J. Austral. Math. Soc. (*Series A*) **58** (1995), 232–247

ON THE FAITHFUL REPRESENTATIONS, OF DEGREE 2^n, OF CERTAIN EXTENSIONS OF 2-GROUPS BY ORTHOGONAL AND SYMPLECTIC GROUPS

S. P. GLASBY

(Received 5 February 1992; revised 7 August 1992)

Communicated by H. Lausch

Abstract

If R is a 2-group of symplectic type with exponent 4, then R is isomorphic to the extraspecial group 2^{1+2n}_{ϵ}, or to the central product $4 \circ 2^{1+2n}$ of a cyclic group of order 4 and an extraspecial group, with central subgroups of order 2 amalgamated. This paper gives an explicit description of a projective representation of the group A of automorphisms of R centralizing $Z(R)$, obtained from a faithful representation of R of degree 2^n. The 2-cocycle associated with this projective representation takes values which are powers of -1 if R is isomorphic to 2^{1+2n}_{ϵ} and powers of $\sqrt{-1}$ otherwise. This explicit description of a projective representation is useful for computing character values or computing with central extensions of A. Such central extensions arise naturally in Aschbacher's classification of the subgroups of classical groups.

1991 *Mathematics subject classification* (*Amer. Math. Soc.*): 20C15, 20G05.

1. Introduction

In [4] a constructive theory is outlined for certain split extensions of extraspecial p-groups by classical groups. The starting point is an absolutely irreducible representation of the extraspecial group, which is extended to the Weil representation of an associated classical group [3]. This theory is generalized here to include representations of the (generally non-split) extensions $2^{1+2n}_{\epsilon} \cdot O^{\epsilon}_{2n}(2)$ and $(4 \circ 2^{1+2n}) \cdot Sp_{2n}(2)$. (This notation is explained in Section 2 below and in [8].) Information about the faithful representations of these groups of degree 2^n can be obtained from a different approach. For example, if Γ is a classical group and R is a subgroup isomorphic to 2^{1+2n}_{ϵ} or $4 \circ 2^{1+2n}$, then the groups $2^{1+2n}_{\epsilon} \cdot O^{\epsilon}_{2n}(2)$ and $(4 \circ 2^{1+2n}) \cdot Sp_{2n}(2)$ may be viewed as subgroups of the normalizer $N_{\Gamma}(R)$ (see [1, 8] for details). The representations of

$2_\epsilon^{1+2n} \cdot O_{2n}^\epsilon(2)$ and $(4 \circ 2^{1+2n}) \cdot Sp_{2n}(2)$ are then obtained by considering the restriction of the action of Γ on its natural module. This approach was motivated by the desire to classify the maximal subgroups of the classical groups, and is useful for determining the quadratic and semilinear forms preserved by such representations. However, the approach taken in this paper is helpful for direct computation in these groups. Theorem 4′ (respectively Theorem 4) gives an explicit description of a projective representation of the group of the automorphisms of 2_ϵ^{1+2n} (respectively $4 \circ 2^{1+2n}$) fixing the centre, whose associated 2-cocycle takes values which are square (respectively fourth) roots of one. Moreover, Theorems 4′ and 4 are also useful for calculating the value of characters in $2_\epsilon^{1+2n} \cdot O_{2n}^\epsilon(2)$ and $(4 \circ 2^{1+2n}) \cdot Sp_{2n}(2)$.

2. Notation and terminology

A p-group E is called *extraspecial* if $E' = Z(E)$ has order p and $E/Z(E)$ is elementary abelian. Therefore $V = E/Z(E)$ may be viewed as a vector space over the field $\mathbf{F}_p$ of p elements. We are interested in the case when $p = 2$. Then the maps $Q : xZ(E) \mapsto x^2$ and $B : (xZ(E), yZ(E)) \mapsto x^{-1}y^{-1}xy$ may be interpreted as quadratic and alternating forms on V (see [7, 13.7, 13.8; 10, p. 97]). Each extraspecial 2-group has order 2^{2n+1} for some integer n, and is isomorphic to the central product of n extraspecial 2-groups of order 2^3 where the central subgroups are amalgamated. Let D_8 and Q_8 denote the dihedral and quaternion groups of order 8 respectively. There are two isomorphism classes of extraspecial 2-groups of order 2^{2n+1}, namely $2_+^{1+2n} = D_8 \circ D_8 \circ \cdots \circ D_8$ and $2_-^{1+2n} = Q_8 \circ D_8 \circ \cdots \circ D_8$, where the quadratic form associated with 2_ϵ^{1+2n}, $\epsilon = \pm$, has $2^{n-1}(2^n + \epsilon 1)$ zeroes. If 4 denotes the cyclic group of order 4, then the central products $4 \circ 2_+^{1+2n}$ and $4 \circ 2_-^{1+2n}$ are isomorphic [7, p. 361], so it is unambiguous to denote this group by $4 \circ 2^{1+2n}$.

It is convenient to use the ordered pair notation in [4, Section 2], for the elements of 2_ϵ^{1+2n} and $4 \circ 2^{1+2n}$, and their automorphism groups. Let V be a $2n$-dimensional vector space over the field $\mathbf{F}_2$, and let f be a bilinear form on V such that

$$B : (x, y) \mapsto f(x, y) - f(y, x) \tag{1}$$

is a non-degenerate alternating form. The set $E = V \times \mathbf{F}_2$ endowed with the multiplication

$$(x_1, \lambda_1)(x_2, \lambda_2) = (x_1 + x_2, \lambda_1 + \lambda_2 + f(x_1, x_2))$$

is an extraspecial group of order 2^{2n+1} denoted by $E(f)$. As noted in [4] it is possible to find a bilinear form f_ϵ such that $E(f_\epsilon) \cong 2_\epsilon^{1+2n}$. Denote the quadratic and alternating forms $x \mapsto f(x, x)$ and $(x, y) \mapsto f(x, y) - f(y, x)$ by Q and B respectively.

The elements of $4 \circ 2^{1+2n}$ are defined similarly. Let $k + 2\mathbb{Z}$ be an element of the quotient ring $\mathbb{Z}/2\mathbb{Z}$. It is notationally convenient, and well-defined, to interpret the

https://doi.org/10.1017/S1446788700038271 Published online by Cambridge University Press

elements $2(k+2\mathbb{Z})$ and $(k+2\mathbb{Z})^2$ of $\mathbb{Z}/2\mathbb{Z}$ as the elements $2k+4\mathbb{Z}$ and $k^2+4\mathbb{Z}$ of $\mathbb{Z}/4\mathbb{Z}$. If f is a $(\mathbb{Z}/2\mathbb{Z})$-bilinear form such that (1) is non-degenerate, then the set $H = V \times \mathbb{Z}/4\mathbb{Z}$ endowed with the multiplication

$$(x_1, \lambda_1)(x_2, \lambda_2) = (x_1 + x_2, \lambda_1 + \lambda_2 + 2f(x_1, x_2))$$

defines a group $H(f) \cong 4 \circ 2^{1+2n}$, where $2f(x_1, x_2)$ is viewed as an element of $\mathbb{Z}/4\mathbb{Z}$.

