}\right) u_1,\ g^l u_2 \right\rangle \pm \left\langle \left(g^k \pm \beta^k g^{-k}\right) u_1,\ \beta^l g^{-l} u_2 \right\rangle \\ &\quad = \left\langle \beta^l g^{-l} \left(g^k \pm \beta^k g^{-k}\right) u_1,\ u_2 \right\rangle \pm \left\langle g^l \left(g^k \pm \beta^k g^{-k}\right) u_1,\ u_2 \right\rangle \\ &\quad = \pm \left\langle \left(g^l \pm \beta^l g^{-l}\right) \left(g^k \pm \beta^k g^{-k}\right) u_1,\ u_2 \right\rangle \\ &\quad = 0,\end{aligned}$$

since

$$\begin{aligned}&\left(g^l \pm \beta^l g^{-l}\right) \left(g^k \pm \beta^k g^{-k}\right) u_1 \\ &\quad = \left(g^{l+k} + \beta^{l+k} g^{-(l+k)}\right) u_1 \pm \beta^k \left(g^{l-k} + \beta^{l-k} g^{-(l-k)}\right) u_1 \in P_1\end{aligned}$$

and $u_2 \in P_1^{\perp}$. So now as before, we have t_1 orthogonal. This exhausts all cases, and the theorem is proved. ■

COROLLARY 1 *Any element of* $g \in \mathrm{GO}(V)$ *is conjugate to* $\mu(g)g^{-1}$ *by an orthogonal involution.*

3. Application over a finite field

Let G be a finite group with an order 2 automorphism ι, let (π, V) be an irreducible complex representation, and let $\hat{\pi}$ denote the contragredient representation. If ${}^{\iota}\pi \cong \hat{\pi}$, where ${}^{\iota}\pi(g) = \pi({}^{\iota}g)$, then we obtain a bilinear form $B_{\iota} : V \times V \to \mathbb{C}$ satisfying

$$B_{\iota}(\pi(g)v, {}^{\iota}\pi(g)w) = B_{\iota}(v, w) \quad \text{for every } v, w \in V. \tag{$*$}$$

By Schur's Lemma, this bilinear form is unique up to scalar, which means we have, for all $v, w \in V$,

$$B_{\iota}(v, w) = \varepsilon_{\iota}(\pi) B_{\iota}(w, v),$$

where $\varepsilon_{\iota}(\pi) = \pm 1$. That is, B_{ι} is either symmetric or skew-symmetric. Since the character of $\hat{\pi}$ is $\bar{\chi}$ if χ is the character of π, then ${}^{\iota}\pi \cong \hat{\pi}$ is equivalent to ${}^{\iota}\chi = \bar{\chi}$.

Let $\mathbb{F}_q$ be the finite field of q elements, and let q be odd. We let $\mathrm{O}(n, \mathbb{F}_q)$ be the orthogonal group for any symmetric form (split or nonsplit) for an $\mathbb{F}_q$-vector space. Let $\mathrm{GO}(n, \mathbb{F}_q)$ be the corresponding orthogonal similitude group with similitude character μ.

PROPOSITION 1 *Let q be odd and $G = \mathrm{GO}(n, \mathbb{F}_q)$. Define ι to be the order 2 automorphism of G that acts as ${}^{\iota}g = \mu(g)^{-1}g$. Then every irreducible representation π of G satisfies ${}^{\iota}\pi \cong \hat{\pi}$, that is, $\varepsilon_{\iota}(\pi) = \pm 1$.* ■

Proof From Corollary 2, we have g is conjugate to $\mu(g)g^{-1}$, and so g^{-1} is always conjugate to ${}^{\iota}g$. Thus every character satisfies ${}^{\iota}\chi = \bar{\chi}$, and so for every π we have $\varepsilon_{\iota}(\pi) = \pm 1$. ■

Gow [2] showed that for q odd, every irreducible representation of $\mathrm{O}(n, \mathbb{F}_q)$ is self-dual and orthogonal. This corresponds to ι being the identity automorphism, and $\varepsilon_{\iota}(\pi) = \varepsilon(\pi) = 1$. We are able to apply his result in order to obtain the following stronger version of Proposition 1.

THEOREM 2 *Let q be odd and $G = \mathrm{GO}(n, \mathbb{F}_q)$. Define ι to be the order 2 automorphism of G that acts as ${}^{\iota}g = \mu(g)^{-1}g$. Then every irreducible representation π of G satisfies $\varepsilon_{\iota}(\pi) = 1$.*

Proof Since $\varepsilon_{\iota}(\pi) = \pm 1$ from Proposition 1, then we have a bilinear form B_{ι} as in (*).

Let Z be the center of $G = \mathrm{GO}(n, \mathbb{F}_q)$ consisting of scalar matrices, and let $H = Z \cdot \mathrm{O}(n, \mathbb{F}_q)$. Then H is an index 2 subgroup of G consisting of elements whose similitude factor is a square in $\mathbb{F}_q^{\times}$. Every irreducible representation ϕ of $\mathrm{O}(n, \mathbb{F}_q)$ may be extended to an irreducible representation of H by just extending the central character to Z, and so any irreducible representation of H restricted to $\mathrm{O}(n, \mathbb{F}_q)$

is irreducible. Since H is an index 2 subgroup of G, every irreducible representation π of G restricted to H is either irreducible or the direct sum of 2 distinct irreducibles.

