J. Austral. Math. Soc. (Series A) 33 (1982), 345–350

ABELIAN 2-SUBGROUPS OF FINITE SYMPLECTIC GROUPS IN CHARACTERISTIC 2

M. J. J. BARRY and W. J. WONG

(Received 25 September 1981)

Communicated by D. E. Taylor

Abstract

If Sp(V) is the symplectic group of a vector space V over a finite field of characteristic p, and r is a positive integer, the abelian p-subgroups of largest order in Sp(V) whose fixed subspaces in V have dimension at least r were determined in the preceding paper, in the case $p \neq 2$. Here we deal with the case $p = 2$. Our results also complete earlier work on the orthogonal groups.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*): 20 G 40.

Introduction

We consider the symplectic group Sp(V) of a vector space V over a finite field of characteristic 2, and, for each positive integer r, determine the abelian 2-subgroups of Sp(V) of largest order fixing the vectors of an r-dimensional subspace of V. (The corresponding problem for odd characteristic was solved in the preceding paper.) We also apply our results to the study of the abelian 2-subgroups of odd-dimensional orthogonal groups in characteristic 2, a case which was omitted in Wong (1981).

This paper is a continuation of the preceding article, Wong (1982). We shall assume familiarity with the notation, terminology and methods of that article, and quote lemmas and theorems from it without further reference.

1. Symplectic group

Let F be a finite field of characteristic 2, and consider a finite-dimensional vector space V over F, with an alternating bilinear form H. Assume V is

https://doi.org/10.1017/S1446788700018760 Published online by Cambridge University Press

nondegenerate, so that V has even dimension $2m$. For $0 \leqslant r \leqslant 2m$, we consider the set $\mathcal{A}(V, r)$ of all abelian p-subgroups of largest order fixing some r-dimensional subspace of V, and denote the order of subgroups in $\mathcal{A}(V, r)$ as $q^{f(m,r)}$, where $q = |F|$.

As for the case of odd characteristic, the analogues of Lemmas 3 and 4 hold for $\mathrm{Sp}(V)$, where now $B(t) = F$ for all t. If A is an abelian p-subgroup of $\mathrm{Sp}(V)$ fixing an r-dimensional subspace X, and x is a nonzero vector in rad X, then S can be defined as in Lemma 5, and $s = \dim S$ satisfies $0 \leqslant s \leqslant 2m - r - 1$. Since H is now symmetric, we do not have a nondegenerate form H_0 to use to show S is totally isotropic, and so we cannot deduce $s \leqslant m - 1$. We have a recursion formula, proved in the same way as Lemma 8. If $1 \leqslant r < 2m$, then

$$f(m, r) = \max\{g(m, r, s) \mid 0 \leqslant s \leqslant 2m - r - 1\},$$

where $g(m, r, s) = 1 + s + f(m - 1, \max(r - 1, s))$.

Our first result shows that we have the same order formulas as in the case of odd characteristic.

THEOREM A. *Let* $\mathrm{Sp}(V)$ *be the symplectic group of a* $2m$*-dimensional vector space* V *over a field* F *of* q *elements having characteristic* 2, *and let* $q^{f(m,r)}$ *be the largest order of an abelian* 2*-subgroup of* $\mathrm{Sp}(V)$ *fixing an* r*-dimensional subspace of* V.

(a) *If* $r \geqslant m$, *then* $f(m, r) = \frac{1}{2}(2m - r)(2m - r + 1)$.

(b) *If* $r < m$, *then* $f(m, r) = \frac{1}{2}m(m + 1)$.

PROOF. The result holds for $m = 0$ or $r = 2m$. We may suppose $m \geqslant 1$, $1 \leqslant r < 2m$, and use induction on m.

First suppose $r \geqslant m$. If $0 \leqslant s \leqslant 2m - r - 1$, then $g(m, r, s) = 1 + s + \frac{1}{2}(2m - r - 1)(2m - r)$, by inductive hypothesis. The maximum in the recursion formula occurs at $s = 2m - r - 1$, and $f(m, r) = \frac{1}{2}(2m - r)(2m - r + 1)$.

Now suppose $r < m$. If $0 \leqslant s \leqslant m - 1$, then $g(m, r, s) = 1 + s + \frac{1}{2}(m - 1)m$, by inductive hypothesis, so that the maximum value of $g(m, r, s)$ in this range is $\frac{1}{2}m(m + 1)$, occurring at $s = m - 1$. If $m - 1 \leqslant s \leqslant 2m - r - 1$, then $g(m, r, s) = 1 + s + \frac{1}{2}(2m - s - 2)(2m - s - 1)$, by inductive hypothesis. This is a convex function of s, so its maximum in this range occurs at $s = m - 1$ or $s = 2m - r - 1$. A check of values shows that the maximum value is $\frac{1}{2}m(m + 1)$, occurring only at $s = m - 1$, unless $m = 2$ and $r = 1$, when it occurs at $s = 1$ and $s = 2$. This proves Theorem A.

