PACIFIC JOURNAL OF MATHEMATICS
Vol. 48, No. 2, 1973

# AUTOMORPHISMS OF EXTRA SPECIAL GROUPS AND NONVANISHING DEGREE 2 COHOMOLOGY

ROBERT L. GRIESS, JR.

**If $E$ is an extra-special 2-group, it is known that Aut$(E)/$Inn$(E)$ is isomorphic to an orthogonal group. We prove that this extension is nonsplit, except in small cases. As a consequence, the nonvanishing of the second cohomology groups of certain classical groups (defined over $F_2$) on their standard modules may be inferred. Also, a criterion for a subgroup of these orthogonal groups to have a nonsplit extension over the standard module is given.**

1. Introduction. Let $E$ be an extra-special 2-group of order $2^{2n+1}$, $n \geqq 1$. That is, $E' = Z(E)$ and $E/E'$ is elementary abelian. Any extra-special group may be expressed as a central product of dihedral groups $D_8$ of order 8 and quaternion groups $Q_8$ of order 8, with the central subgroup of order 2 in each factor amalgamated. The expression of $E$ as such a central product is not unique in general because $D_8 \circ D_8 \cong Q_8 \circ Q_8$. However, the number of quaternion central factors is unique modulo 2 for any such expression (see [9] or [12]).

The commutator quotient $E/E'$ may be regarded as a vector space over the field of two elements $F_2$ equipped with a quadratic form $q$, where $q(xE') = x^2 \in E'$, for $x \in E$ (we identify $E'$ with the additive group of $F_2$). The bilinear form $b$ associated with $q$ is defined by $b(xE', yE') = q(xE')q(yE')q(xyE')$ (in multiplicative notation, and, in fact $b(xE', yE') = x^{-1}y^{-1}xy = [x, y]$ is the commutator of $x$ and $y$. Clearly, any automorphism of $E$ induces an automorphism of $E/E'$ which preserves this quadratic form. Hence, as Inn$(E)$ consider with the group of central automorphisms of $E$, Aut$(E)/$Inn$(E)$ is isomorphic with a subgroup of some orthogonal group $0^{\pm}(2n, 2)$.

On the other hand, it is not difficult to see that of the full orthogonal group may be lifted to automorphisms of $E$ ([12], 13.9). However, as we shall prove, there is usually no subgroup of Aut$(E)$, (Aut$(E)'$) isomorphic to the relevant (simple) orthogonal group complementing Inn$(E)$. For the case $|E| \geqq 2^9$, the argument is surprisingly easy, and gives a criterion for a subgroups of $0^{\varepsilon}(2n, 2)$ to have a nonsplit extension over the standard $2n$-dimensional module.

With similar considerations, one can see that, if $E$ is an extra-special 2-group of order $2^{2n+1}$, $Y \cong Z_4$, the group $E \circ Y$ (with a group of order two amalgamated) has $Z_2 \times \mathrm{Sp}(2n, 2)$ as the outer automorphism group (the isomorphism $D_8 \circ Z_4 \cong Q_8 \circ Z_4$ is useful here; [12],

p. 361).

We argue as follows. Since $Y = Z(E \circ Y)$, $Y$ is characteristic in $E \circ Y$. There is an automorphism $\alpha$ of $E \circ Y$ which inverts $Y$ and centralizes $E$. Thus, $B$, the centralizer of $Y$ in $\mathrm{Aut}(E \circ Y)$ has index 2 in $\mathrm{Aut}(E \circ Y)$. Now $\mathrm{Inn}(E \circ Y)$ has order $|E/E'| = 2^{2n}$. Also, $\mathrm{Inn}(E \circ Y) \subseteqq M$, the group of central automorphisms, and $|M| = |\mathrm{Hom}((E \circ Y), Y)| = 2^{2n+1}$. It follows that $M = \mathrm{Inn}(E \circ Y) \times \langle \alpha \rangle$. Note, $B \cap M = \mathrm{Inn}(E \circ Y)$.

Since $B$ preserves the alternating form $E \circ Y/Y \times E \circ Y/Y \rightarrow E'$ induced by commutation, $B/\mathrm{Inn}(E \circ Y)$ is isomorphic to a subgroup of $\mathrm{Sp}(2n, 2)$. To get $B/\mathrm{Inn}(E \circ Y) \cong \mathrm{Sp}(2n, 2)$, we must show that every symplectic transformation on $E \circ Y/Y$ can be lifted to $E \circ Y$. But, a variation of the argument of [12] showing $\mathrm{Out}(E)$ is isomorphic to the full orthogonal group can easily be made. The relevant fact is that every coset of $Y$ in $E$ contains involutions and elements of order 4.