If $\alpha \in \mathrm{Aut}(E)$, then α fixes (0,1), so there exist maps $g_\alpha : V \to V$ and $q_\alpha : V \to \mathbf{F}_2$ defined by $(x, \lambda)\alpha = (xg_\alpha, \lambda + q_\alpha(x))$. Hence α corresponds to the ordered pair (q_α, g_α), and

$$(q_\alpha, g_\alpha)(q_\beta, g_\beta) = (q_\alpha + q_\beta g_\alpha, g_\alpha g_\beta)$$

where $q_\alpha + q_\beta g_\alpha$ denotes the function $x \mapsto q_\alpha(x) + q_\beta(xg_\alpha)$. Since $Q(x) = f(x, x)$ and $(x, 0)^2\alpha = ((x, 0)\alpha)^2$, g_α is an element of the orthogonal group $O(Q)$. Furthermore, since $((x, 0)(y, 0))\alpha = (x, 0)\alpha(y, 0)\alpha$, q_α is a quadratic form satisfying

$$f(xg_\alpha, yg_\alpha) - f(x, y) = q_\alpha(x + y) - q_\alpha(x) - q_\alpha(y) \tag{2}$$

for all $x, y \in V$. Conversely, if $g_\alpha \in O(Q)$, then the left-hand side of (2) is an alternating form so there exist $|V|$ quadratic forms q_α satisfying (2), all of which differ by a linear functional $V \to \mathbf{F}_2$, Given $y \in V$, let $B(-, y)$ denote the linear functional $x \mapsto B(x, y)$. As B is non-degenerate, $y \mapsto B(-, y)$ is an isomorphism between V and its dual. Since $(y, 0)^{-1}(x, \lambda)(y, 0) = (x, \lambda + B(x, y))$, it follows that the ordered pair $(B(-, y), 1)$ is a typical inner automorphism and $y \mapsto (B(-, y), 1)$ is an isomorphism $V \to \mathrm{Inn}(E)$. It is straightforward to check that

$$(q_\alpha, g_\alpha)^{-1}\,(B(-, y), 1)\,(q_\alpha, g_\alpha) = (B(-, yg_\alpha), 1)$$

and so $\mathrm{Aut}(E)$ is an extension $V \cdot O(Q)$ with the natural action of $O(Q)$ on V. (Greiss [6] showed that this extension is non-split if and only if $n \geq 3$.)

The elements of $\mathrm{Aut}(H)$ either fix or invert the central element (0,1). Thus the centralizer A of (0,1), has index 2 in $\mathrm{Aut}(H)$, and $\mathrm{Aut}(H)$ is a split extension of A by the subgroup $\langle \zeta \rangle$ where ζ is the automorphism $(x, \lambda) \mapsto (x, -\lambda)$. If $\alpha \in A$ then there exist maps $g_\alpha : V \to V$ and $q_\alpha : V \to \mathbb{Z}/4\mathbb{Z}$ defined by $(x, \lambda)\alpha = (xg_\alpha, \lambda + q_\alpha(x))$. Since α preserves commutators, so $g_\alpha \in \mathrm{Sp}(B)$, and since α preserves products, q_α satisfies

$$2f(xg_\alpha, yg_\alpha) - 2f(x, y) = q_\alpha(x + y) - q_\alpha(x) - q_\alpha(y). \tag{2'}$$

Conversely, if $g \in \mathrm{Sp}(B)$, then $B(xg, yg) = B(x, y)$ or

$$f(xg, yg) + f(yg, xg) = f(x, y) + f(y, x).$$

https://doi.org/10.1017/S1446788700038271 Published online by Cambridge University Press

So the function $F : V \times V \to \mathbf{F}_2$ defined by $(x, y) \mapsto f(xg, yg) - f(x, y)$ is symmetric (skew-symmetry equals symmetry in characteristic 2). As above, it is not hard to construct a function $q : V \to \mathbb{Z}/4\mathbb{Z}$ such that

$$2F(x, y) = q(x + y) - q(x) - q(y) \quad \text{for all } x, y \in V.$$

Indeed, if $e_1, \ldots, e_{2n}$ is a basis for V, then

$$(3') \qquad q\left(\sum_{i=1}^{2n} x_i e_i\right) = \sum_{i=1}^{2n} F(e_i, e_i)^2 x_i^2 + \sum_{1 \le i < j \le 2n} 2F(e_i, e_j) x_i x_j$$

is such a function. (As usual, the x_i and $F(e_i, e_j)$ are viewed as elements of $\mathbb{Z}/2\mathbb{Z}$ while $F(e_i, e_i)^2$, x_i^2 and $2F(e_i, e_j)x_i x_j$ are viewed as elements of $\mathbb{Z}/4\mathbb{Z}$.) Hence $V \cong \mathrm{Inn}(H)$ and A is an extension of V by $\mathrm{Sp}(B)$. (Greiss [6] showed that this extension is non-split for $n \ge 3$.)

The formula (3′) is useful for constructing explicit isomorphisms. For example, if $E(f_\epsilon) \cong 2_\epsilon^{1+2n}$, then we can show $4 \circ 2_+^{1+2n} \cong 4 \circ 2_-^{1+2n}$ by constructing an isomorphism $H(f_+) \to H(f_-)$. Assume, without loss of generality, that

$$f_+(x, y) - f_+(y, x) = f_-(x, y) - f_-(y, x) \quad \text{for all } x, y \in V,$$

then $(x, y) \mapsto f_+(x, y) + f_-(y, x)$ is symmetric. Using (3′) there is a function $q : V \to \mathbb{Z}/4\mathbb{Z}$ satisfying

$$2f_+(x, y) + 2f_-(x, y) = q(x + y) - q(x) - q(y).$$

Hence $(x, \lambda) \mapsto (x, \lambda + q(x))$ is an isomorphism $H(f_+) \to H(f_-)$.

3. Extending representations of H and E

Let $\rho = \rho_\epsilon$ be a faithful absolutely irreducible representation $2_\epsilon^{1+2n} \to GL_m(K)$. It follows from [5, Theorem 5.5.5] that ρ is (equivalent to) a tensor product of n two-dimensional irreducible representations of D_8 or Q_8. Hence $m = 2^n$ and K has characteristic $\neq 2$. It follows from the absolute irreducibility of ρ that the m^2 linear transformations $\{\rho(x, 0) \mid x \in V\}$ of the m-dimensional representation space over K, are linearly independent and hence form a basis. Ward [12] used this fact applied to the exponent-p extraspecial group to describe the Weil representation of $\mathrm{Sp}_{2n}(p)$ where p is odd. Using similar techniques, we will explicitly describe analogous projective representations of $\mathrm{Aut}(E)$ and A when $p = 2$.

Let $E = 2_\epsilon^{1+2n}$. If $\alpha \in \mathrm{Aut}(E)$, then denote by ρ^α the representation $e \mapsto \rho(e\alpha)$ of E. Since E has only one faithful absolutely irreducible representation of degree

https://doi.org/10.1017/S1446788700038271 Published online by Cambridge University Press

2^n (see [5, Theorem 5.5.5]), ρ and ρ^α are equivalent. Therefore there exists a linear transformation $s(\alpha)$, defined up to a scalar, such that $s(\alpha)^{-1}\rho(e)s(\alpha) = \rho^\alpha(e)$ for all $e \in E$. Hence $\alpha \mapsto s(\alpha)$ is a projective representations of $\mathrm{Aut}(E)$ extending the projective representation $(B(-, y), 1) \mapsto \rho(y, 0)$ of $\mathrm{Inn}(E)$. Similarly, we obtain a projective representation of A.