Again we denote by $\mathcal{S}_r(V)$ the set of all r-dimensional subspaces X of V such that $X \subseteq X^{\perp}$ or $X \supseteq X^{\perp}$, and write $A(X)$ for the subgroup of $\mathrm{Sp}(V)$ of all elements fixing X. If $X \subseteq Y$, we write $A(X, Y/X)$ for the subgroup of $\mathrm{Sp}(V)$ of all elements which fix both X and Y/X.

If $q = 2$ and $m = 2$, we also define a special subgroup as follows. Let $X \subset X'$, where X' is a totally isotropic subspace of dimension 2 in V, and X is a subspace of dimension 1 in X'. Then $A(X, X'/X)$ is a subgroup of order 16 in $\mathrm{Sp}(V)$ (actually a Sylow 2-subgroup), and we let $A^*(X, X'/X)$ be the subgroup of $A(X, X'/X)$ generated by all its elements of order 4. Choose another totally isotropic subspace Y' of dimension 2 such that $V = X' \oplus Y'$, take a basis x, x' of X' with $x \in X$, and let y, y' be the basis of Y' dual to x, x' relative to H. Then the elements of $A^*(X, X'/X)$ are just the linear transformations on V of the form

$$\begin{aligned} x &\to x, \\ x' &\to x' + ax, \\ y' &\to y' + ax' + (a + c)x, \\ y &\to y + ay' + cx' + bx, \end{aligned}$$

where $a, b, c \in F$, and $A^*(X, X'/X)$ is abelian of order 8.

THEOREM B. *Let* $\mathrm{Sp}(V)$ *be the symplectic group of a* $2m$*-dimensional vector space* V *over a field* F *of* q *elements having characteristic* 2, *and let* $\mathcal{A}(V, r)$ *be the set of all abelian* 2*-subgroups of* $\mathrm{Sp}(V)$ *of largest order fixing an* r*-dimensional subspace of* V.

(a) *If* $r \geqslant m$, *then* $\mathcal{A}(V, r) = \{A(X) \mid X \in \mathcal{S}_r(V)\}$.

(b) *If* $r < m$ *and* $m \neq 2$, *then* $\mathcal{A}(V, r) = \mathcal{A}(V, m)$.

(c) *If* $m = 2$ *and* $q > 2$, *then* $\mathcal{A}(V, 1)$ *consists of* $\mathcal{A}(V, 2)$ *together with all groups* $A(X, X^{\perp}/X)$, *where* $X \in \mathcal{S}_1(V)$.

(d) *If* $m = 2$ *and* $q = 2$, *then* $\mathcal{A}(V, 1)$ *consists of* $\mathcal{A}(V, 2)$, *the groups* $A(X, X^{\perp}/X)$, *and the groups* $A^*(X, X'/X)$, *where* $X \in \mathcal{S}_1(V)$, $X' \in \mathcal{S}_2(V)$, $X \subset X'$.

PROOF. It is easy to see, as in Theorem 2, that the groups named do lie in $\mathcal{A}(V, r)$ in each case.

Conversely, let $A \in \mathcal{A}(V, r)$, where we may assume $1 \leqslant r < 2m$. Take a degenerate r-dimensional subspace X fixed by A, choose a nonzero vector x in $\mathrm{rad}\, X$, and set up the situation of the proof of Lemma 6.

If $r \geqslant m$, then we know that $s = 2m - r - 1 \leqslant r - 1$, and so $A_1 \in \mathcal{A}(Z, r - 1)$. Since $f(m - 1, r) < f(m - 1, r - 1)$ from Theorem A, and A_1 fixes both S and the $(r - 1)$-dimensional subspace W, it follows that $S \subseteq W$. Since S and W are orthogonal to each other, S is totally isotropic, and the proof of Theorem 2(a) applies.

Now let $r < m$. We recall the crossed homomorphism method of Wong (1981). If $\mu \in A_1$, set

$$C_\mu = \{t \in Z \mid \sigma(\mu, t, b) \in A, \text{some } b\}.$$

https://doi.org/10.1017/S1446788700018760 Published online by Cambridge University Press

Then $\mu \to C_\mu$ is a crossed homomorphism $\gamma\colon A_1 \to Z/S$. If K is the kernel of γ,

$$K = \{\mu \in A_1 \mid C_\mu = S\},$$

then $|K| \geqslant |A_1|/q^{2m-s-2}$. Theorem A now gives an upper bound on the dimension of the subspace

$$T = \bigcap_{\mu \in K} \ker(\mu - 1).$$

The image of γ lies in T/S, and so we obtain a new lower bound $|K| \geqslant |A_1|/q^{\dim T - s}$, then a new upper bound for $\dim T$, and so on.