First assume that (π, V) of G restricts to an irreducible (π', V) of H. Then π' restricted to $\mathrm{O}(n, \mathbb{F}_q)$ is some irreducible ϕ. Note that for $g \in \mathrm{O}(n, \mathbb{F}_q)$, we have ${}^{\iota}g = g$. Then for any $g \in \mathrm{O}(n, \mathbb{F}_q)$ and $u, v \in V$, we have

$$B_\iota(\pi(g)u, {}^{\iota}\pi(g)v) = B_\iota(\phi(g)u, \phi(g)v) = B_\iota(u, v).$$

From Gow's result, we know that $\varepsilon(\phi) = 1$, so there is a nondegenerate symmetric bilinear form, unique up to scalar, satisfying

$$B(\phi(g)u, \phi(g)v) = B(u, v),$$

for all $g \in \mathrm{O}(n, \mathbb{F}_q)$, $u, v \in V$. So then B_ι must be a scalar multiple of B, and therefore must also be symmetric. Then we have $\varepsilon_\iota(\pi) = 1$.

Now assume that the irreducible (π, V) of G, when restricted to H, is isomorphic to the direct sum of two irreducible representations (π_1, V_1) and (π_2, V_2), which restrict to $\mathrm{O}(n, \mathbb{F}_q)$ to give the irreducibles (ϕ_1, V_1) and (ϕ_2, V_2), respectively. Now for any $g \in \mathrm{O}(n, \mathbb{F}_q)$, and $u, v \in V_1$, we have

$$B_\iota(\phi_1(g)u, \phi_1(g)v) = B_\iota(u, v).$$

Again from Gow's result, $\varepsilon(\phi_1) = 1$, and so there is a symmetric nondegenerate $\mathrm{O}(n, \mathbb{F}_q)$-invariant bilinear form B on V_1, unique up to scalar. Then if B_ι restricted to $V_1 \times V_1$ is nondegenerate, it would have to be a scalar multiple of B, and so B_ι would be symmetric on $V_1 \times V_1$. But since B_ι is either symmetric or skew-symmetric on all of $V \times V$, then being nondegenerate and symmetric on a subspace forces it to be symmetric everywhere. So now we must show B_ι is nondegenerate on $V_1 \times V_1$.

For $g \in \mathrm{O}(n, \mathbb{F}_q)$, $u \in V_1$, and $v \in V_2$, we have

$$B_\iota(\pi(g)u, {}^{\iota}\pi(g)v) = B_\iota(\phi_1(g)u, \phi_2(g)v) = B_\iota(u, v).$$

So if B_ι is nondegenerate on $V_1 \times V_2$, then we would have $\hat{\phi}_1 \cong \phi_2$. But $\phi_2 \cong \hat{\phi}_2$, and so we would have $\phi_2 \cong \phi_1$. This would imply that $\pi_1 \cong \pi_2$, since the central characters of π_1 and π_2 agree with the central character of π. But we cannot have π restricted to an index 2 subgroup be the direct sum of 2 isomorphic representations, by [5, Corollary 6.19]. So now B_ι must be zero on $V_1 \times V_2$, by Schur's Lemma, which means B_ι must be nondegenerate on $V_1 \times V_1$, since B_ι is nondegenerate on $V \times V$ and $V = V_1 \oplus V_2$. Therefore, B_ι is symmetric, and $\varepsilon_\iota(\pi) = 1$. ∎

Kawanaka and Matsuyama [6] obtained a formula for the invariants $\varepsilon_\iota(\pi)$ which generalized the classical formula of Frobenius and Schur. One of the results in [6], which generalizes the Frobenius–Schur involution formula, is that if $\varepsilon_\iota(\pi) = 1$ for all irreducible representations π of a group G, then the sum of the degrees of the irreducibles of G is equal to the number of elements in G satisfying $g\,{}^{\iota}g = 1$. From this and Theorem 2, we obtain the following.

Corollary 2 *Let q be odd and let* $G = \mathrm{GO}(n, \mathbb{F}_q)$*. The sum of the degrees of the irreducible representations of G is equal to*

$$\left|\{g \in G \mid g^2 = \mu(g)I\}\right|.$$

It is perhaps worth noting that in the case of the group of similitudes for a split orthogonal group over $\mathbb{F}_q$, this is equal to the number of symmetric matrices in G.

Acknowledgements

The author thanks Dipendra Prasad for pointing out the importance and interest of the orthgonal case, and the referee for several helpful suggestions.

References

[1] Vinroot, C.R., 2004, A factorization in $GSp(V)$. *Linear and Multilinear Algebra*, **52**(6), 385–403.
[2] Gow, R., 1985, Real representations of the finite orthogonal and symplectic groups of odd characteristic. *Journal of Algebra*, **96**(1), 249–274.
[3] Adler, J.D. and Prasad, D., On certain multiplicity one theorems. *Israel Journal of Mathematics* (To appear).
[4] Wonenburger, M., 1966, Transformations which are products of two involutions. *Journal of Mathematics and Mechanics*, **16**, 327–338.
[5] Isaacs, I.M., 1976, Character theory of finite groups. In: *Pure and Applied Mathematics*, Vol. 69 (New York: Academic Press [Harcourt Brace Jovanovich Publishers]).
[6] Kawanaka, N. and Matsuyama, H., 1990, A twisted version of the Frobenius–Schur indicator and multiplicity-free representations. *Hokkaido Mathematical Journal*, **19**(3), 495–508.