If $\alpha \in \mathrm{Aut}(E)$ or A, then define $I(\alpha)$ and $K(\alpha)$ to be the subspaces $\{v(1+g_\alpha) \mid v \in V\}$ and $\{v \in V \mid v(1+g_\alpha) = 0\}$, and set $i(\alpha) = \dim_{\mathbf{F}_2} I(\alpha)$ and $k(\alpha) = \dim_{\mathbf{F}_2} K(\alpha)$.

THEOREM 1. *The restriction of q_α to $K(\alpha)$ is $\mathbf{F}_2$-linear so there exists $y \in V$ such that $q_\alpha(x) = B(x, y)$ for all $x \in K(\alpha)$. If $y' \in V$ has a similar property, then $y + y' \in I(\alpha)$. Let $s = s(\alpha, y)$ be the linear transformation*

$$s = |K(\alpha)|^{-1} \sum_{u \in V} \rho(u, 0)\rho(y, 0)\rho^\alpha(u, 0)^{-1}.$$

Then

$$s^{-1}\rho(x, \lambda)s = \rho^\alpha(x, \lambda)$$

for all $(x, \lambda) \in E$ and

$$s = \sum_{x \in I(\alpha)} (-1)^{q_\alpha(u)+B(u,y)+f(u+y,x)}\rho(x + y, 0), \tag{4}$$

where u depends on x and satisfies $x = u(1+g_\alpha)$. Furthermore, $s(\alpha, y) = \pm s(\alpha, y')$.

PROOF. If $x_1, x_2 \in K(\alpha)$, then $q_\alpha(x_1 + x_2) = q_\alpha(x_1) + q_\alpha(x_2)$ follows from (2). If $q_\alpha(x) = B(x, y) = B(x, y')$ for all $x \in K(\alpha)$, then $y + y' \in K(\alpha)^\perp$. It is shown in [4, Lemma 5.2], that $K(\alpha)^\perp = I(\alpha)$.

Note that $|K(\alpha)|^{-1} = 2^{-k(\alpha)}$ and $2 \neq 0$. Since $\rho(0, 1) = \rho^\alpha(0, 1) = -1$, it is straightforward to show that $\rho(x, \lambda)s = s\rho^\alpha(x, \lambda)$ for all $(x, \lambda) \in E$. Hence, using the absolute irreducibility of ρ and Schur's lemma, we need only show $s \neq 0$ in order to conclude that s is invertible. It follows that $s \neq 0$ once we have established (4), as $\{\rho(x, 0) \mid x \in V\}$ is linearly independent and the coefficient of $\rho(x + y, 0)$ is ± 1 if $x \in I(\alpha)$. Now

$$\begin{aligned}\rho(u, 0)\rho(y, 0)\rho^\alpha(u, 0)^{-1} &= \rho(u + y, f(u, y))\rho(ug_\alpha, q_\alpha(u) + f(u, u)) \\ &= \rho(u(1 + g_\alpha)+y, q_\alpha(u)+B(u, y)+f(u + y, u(1 + g_\alpha))) \\ &= \rho(x + y, q_\alpha(u) + B(u, y) + f(u + y, x)),\end{aligned}$$

where $x = u(1 + g_\alpha)$. Since there are $|K(\alpha)|$ vectors u satisfying $x = u(1 + g_\alpha)$, it suffices to establish (4) by showing that for a fixed y, the expression $q_\alpha(u) + B(u, y) + f(u, x)$ depends on x and not on the element u satisfying $x = u(1 + g_\alpha)$. If $x = u(1 + g_\alpha) = u'(1 + g_\alpha)$, then $u + u' \in K(\alpha)$ so it follows from (2) that

$$f(u + u', x) = f((u + u')g_\alpha, u'g_\alpha) + f(u + u', u') = q_\alpha(u) + q_\alpha(u + u') + q_\alpha(u').$$

https://doi.org/10.1017/S1446788700038271 Published online by Cambridge University Press

Adding the equation $q_\alpha(u+u') = B(u+u', y)$ to the previous equation gives

$$q_\alpha(u) + B(u, y) + f(u, x) = q_\alpha(u') + B(u', y) + f(u', x),$$

as desired. Finally, since the coefficients in (4) of the basis elements are ± 1, it follows that $s(\alpha, y) = \pm s(\alpha, y')$. This completes the proof.

Suppose now that ρ is an absolutely irreducible faithful representation of H. Then ρ has degree 2^n and K is any field of characteristic $\neq 2$ containing a square root i of -1. If $\alpha \in \mathrm{Aut}(H)$, then ρ is equivalent to ρ^α if and only if $\alpha \in A$. Let $s(\alpha, y)$ be defined as above. The proof of Theorem 1′ is similar to that of Theorem 1 and hence is omitted.

THEOREM 1′. *If $\alpha \in A$, then*

$$s(\alpha, y)^{-1}\rho(x, \lambda)s(\alpha, y) = \rho^\alpha(x, \lambda)$$

for all $(x, \lambda) \in H$ and

$$s(\alpha, y) = \sum_{x \in I(\alpha)} i^{q_\alpha(u)+2B(u,y)+2f(u+y,x)}\rho(x+y, 0), \tag{4′}$$

where u depends on x and satisfies $x = u(1+g_\alpha)$. Furthermore, $s(\alpha, y)$ and $s(\alpha, y')$ differ by a multiple of a fourth root of 1.

4. Constructing the 2-cocycles

Let R equal $E = 2_\epsilon^{1+2n}$ or $H = 4\circ 2^{1+2n}$ and let $C = C_{\mathrm{Aut}(R)}(Z(R))$. For each $\alpha \in C$ choose some fixed y such that $q_\alpha(x) = B(x, y)$ for all $x \in K(\alpha)$, and denote $s(\alpha, y)$ by $s(\alpha)$. Let K_C denote the multiplicative group $\{\pm 1\}$ if $R = E$, and $\{\pm 1, \pm i\}$ if $R = H$. Then s is a projective representation of C satisfying $s(\alpha)s(\beta) = \sigma(\alpha, \beta)s(\alpha\beta)$ and σ is a 2-cocycle $C \times C \to K$. In this section, we define a new projective representation t of C whose corresponding 2-cocycle τ takes values in K_C. Using Schur's idea [9], we may construct a central extension C_τ of K_C by C, where multiplication in C_τ is defined by

$$(\lambda_1, \alpha_1)(\lambda_2, \alpha_2) = (\lambda_1\lambda_2\tau(\alpha_1, \alpha_2), \alpha_1\alpha_2), \qquad (\lambda_i, \alpha_i) \in K_C \times C.$$

Given a fixed $v \in V$, let g_v denote that symplectic transvection $g_v : x \mapsto x + B(x, v)v$. The set $\{g_v \mid v \in V\}$ is known to generate $\mathrm{Sp}_{2n}(2)$ (see [2]). Using the method outlined above, we may construct functions $q_v : V \to \mathbb{Z}_4$ such that $(x, \lambda) \mapsto$

https://doi.org/10.1017/S1446788700038271 Published online by Cambridge University Press