Take $s = m - 1$, which is the case except possibly when $m = 2$ and $r = 1$. If $m > 2$, or $m = 2$ and $K \neq 1$, then the method leads to the conclusion that $\dim T \leqslant m - 1$, so that $T = S$, and $A = \{\sigma(\mu, t, b) \mid \mu \in A_1,\ t \in S,\ b \in F\}$. Since $A_1 \in \mathcal{Q}(Z, m - 1)$, it follows from part (a) that S is totally isotropic, and hence A fixes $\langle x \rangle \oplus S$, so that $A \in \mathcal{Q}(V, m)$.

If $m = 2$, $s = 1$, and $K = 1$, then fix a hyperbolic pair x', $y' \in Z$, with $x' \in S$. Each element of A_1 has the form $\mu(a)$, where $a \in F$, and

$$\mu(a)x' = x',$$
$$\mu(a)y' = y' + ax'.$$

We can then write $\gamma(\mu(a)) = g(a)y' + S$, where g is a map of F into itself. The equations $(\mu - 1)t' = (\mu' - 1)t$, $H(\mu t', t) = H(\mu' t, t')$ of Lemma 4 give

$$g(a')ax' = g(a)a'x',$$
$$g(a)g(a')a' = g(a')g(a)a,$$

for all a, $a' \in F$. Take $a' = 1$, and let $k = g(a')$. Then

$$g(a) = ka, \qquad k^2 a = k^2 a^2,$$

for all $a \in F$. Since $K = 1$, we have $k \neq 0$, so that $a = a^2$ for all $a \in F$. Hence $q = 2$. Since $k = 1$, we see that $C_{\mu(a)} = \{ay' + cx' \mid c \in F\}$, and so

$$A = \{\sigma(\mu(a), ay' + cx', b) \mid a, b, c \in F\}.$$

Thus, $A = A^*(X, X'/X)$, where $X = \langle x \rangle$, $X' = \langle x, x' \rangle$.

We finally have the case $m = 2$, $s = 2$. Then $A_1 = 1$, $S = Z$, $A = \{\sigma(1, t, b) \mid t \in Z,\ b \in F\} = A(X, X^\perp/X)$, where $X = \langle x \rangle$. This completes the proof of Theorem B.

All the groups occurring in Theorem B are elementary abelian, except for the groups $A^*(X, X'/X)$, which have exponent 4. The existence of the groups $A(X, X^\perp/X)$ $(X \in \mathbb{S}_1(V))$ in $\mathcal{Q}(V, 1)$ in the case $m = 2$ can be explained in the theory of groups of Lie type. Here $\mathrm{Sp}(V)$ is a group of type B_2, and has a nontrivial graph automorphism which transforms the groups in $\mathcal{Q}(V, 2)$ into the groups $A(X, X'/X)$. Also, it can be shown that $\mathrm{Sp}(V)$ has a third class of maximal abelian 2-subgroups, of order $2q^2$, which are the groups $A^*(X, X'/X)$ when $q = 2$. Thus the existence of these groups in $\mathcal{Q}(V, 1)$ may be regarded as following from the "accidental" equality $2q^2 = q^3$.

A Sylow 2-subgroup P of $\mathrm{Sp}(V)$ is determined by a sequence of totally isotropic subspaces

$$0 = W_0 \subset W_1 \subset W_2 \subset \cdots \subset W_m,$$

such that $\dim W_i = i$, as the group $P(W_0, W_1, \ldots, W_m)$ of all elements of $\mathrm{Sp}(V)$ fixing all W_i/W_{i-1} $(1 \leqslant i \leqslant m)$. The proof of the following result is omitted.

THEOREM C. *Let $P = P(W_0, W_1, \ldots, W_m)$ be a Sylow 2-subgroup of the symplectic group* $\mathrm{Sp}(V)$ *of a $2m$-dimensional vector space V over a finite field of q elements having characteristic* 2.