$(xg_v, \lambda + q_v(x))$ defines an automorphism of H. It is straightforward to verify that if q_v is defined by

$$q_v(x) = \begin{cases} f(x,v)^2 + f(v,x)^2 + 2f(x,v) & \text{if} \quad f(v,v) = 0, \\ 2f(x,v)f(v,x) + 2f(x,v) & \text{if} \quad f(v,v) = 1, \end{cases}$$

then g_v and q_v satisfy (2). Let α_v be the automorphism corresponding to the ordered pair (q_v, g_v). Clearly $K(\alpha_v) = \ker(1 + g_v) = \langle v \rangle^\perp$, and if $x \in K(\alpha_v)$, then $0 = B(x,v) = f(x,v) + f(v,x)$. Hence, if $x \in K(\alpha_v)$ then

$$\begin{aligned} f(x,v)^2 + f(v,x)^2 &= 2f(x,v)^2 = 2f(x,v) \quad \text{and} \\ 2f(x,v)f(v,x) &= 2f(x,v)^2 = 2f(x,v) \end{aligned}$$

so the restriction of q_v to $K(\alpha_v)$ is zero. If u satisfies $v = u(1 + g_v)$, then $B(u,v) = 1$ and calculations similar to those above show that

$$q_v(u) + 2f(u,v) = \begin{cases} f(u,v)^2 + (1 + f(u,v))^2 = 1 & \text{if} \quad f(v,v) = 0, \\ 2f(u,v)(1 + f(u,v)) \quad\quad = 0 & \text{if} \quad f(v,v) = 1. \end{cases}$$

Setting $y = 0$ in equation (4′) gives

$$s(\alpha_v) = \begin{cases} \rho(0,0) + i\rho(v,0) & \text{if} \quad f(v,v) = 0, \\ \rho(0,0) + \rho(v,0) & \text{if} \quad f(v,v) = 1. \end{cases} \tag{5′}$$

The following lemma provides useful information about symplectic (and orthogonal) transvections and underpins the proofs of Theorems 4 (and 4′). The proof of Lemma 2 is standard but is included here for the reader's convenience.

LEMMA 2. *Let B be a non-degenerate alternating bilinear form and let $g, h \in \mathrm{Sp}(B)$ where h is the symplectic transvection $x \mapsto x + B(x,v)v$ with $v \neq 0$.*

(a) *If $v \notin \mathrm{im}(1-g)$, then $\mathrm{im}(1-gh) = \mathrm{im}(1-g) \oplus \langle v \rangle$.*
(b) *If $v = u(1-g)$ and $B(u,v) \neq 1$, then $\mathrm{im}(1-gh) = \mathrm{im}(1-g)$.*
(c) *If $v = u(1-g)$ and $B(u,v) = 1$, then $\mathrm{im}(1-gh) = \mathrm{im}(1-g) \cap \langle u \rangle^\perp$.*

Hence, $\dim(\mathrm{im}(1-gh)) = \dim(\mathrm{im}(1-g)) + \epsilon$ where $\epsilon = 1, 0, -1$ depending on which of the above cases arise.

PROOF. If $w \in \ker(1-gh)$, then $wgh = w$ and so $wg = wh^{-1} = w - B(w,v)v$. Hence,

$$w(1-g) = w(1-h^{-1}) = B(w,v)v. \tag{6}$$

Suppose first that $v \notin \mathrm{im}(1-g)$. Then $w(1-g) = 0$ and $B(w,v) = 0$, so $w \in \ker(1-g) \cap \ker(1-h)$. Conversely, if $w \in \ker(1-g) \cap \ker(1-h)$, then $wgh = w$ and $w \in \ker(1-gh)$. Therefore,

$$\ker(1-gh) = \ker(1-g) \cap \ker(1-h)$$

https://doi.org/10.1017/S1446788700038271 Published online by Cambridge University Press

and taking orthogonal complements with respect to B gives

$$\operatorname{im}(1-gh) = \operatorname{im}(1-g) + \operatorname{im}(1-h).$$

This proves (a) because $\operatorname{im}(1-h) = \langle v\rangle \not\subseteq \operatorname{im}(1-g)$.

Suppose now that $v = u(1-g)$. If $w \in \ker(1-gh)$, then it follows from (6) that $(w - B(w,v)u)(1-g) = 0$. Hence, $w - B(w,v)u \in \ker(1-g)$ and $\ker(1-gh) \subseteq \ker(1-g)+\langle u\rangle$. Taking orthogonal complements gives $\operatorname{im}(1-gh) \supseteq \operatorname{im}(1-g)\cap\langle u\rangle^{\perp}$.

Clearly $\operatorname{im}(1-gh) \subseteq \operatorname{im}(1-g)$ because

$$\begin{aligned} x(1-gh) &= x - (xg)h \\ &= x - xg - B(xg, v)v \\ &= (x - B(xg, v)u)(1-g). \end{aligned}$$

Also $\operatorname{im}(1-gh) \subseteq \langle u\rangle^{\perp}$ is equivalent to $\langle u\rangle \subseteq \ker(1-gh)$, or $ug = uh^{-1}$, or $u - v = u - B(u,v)v$, or $B(u,v) = 1$.

Now $\operatorname{im}(1-g)\cap\langle u\rangle^{\perp}$ has codimension 1 in $\operatorname{im}(1-g)$ because $\langle u\rangle^{\perp}$ has codimension 1 in V, and $u \notin \ker(1-g)$ as $v \neq 0$. It follows from $\operatorname{im}(1-g) \supseteq \operatorname{im}(1-gh) \supseteq \operatorname{im}(1-g)\cap\langle u\rangle^{\perp}$ and the previous paragraph that $\operatorname{im}(1-gh) = \operatorname{im}(1-g)$ precisely when $B(u,v) \neq 1$ and $\operatorname{im}(1-gh) = \operatorname{im}(1-g)\cap\langle u\rangle^{\perp}$ precisely when $B(u,v) = 1$.

LEMMA 3. *Let $\alpha, \beta \in C = C_{\mathrm{Aut}(R)}(Z(R))$, and $K_C = \langle -1\rangle$ if $R \cong E$ and $\langle i\rangle$ if $R \cong H$.*

(i) *If $I(\alpha)\cap I(\beta) = \{0\}$, then $s(\alpha)s(\beta) = \sigma(\alpha,\beta)s(\alpha\beta)$ where $\sigma(\alpha,\beta) \in K_C$.*

(ii) *If $I(\alpha)\cap I(\beta) = I(\beta)\cap I(\beta^{-1}\alpha\beta) = \{0\}$, then $s(\beta)^{-1}s(\alpha)s(\beta) = \sigma s(\beta^{-1}\alpha\beta)$ where $\sigma \in K_C$.*

PROOF. (i) By (4) and (4′), $s(\alpha)$ and $s(\beta)$ have the form $\sum\lambda_x\rho(x,0)$ and $\sum\mu_y\rho(y,0)$ where x and y range over cosets $a + I(\alpha)$ and $b + I(\beta)$ respectively, and where $\lambda_x, \mu_y \in K_C$. If $z \in a + b + I(\alpha) + I(\beta)$, then the coefficient of $\rho(z,0)$ in the product $s(\alpha)s(\beta)$ is

$$\sum_{x+y=z} \lambda_x\mu_y(-1)^{f(x,y)}. \tag{7}$$

Since $I(\alpha)\cap I(\beta) = \{0\}$, each z can be written *uniquely* as $x+y$ with $x \in a+I(\alpha)$ and $y \in b + I(B)$. Therefore, the sum (7) has one summand and so is an element of K_C. Therefore by (4) or (4′), $\sigma \in K_C$.

(ii) It follows from part (i) that $s(\alpha)s(\beta) = \sigma_1 s(\alpha\beta)$ and $s(\beta)s(\beta^{-1}\alpha\beta) = \sigma_2 s(\alpha\beta)$ where $\sigma_1, \sigma_2 \in K_C$. Thus $s(\alpha)s(\beta) = \sigma s(\beta)s(\beta^{-1}\alpha\beta)$ where $\sigma = \sigma_1\sigma_2^{-1} \in K_C$. This completes the proof.

https://doi.org/10.1017/S1446788700038271 Published online by Cambridge University Press

Recall that $i(\alpha)$ is the $\mathbf{F}_2$-dimension of $I(\alpha) = \mathrm{im}(1 + g_\alpha)$.

THEOREM 4. *Let $s(\alpha)$ be defined as in (4′) and let t be the projective representation*

$$t : A \to GL_{2^n}(K) \quad \text{given by} \quad \alpha \mapsto (1+i)^{-i(\alpha)} s(\alpha).$$

If $t(\alpha)t(\beta) = \tau(\alpha, \beta)t(\alpha\beta)$, then $\tau(\alpha, \beta)^4 = 1$. Furthermore, the group

$$G = \left\{ i^k t(\alpha) \mid k \in \mathbb{Z}, \alpha \in A \right\}$$

normalizes $\rho(H)$ and is an extension of $H = 4 \circ 2^{1+2n}$ by $\mathrm{Sp}(B) = \mathrm{Sp}_{2n}(2)$.

PROOF. Let

$$s(\alpha) = \sum_{x \in a + I(\alpha)} \lambda_x \rho(x, 0), \quad s(\beta) = \sum_{y \in b + I(\beta)} \mu_y \rho(y, 0)$$

$$\text{and} \quad s(\alpha\beta) = \sum_{z \in c + I(\alpha\beta)} \nu_z \rho(z, 0)$$

where by (4′) $\lambda_x, \mu_y, \nu_z \in K_C$. If $z \in c + I(\alpha\beta)$, then equating the coefficient of $\rho(z, 0)$ in the equation $t(\alpha)t(\beta) = \tau(\alpha, \beta)t(\alpha\beta)$ gives

$$(1+i)^{-i(\alpha)-i(\beta)} \sum_{x+y=z} \lambda_x \mu_y (-1)^{f(x,y)} = \tau(\alpha, \beta)(1+i)^{-i(\alpha\beta)} \nu_z.$$

Hence to show that $\tau(\alpha, \beta) \in K_C$, it suffices to show that

$$\tau_z = (1+i)^{i(\alpha\beta)-i(\alpha)-i(\beta)} \sum_{x+y=z} \lambda_x \mu_y (-1)^{f(x,y)} \tag{8}$$

is an element if K_C for some $z \in c + I(\alpha\beta)$. If X is the set of inner automorphisms together with the α_v, $v \in V$, then $A = \langle X \rangle$ (see [2]). It suffices to show that $\tau(\alpha, \beta_i) \in K_C$ for all $\alpha \in A$ and $\beta_i \in X$ because it follows by induction and the 2-cocycle condition

$$\tau(\alpha, \beta_1 \cdots \beta_{r-1})\tau(\alpha\beta_1 \cdots \beta_{r-1}, \beta_r) = \tau(\alpha, \beta_1 \cdots \beta_r)\tau(\beta_1 \cdots \beta_{r-1}, \beta_r)$$

that $\tau(\alpha, \beta_1 \cdots \beta_r) \in K_C$.

If β is inner, then $g_\beta = 1$ so $I(\beta) = \{0\}$ and $i(\alpha\beta) - i(\alpha) - i(\beta) = 0$, also $\sigma(\alpha, \beta) \in K_C$ by Lemma 3(i). Similarly, if $\beta = \alpha_v$ and $v \notin I(\alpha)$, then $I(\alpha) \cap I(\beta) = \{0\}$. By Lemma 2(a), $i(\alpha\beta) = i(\alpha) + 1$ so $i(\alpha\beta) - i(\alpha) - i(\beta) = 0$. Hence, in both cases $\tau_z^4 = 1$ holds.

We now consider cases (b) and (c) of Lemma 2. Suppose that $\beta = \alpha_v$ and $v = u(1 + g_\alpha)$. An argument as in the previous paragraph shows that $\tau(\gamma, \alpha) \in K_C$ for all inner automorphisms γ. Since

$$\tau(\gamma, \alpha)\tau(\gamma\alpha, \beta) = \tau(\gamma, \alpha\beta)\tau(\alpha, \beta)$$

https://doi.org/10.1017/S1446788700038271 Published online by Cambridge University Press

and $\tau(\gamma, \alpha), \tau(\gamma, \alpha\beta) \in K_C$, it follows that $\tau(\alpha, \beta) \in K_C$ if and only if $\tau(\gamma\alpha, \beta) \in K_C$ for some inner automorphism γ. Therefore, by Theorem 1 there is no loss of generality in assuming that $q_\alpha(K(\alpha)) = 0$ and hence by (4′) that $\lambda_0 = 1$ and $\lambda_v = i^{q_\alpha(u)+2f(u,v)}$. Putting $z = 0$ in (8) gives

$$\tau_0 = (1+i)^{i(\alpha\beta)-i(\alpha)-i(\beta)}\left(\lambda_0\mu_0 + \lambda_v\mu_v(-1)^{f(v,v)}\right) \tag{9}$$

where by (5′) $\mu_0 = 1$ and

$$\mu_v = \begin{cases} i & \text{if} \quad f(v,v) = 0, \\ 1 & \text{if} \quad f(v,v) = 1. \end{cases}$$

It follows from the definition of q_α that $q_\alpha(0) = 0$ and it follows by setting $x = y = u$ in (2′) that $2q_\alpha(u) = 2f(ug_\alpha, ug_\alpha) + 2f(u,u)$. Substituting $u + v$ for ug_α shows

$$\begin{aligned} 2q_\alpha(u) &= 2f(u+v, u+v) + 2f(u,u) \\ &= 2(B(u,v) + f(v,v)). \end{aligned}$$

Hence,

$$\lambda_v = i^{q_\alpha(u)+2f(u,v)} = \pm i^{q_\alpha(u)} = \begin{cases} \pm 1 & \text{if} \quad B(u,v) + f(v,v) = 0, \\ \pm i & \text{if} \quad B(u,v) + f(v,v) = 1. \end{cases}$$

Consider case (b) of Lemma 2. Suppose that $\beta = \alpha_v$ where $v = u(1 + g_\alpha)$ and $B(u,v) = 0$. By Lemma 2(b), $i(\alpha\beta) = i(\alpha)$ and

$$\lambda_v = \begin{cases} \pm 1 & \text{if} \quad f(v,v) = 0, \\ \pm i & \text{if} \quad f(v,v) = 1, \end{cases}$$

and so substituting into (9) gives $\tau_0 = (1+i)^{-1}(1 \pm i) \in K_C$ as claimed.