(a) *If $m \neq 2$, then $A(W_m)$ is the unique abelian subgroup of largest order in P.*

(b) *If $m = 2$ and $q > 2$, then the abelian subgroups of largest order in P are $A(W_2)$ and $A(W_1, W_1^{\perp}/W_1)$.*

(c) *If $m = 2$ and $q = 2$, then the abelian subgroups of largest order in P are $A(W_2)$, $A(W_1, W_1^{\perp}/W_1)$ and $A^*(W_1, W_2/W_1)$.*

2. Orthogonal group, odd dimension

We can now complete the work on the orthogonal groups in Wong (1981), where the case of odd dimension and characteristic 2 was omitted. Let V be a vector space of dimension $2m + 1$ over a finite field F of characteristic 2, with a nondegenerate quadratic form Q. Then Q has defect 1, that is, the radical $V^{\perp}$ of V relative to the alternating bilinear form B associated with Q has dimension 1, by Dieudonné (1955), page 35. Also, the orthogonal group $O(V)$ fixes $V^{\perp}$ and acts faithfully as the symplectic group of degree $2m$ on the quotient space $\overline{V} = V/V^{\perp}$, which has a nondegenerate alternating bilinear form inherited naturally from B.

LEMMA. *Let $\sigma \in O(V)$, $x \in V$. Then σ fixes x if and only if σ fixes the image $\bar{x}$ of x in $\overline{V}$.*

PROOF. Suppose σ fixes $\bar{x}$, that is, $\sigma x - x \in V^{\perp}$. Then $B(x, \sigma x - x) = 0$, and so $Q(\sigma x) = Q(x) + Q(\sigma x - x)$. Since σ is orthogonal, we have $Q(\sigma x - x) = 0$. By nondegeneracy of Q, $\sigma x - x = 0$, so that σ fixes x. The converse is trivial. This proves the lemma.

https://doi.org/10.1017/S1446788700018760 Published online by Cambridge University Press

It follows that the fixed subspace in V of a subgroup A of $O(V)$ is the preimage of the fixed subspace in $\overline{V}$ of A as a subgroup of $\mathrm{Sp}(\overline{V})$. Now our results on the symplectic group translate immediately into results on the orthogonal group $O(V)$. Let $\mathcal{S}_r(V)$ denote the set of all r-dimensional subspaces X of V such that $X \supseteq X^\perp$ or $V^\perp \subseteq X \subseteq X^\perp$, where $X^\perp$ is the orthogonal complement of X in V relative to B, and write $A(X)$ for the subgroup of $O(V)$ of all elements fixing X. If $X \subseteq Y$, we write $A(X, Y/X)$ for the subgroup of $O(V)$ of all elements which fix both X and Y/X. For $q = 2$, $m = 2$, $X \in \mathcal{S}_2(V)$, $X' \in \mathcal{S}_3(V)$, $X \subset X'$, let $A^*(X, X'/X)$ be the subgroup of $A(X, X'/X)$ generated by its elements of order 4.

THEOREM D. *Let $O(V)$ be the orthogonal group of a $(2m+1)$-dimensional vector space V over a finite field of q elements having characteristic 2, let $\mathcal{A}(V, r)$ be the set of all abelian 2-subgroups of largest order fixing an r-dimensional subspace of V, and let $q^{f(m,r)}$ be the order of a subgroup in $\mathcal{A}(V, r)$.*

(a) *If $r > m$, then $f(m, r) = \frac{1}{2}(2m - r + 1)(2m - r + 2)$, and $\mathcal{A}(V, r) = \{A(X) \mid X \in \mathcal{S}_r(V)\}$.*

(b) *If $r \leqslant m$ and $m \neq 2$, then*

$$f(m, r) = \tfrac{1}{2}m(m+1), \quad \text{and} \quad \mathcal{A}(V, r) = \mathcal{A}(V, m+1).$$

(c) *If $m = 2$, $q > 2$, $r \leqslant 2$, then $f(2, r) = 3$, and $\mathcal{A}(V, r)$ consists of $\mathcal{A}(V, 3)$ together with all groups $A(X, X^\perp/X)$, where $X \in \mathcal{S}_2(V)$.*

(d) *If $m = 2$, $q = 2$, $r \leqslant 2$, then $f(2, r) = 3$, and $\mathcal{A}(V, r)$ consists of $\mathcal{A}(V, 3)$, the groups $A(X, X^\perp/X)$, and the groups $A^*(X, X'/X)$, where $X \in \mathcal{S}_2(V)$, $X' \in \mathcal{S}_3(V)$, $X \subset X'$.*

References

J. Dieudonné (1955), *La géométrie des groupes classiques* (Springer-Verlag, Berlin).

W. J. Wong (1981), 'Abelian unipotent subgroups of finite orthogonal groups,' *J. Austral. Math. Soc. Ser. A* **32**, 223–245.

W. J. Wong (1982), 'Abelian unipotent subgroups of finite unitary and symplectic groups,' J. *Austral. Math. Soc. Ser. A* **33**, 331–344.

Mathematics Department
Our Lady of Mercy College
Carysfort Park
Blackrock Co. Dublin
Ireland

Department of Mathematics
University of Notre Dame
Notre Dame, Indiana 46556
U.S.A.