Suppose now that $\beta = \alpha_v$ and $v = u(l + g_\alpha)$ where $B(u,v) = 1$. By Lemma 2(c), $i(\alpha\beta) = i(\alpha) - 1$ and

$$\lambda_v = \begin{cases} \pm i & \text{if} \quad f(v,v) = 0, \\ \pm 1 & \text{if} \quad f(v,v) = 1, \end{cases}$$

and so substituting into (9) gives $\tau_0 = (1+i)^{-2}(1 \pm 1) = 0$ or $-i$. However, τ_0 is non-zero and so $\tau_0 \in K_C$. Hence in all three cases $\tau(\alpha, \beta) \in K_C$. It is straightforward now to show that G is an extension of H by $\mathrm{Sp}(B)$. This completes the proof.

We now concentrate on projective representations of $\mathrm{Aut}(E)$. Let σ be the 2-cocycle associated with the projective representation s of $\mathrm{Aut}(E)$. Then the 2-cocycle τ associated with $t : \alpha \mapsto \lambda_\alpha s(\alpha)$ satisfies

$$\tau(\alpha, \beta) = \frac{\lambda_\alpha\lambda_\beta}{\lambda_{\alpha\beta}}\sigma(\alpha, \beta) \quad \text{for all } \alpha, \beta \in \mathrm{Aut}(E).$$

https://doi.org/10.1017/S1446788700038271 Published online by Cambridge University Press

We will choose the λ_α such that $\tau(\alpha, \beta)^2 = 1$, that is, so that σ is split up to a sign. Since $s((B(-, u), 1)) = \rho(u, 0)$ and $\rho(u, 0)\rho(v, 0) = \pm\rho(u + v, 0)$, we set $\lambda_\alpha = 1$ for all $\alpha \in \mathrm{Inn}(E)$.

Now $g_v : x \mapsto x + B(x, v)v$ is an element of the orthogonal group if and only if v is non-singular, that is $Q(v) = 1$. We argue that case (b) of Lemma 2 does not arise if $g, h \in O(Q)$. (Suppose to the contrary that $g, h \in O(Q)$ where $h : x \mapsto x+B(x, v)v$, $Q(v) = 1$, $v = u(1 - g)$ and $B(u, v) \neq 1$. Then

$$Q(ug) = Q(u + v) = Q(u) + Q(v) - B(u, v) \neq Q(u),$$

a contradiction.) If $\alpha_v = (q_v, g_v)$ where $Q(v) = 1$, then $\tau(\alpha_v) = \lambda_v(\rho(0, 0)+\rho(v, 0))$ by (5′). Thus

$$t(\alpha_v)^2 = \lambda_v^2(\rho(0, 0) + 2\rho(v, 0) - \rho(0, 0)) = 2\lambda_v^2\rho(v, 0).$$

Since $\alpha_v^2 = (B(-, v), 1)$ is inner, $t(\alpha_v^2) = s((B(-, v), 1)) = \rho(v, 0)$. Therefore $2\lambda_v^2 = \pm 1$ and it is necessary that the field K contain a square root of 2 or -2. Theorem (4′) shows that this condition is also sufficient to split σ up to a sign.

Let N be the set of non-singular vectors and let S be the set of singular vectors in V. The set $\{g_v \mid v \in N\}$ generates $O_{2n}^\epsilon(2)$, except for $O_4^+(2)$ where it generates a subgroup of index 2 (see [2, 11]). We consider this exceptional case. Let V be a 4-dimensional vector space with basis $e_1, \ldots, e_4$ over $\mathbf{F}_2$. Lee f be the bilinear form

$$f\left(\sum_{i=1}^{4} x_i e_i, \sum_{i=1}^{4} y_i e_i\right) = \sum_{i=1}^{2} (x_{2i-1}y_{2i-1} + x_{2i-1}y_{2i} + x_{2i}y_{2i}).$$

Then $E(f) \cong Q_8 \circ Q_8$ and $O_4^+(2)$ preserves the corresponding quadratic form. Now $O_4^+(2)$ permutes the set $N = \{e_1, e_1 + e_2, e_2, e_3, e_3 + e_4, e_4\}$ of non-singular vectors and is isomorphic to S_3 wr S_2 [8, 2.5.9]. The transvections stabilize the sets $\{e_1, e_1 + e_2, e_2\}$ and $\{e_3, e_3 + e_4, e_4\}$ and generate the subgroup $S_3 \times S_3$, while the orthogonal transformation $h' : e_1 \leftrightarrow e_2$, $e_3 \leftrightarrow e_4$ interchanges these sets. Thus $\{g_v \mid v \in N\} \cup \{h'\}$ generates $O_4^+(2)$. Furthermore, as $f(xh', yh') - f(x, y) = 0$ for all $x, y \in V$, there is an automorphism β' such that $g_{\beta'} = h'$ and $q_{\beta'} = 0$. Let X be the set of inner automorphisms together with the α_v, $v \in N$. Then X generates $\mathrm{Aut}(E)$ except when $E \cong Q_8 \circ Q_8$, in which case $X \cup \{\beta'\}$ does.

THEOREM 4′. *Let $s(\alpha)$ be defined as in* (4) *and let t be the projective representation*

$$t : \mathrm{Aut}(E) \to GL_{2^n}(K), \quad \alpha \mapsto \theta^{-i(\alpha)}s(\alpha)$$

where $\theta \in K$ satisfies $\theta^2 = \eta 2, \eta = \pm$. If $t(\alpha)t(\beta) = \tau(\alpha, \beta)t(\alpha\beta)$, then $\tau(\alpha, \beta)^2 = 1$. Furthermore, the group

$$G_{\epsilon,\eta} = \{\pm t(\alpha) \mid \alpha \in \mathrm{Aut}(E)\}$$

normalizes $\rho(E)$ and is an extension of $E = 2_\epsilon^{1+2n}$ by $O(Q) = O_{2n}^\epsilon(2)$.

https://doi.org/10.1017/S1446788700038271 Published online by Cambridge University Press

PROOF. Let

$$s(\alpha) = \sum_{x \in a + I(\alpha)} \lambda_x \rho(x, 0), \quad s(\beta) = \sum_{y \in b + I(\beta)} \mu_y \rho(y, 0)$$

$$\text{and} \quad s(\alpha\beta) = \sum_{z \in c + I(\alpha\beta)} \nu_z \rho(z, 0)$$

where by (4), $\lambda_x, \mu_y, \nu_z \in K_C$. If $z \in c + I(\alpha\beta)$, then equating the coefficient of $\rho(z, 0)$ in the equation $t(\alpha)t(\beta) = \tau(\alpha, \beta)t(\alpha\beta)$ gives

$$\theta^{-i(\alpha)-i(\beta)} \sum_{x+y=z} \lambda_x \mu_y (-1)^{f(x,y)} = \tau(\alpha, \beta)\theta^{-i(\alpha\beta)} \nu_z.$$

Hence to show that $\tau(\alpha, \beta) \in K_C$, it suffices to show that

$$\tau_z = \theta^{i(\alpha\beta)-i(\alpha)-i(\beta)} \sum_{x+y=z} \lambda_x \mu_y (-1)^{f(x,y)} \tag{8'}$$

is an element in K_C for some $z \in c + I(\alpha\beta)$. Let X be the set of inner automorphisms together with the α_v, $v \in N$. Then X generates $\mathrm{Aut}(E)$ if $E \ncong Q_8 \circ Q_8$, and $X \cup \{\beta'\}$ generates $\mathrm{Aut}(E)$ otherwise. As in Theorem 4, it suffices to show that $\tau(\alpha, \beta) \in K_C$ for all $\alpha \in A$ and β in some generating set for $\mathrm{Aut}(E)$.

If β is inner, then $g_\beta = 1$ so $I(\beta) = \{0\}$ and $i(\alpha\beta) - i(\alpha) - i(\beta) = 0$. Moreover, $\sigma(\alpha, \beta) \in K_C$ by Lemma 3(i). Suppose now that $\beta = \alpha_v$ and $v \notin I(\alpha)$, so $I(\alpha) \cap I(\beta) = \{0\}$. Since $O(Q)$ is a subgroup of $\mathrm{Sp}(B)$, $i(\alpha\beta) = i(\alpha) + 1$ by Lemma 2(a), so $i(\alpha\beta) - i(\alpha) - i(\beta) = 0$. Hence, in both cases $\tau_z \in K_C$.

We now consider case (c) of Lemma 2. Suppose that $\beta = \alpha_v$ where $Q(v) = 1$ and $v = u(1 + g_\alpha)$. Arguing as in Theorem 4, we may assume that $q_\alpha(K(\alpha)) = 0$ and hence by (4) that $\lambda_0 = 1$ and $\lambda_v = (-1)^{q_\alpha(u)+f(u,v)}$. Putting $z = 0$ in (8') gives

$$\tau_0 = \theta^{i(\alpha\beta)-i(\alpha)-i(\beta)} \left(\lambda_0\mu_0 + \lambda_v\mu_v(-1)^{f(v,v)}\right), \tag{9'}$$

where by (5'), $\mu_0 = 1$ and $\mu_v = 1$. By Lemma 2(c), we have $i(\alpha\beta) = i(\alpha) - 1$ and so $\tau_0 = \theta^{-2}(1 \pm 1)$. Therefore $\tau_0 = 0$ or $\eta 1$. However, τ_0 is non-zero, so it equals ± 1. This is sufficient to prove the theorem in the case when $E \ncong Q_8 \circ Q_8$. If $E \cong Q_8 \circ Q_8$, then our proof constructs an extension of 2_+^{1+4} by $\Omega_4^+(2)$ rather than an extension of 2_+^{1+4} by the full orthogonal group $O_4^+(2)$.

To complete the proof, it suffices to show that $\tau(\alpha, \beta') = \pm 1$ for all α in this subgroup of index 2 where β' is the automorphism described before this proof. Applying (4) to the automorphism $\beta' = (0, h')$ gives

$$s(\beta') = \rho(0, 0) - \rho(e_1 + e_3, 0) - \rho(e_2 + e_4, 0) - \rho(e_1 + e_2 + e_3 + e_4, 0).$$

The restriction of f to $I(\beta') = \langle e_1 + e_3, e_2 + e_4 \rangle$ is zero. Hence, in particular, $I(\beta')$ is totally singular and $s(\beta')^2 = 4\rho(0, 0)$. Therefore both β' and $t(\beta') =$

https://doi.org/10.1017/S1446788700038271 Published online by Cambridge University Press

$\theta^{-2}s(\beta') = \eta s(\beta')/2$ are involutions. To complete our proof, it suffices to show that $t(\beta')^{-1}t(\alpha)t(\beta') = t(\beta'^{-1}\alpha\beta')$ for all $\alpha \in \langle X\rangle$. Equivalently, we may show that $s(\beta')^{-1}s(\alpha)s(\beta') = s(\beta'^{-1}\alpha\beta')$ where $\alpha \in X$. If α is inner, then $I(\alpha) = \{0\}$, and if $\alpha = \alpha_v$ for some $v \in N$, then $I(\alpha) \cap I(\beta') = \{0\}$ as $I(\beta')$ is totally singular and v is non-singular. The result follows in either case by Lemma 3(ii).

5. Properties of G and $G_{\epsilon,\eta}$

The groups G and $G_{\epsilon,\eta}$ in Theorem 4 and 4′ were constructed from a representation ρ, and so their isomorphism type could conceivably depend on the associated field K. The notation $G(K)$ and $G_{\epsilon,\eta}(K)$ takes into account the possible dependence on K.

THEOREM 5. *The isomorphism type of $G_{\epsilon,\eta}$ is independent of the field K but depends on both ϵ and η.*

PROOF. Now $E = 2_{\epsilon}^{1+2n}$ is a characteristic subgroup of $G_{\epsilon,\eta}(K)$. (If $n = 1$, and $E \cong D_8$, then E is the subgroup generated by all the elements of order 2; otherwise $E = O_2(G_{\epsilon,\eta}(K))$.) Since $2_{+}^{1+2n} \ncong 2_{-}^{1+2n}$, the isomorphism type of $G_{\epsilon,\eta}(K)$ depends on ϵ.

We show that the isomorphism type of $G_{\epsilon,\eta}(K)$ is independent of K by showing the value of $\tau(\alpha, \beta)(= \pm 1)$ is independent of K. Now $\tau(\alpha, \beta)$ satisfies the linear equation

$$\nu_z\tau(\alpha, \beta) = \theta^{i(\alpha\beta)-i(\alpha)-i(\beta)} \sum_{x+y=z} \lambda_x\mu_y(-1)^{f(x,y)}. \tag{10}$$

Since $i(\alpha\beta) - i(\alpha) - i(\beta)$ is even, and $\theta^2 = \eta 2$, (10) may be viewed as an integer equation. If K and K' have characteristic zero, then the solution for $\tau(\alpha, \beta)$ is independent of the field. If K and K' have odd characteristic p, then reading (10) modulo p shows that the value of $\tau(\alpha, \beta)$ is independent of the field.

We now show that $G_{\epsilon,+} \ncong G_{\epsilon,-}$. Suppose that $\phi \in \mathrm{Aut}(G_{\epsilon,\eta})$ and ϕ maps $t(\alpha)$ to $\pm t(\beta)$. Since E is characteristic, so is its centre Z, and ϕ maps $[t(\alpha), E]\,Z/Z$ to $[\pm t(\beta), E]\,Z/Z$. This show $i(\alpha) = i(\beta)$. Now -1 generates Z and so is fixed by every automorphism. Thus the sets

$$A_{\epsilon,\eta} = \left\{\pm t(\alpha) \in G_{\epsilon,\eta} \mid t(\alpha)^2 = -1 \quad \text{and} \quad i(\alpha) = 1\right\}$$

are characteristic. We will show that $A_{\epsilon,+}$ and $A_{\epsilon,-}$ have different cardinalities and so $G_{\epsilon,+} \ncong G_{\epsilon,-}$. By Theorem 4′, elements of these sets have the form $s = \theta^{-1}(\lambda_x\rho(x, 0) + \lambda_y\rho(y, 0))$ where $x \neq y$. Since

$$s^2 = \frac{\eta}{2}\Big\{\left[(-1)^{f(x,x)} + (-1)^{f(y,y)}\right]\rho(0, 0) + \lambda_x\lambda_y\left[(-1)^{f(x,y)} + (-1)^{f(y,x)}\right]\rho(x + y, 0)\Big\},$$

https://doi.org/10.1017/S1446788700038271 Published online by Cambridge University Press

we see that $s \in A_{\epsilon,+}$ if and only if

$$f(x,x) = f(y,y) = 1 \text{ and } B(x,y) = f(x,y) + f(y,x) = 1 \tag{11}$$

and $s \in A_{\epsilon,-}$ if and only if

$$f(x,x) = f(y,y) = 0 \quad \text{and} \quad B(x,y) = f(x,y) + f(y,x) = 1. \tag{12}$$

In either case, $Q(x+y) = Q(x) + Q(y) + B(x,y) = 1$.

Let $S = \{x \in V \mid Q(x) = 0\}$ and $N = \{x \in V \mid Q(x) = 1\}$. Given subsets X, Y and Z of V, define $\{X, Y; Z\}$ to be the set $\{(x,y) \in X \times Y \mid x + y \in Z\}$. It follows from (11) and (12) that $|A_{\epsilon,+}| = 4\,|\{N, N; N\}|$ and $|A_{\epsilon,-}| = 4\,|\{S, S; N\}|$. Let v, s and n denote the number of elements in V, S and N respectively. Then $v = s + n$. If $x \neq 0$ is fixed, then the equation $B(x,y) = 1$ has $v/2$ solutions for y. Thus the set

$$\{(x,y) \in N \times V \mid B(x,y) = 1\}$$

has $nv/2$ elements and is a disjoint union of $\{N, S; S\}$ and $\{N, N; N\}$. Since $0 \in S$, a similar argument shows that the set $\{(x,y) \in V \times S \mid B(x,y) = 1\}$ has cardinality $v(s-1)/2$ and is a disjoint union of $\{N, S; S\}$ and $\{S, S; N\}$. Subtracting the equation $|\{N, S; S\}| + |\{S, S; N\}| = v(s-1)/2$ from $|\{N, S; S\}| + |\{N, N; N\}| = vn/2$ gives

$$|\{N, N; N\}| - |\{S, S; N\}| = v(n - s + 1)/2 = v(v - 2s + 1)/2.$$

Since $v - 2s + 1$ is an odd integer, this difference is non-zero. Hence $A_{\epsilon,+}$ and $A_{\epsilon,-}$ have different cardinalities and so $G_{\epsilon,+} \ncong G_{\epsilon,-}$.

THEOREM 6. *If $t(\alpha) \in G_{\epsilon,\eta}$ then*

$$\operatorname{trace}(t(\alpha)) = \begin{cases} \eta^n \theta^{k(\alpha)} & \text{if } q_\alpha(K(\alpha)) = 0, \\ 0 & \text{otherwise.} \end{cases}$$

If $t(\alpha) \in G$ then

$$\operatorname{trace}(t(\alpha)) = \begin{cases} (-i)^n (1+i)^{k(\alpha)} & \text{if } q_\alpha(K(\alpha)) = 0, \\ 0 & \text{otherwise.} \end{cases}$$

PROOF. As ρ is a tensor product of n two-dimensional representations of D_8 or Q_8, it follows that

$$\operatorname{trace}(\rho(x,0)) = \begin{cases} 2^n & \text{if } q_\alpha(K(\alpha)) = 0, \\ 0 & \text{otherwise.} \end{cases}$$

It follows from (4) and (4′) that $\rho(0,0)$ is a summand of $t(\alpha)$ if and only if $q_\alpha(K(\alpha)) = 0$. The proof now follows from the fact that $2n - i(\alpha) = k(\alpha)$.

https://doi.org/10.1017/S1446788700038271 Published online by Cambridge University Press

It is shown in [4, Section 2] that $\rho(E)$ preserves a non-degenerate symmetric form if $E \cong 2_+^{1+2n}$, and preserves a non-degenerate skew-symmetric form if $E \cong 2_-^{1+2n}$. The groups G and $G_{\epsilon,\eta}$ preserve this form up to a scalar multiple. (See [8] for a different approach.)

THEOREM 7. *If f' is a bilinear form preserved by $\rho(E)$, then $G_{\epsilon,+}$ preserves f', $G_{\epsilon,-}$ preserves f' up to a sign, and G preserves f' up to a multiple of a fourth root of* 1.

PROOF. First consider the groups $G_{\epsilon,\eta}$. Let J be the matrix of f' relative to some choice of basis for V. Then

$$\rho(x,\lambda)^t J \rho(x,\lambda) = J \quad \text{for all } (x,\lambda) \in E.$$

Let v be non-singular. Then $t(\alpha_v) = \theta^{-1}(\rho(0,0) + \rho(v,0))$ and

$$\rho(v,0)^t J = J\rho(v,0)^{-1} = -J\rho(v,0).$$

Hence

$$\begin{aligned} t(\alpha_v)^t J t(\alpha_v) &= \theta^{-2}\left[J + \rho(v,0)^t J + J\rho(v,0) + \rho(v,0)^t J \rho(v,0)\right] \\ &= \eta J \end{aligned}$$

as $2\theta^{-2} = \eta 1$. This proves our claim provided $E \ncong Q_8 \circ Q_8$. A straightforward calculation shows that

$$t(\beta')^t J t(\beta') = 4\theta^{-4} J = J.$$

Now consider the group G. Then

$$\rho(x,\lambda)^t J \rho(x,\lambda) = i^{2\lambda} J \quad \text{for all } (x,\lambda) \in H.$$

Since G is generated by $\rho(H)$ and the $(1+i)^{-1}s(\alpha_v)$, $v \in V$, the result follows from (5′) and the facts

$$(1+i)^{-1}\left[\rho(0,0) + i\rho(v,0)^t\right] J (1+i)^{-1}\left[\rho(0,0) + i\rho(v,0)\right] = J \text{ if } f(v,v) = 0,$$

and

$$(1+i)^{-1}\left[\rho(0,0) + i\rho(v,0)^t\right] J (1+i)^{-1}\left[\rho(0,0) + \rho(v,0)\right] = -iJ \text{ if } f(v,v) = 1.$$

References

[1] M. Aschbacher, 'On the maximal subgroups of the finite classical groups', *Invent. Math.* **76** (1984), 469–514.

https://doi.org/10.1017/S1446788700038271 Published online by Cambridge University Press

[2] J. Dieudonné, *Sur les groupes classique* (Hermann, Paris, 1948).
[3] P. Gérardin, 'Weil representations associated to finite fields', *J. Algebra* **46** (1977), 54–101.
[4] S. P. Glasby and R. B. Howlett, 'Extraspecial towers and Weil representations', *J. Algebra* **151** (1992), 236–260.
[5] D. Gorenstein, *Finite groups* (Chelsea, New York, 1980).
[6] R. L. Greiss, 'Automorphisms of extra special groups and nonvanishing degree 2 cohomology', *Pacific J. Math.* **48** (1973), 402–422.
[7] B. Huppert, *Endliche Gruppen I* (Springer, Berlin, 1967).
[8] P. Kleidman and M. Liebeck, *The subgroup structure of the finite classical groups*, London Mathematical Society Lecture Note Series 129 (Cambridge Univ. Press, Cambridge, 1990).
[9] I. Schur, 'Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen', *J. Reine Angew. Math.* **132** (1907), 85–137.
[10] M. Suzuki, *Group Theory II* (Springer, New York, 1986).
[11] D. E. Taylor, *The geometry of the classical groups*, (Helderman, Berlin, 1992).
[12] H. N. Ward, 'Representations of symplectic groups', *J. Algebra* **20** (1974), 182–195.

School of Mathematics and Statistics
The University of Sydney
NSW 2006
AUSTRALIA