So, we have $\langle B, \alpha \rangle = \mathrm{Aut}(E \circ Y)$. But clearly $\langle B, \alpha \rangle/\mathrm{Inn}(E \circ Y) \cong Z_2 \times \mathrm{Sp}(2n, 2)$ because $\langle \alpha \rangle$ covers $M/\mathrm{Inn}(E \circ Y) \lhd \mathrm{Out}(E \circ Y)$ and we already know $B$ is normal in $\mathrm{Out}(E \circ Y)$.

By the well-known connection between equivalence classes of group extensions and elements of the relevant second cohomology group [13], our results on automorphism groups may be viewed as statements about nonvanishing cohomology. Some related results are presented as well (Theorems 2, 3, 4, 5). Unfortunately, our methods do not indicate how big these nonzero cohomology groups are.

The corresponding question about extra-special $p$-groups leads to split extensions. More precisely, if $E$ is isomorphic to an extra-special $p$-group of order $p^{2n+1}$, $n \geqq 1$, $p$ an odd prime, then

(i) if $E$ has exponent $p$, $\mathrm{Out}(E) \cong \mathrm{Sp}(2n, p)H$, where $H$ is cyclic of order $p - 1$ and $H$ effects an outer automorphism of order 2 on $\mathrm{Sp}(2n, p)$.

(ii) If $E$ has exponent $p^2$, $\mathrm{Out}(E) \cong WSD$, where $W$ is a normal extra-special group of order $p^{2n-1}$, exponent $p$, $S \cong \mathrm{Out}(W)' \cong \mathrm{Sp}(2n - 2, p)$, and $D \cong Z_{p-1}$.

In either case, $\mathrm{Aut}(E)$ is a split extension of $\mathrm{Out}(E)$ by $\mathrm{Inn}(E)$. The splitting in (i) follows from an argument as in [12], p. 124. Case (ii) is technically more complicated. The details are omitted.

The author thanks J. McLaughlin for many helpful conversations and, particularly, for contributing Theorem 3. The author also thanks J. G. Thompson for pointing out that the centralizer of an involution in Conway's group·1, [4] is a nonsplit extension of an extra-special group of order $2^9$ by the simple orthogonal group $\Omega^+(8, 2) \cong D_4(2)$, and for raising the general question which led to Theorem 1.

**2. Notation and assumed results.** Most group-theoretic notation used is fairly standard (see [9] or [12]). In particular, $\sum_n$, resp. $A_n$ denotes the symmetric, resp. alternating group of degree $n$; $\mathrm{Sp}(2n, 2)$ denotes the symplectic group of dimension $2n$ defined over the field of 2 elements; $0^+(2n, 2)$, resp. $0^-(2n, 2)$, denotes the orthogonal group of dimension $2n$ defined over the field of 2 elements stabilizing a quadratic form of index $n$, resp. $n - 1$ (i.e., for which there is a maximal isotropic subspace of dimension $n$, resp. $n - 1$); $\Omega^+(2n, 2)$, resp. $\Omega^-(2n, 2)$ denotes the subgroup of index 2 in $0^+(2n, 2)$, resp. $0^-(2n, 2)$, for which Dickson invariant is zero ([6], p. 64)-it is the commutator subgroup of the orthogonal group, except for $\Omega^+(4, 2)$, and excluding $\Omega^+(4,2)$, it is generated by products of two orthogonal transvections ([6], p. 36) (here, we are differing slightly from common practice in which $\Omega^\pm(2n, 2)$ is defined to be $0^\pm(2n, 2)'$).

We assume the reader is familiar with elementary properties of symplectic and orthogonal groups in characteristic 2 [6]. To get subgroup structure, it is often useful to use the isomorphisms of these groups with groups of Lie type [3]:

$$\Omega^+(2n, 2) \cong D_n(2) \qquad \Omega^-(2n, 2) \cong {}^2D_n(2)$$
$$\mathrm{Sp}(2n, 2) \cong B_n(2) \cong C_n(2) , \quad \text{for} \quad n \geqq 2 .$$

We collect some of our most often used results below.

PROPOSITION 0. (i) *For $n \geqq 2$, $\Omega^\pm(2n, 2)$ is simple, except for $\Omega^+(4, 2) \cong SL(2, 2) \times SL(2, 2)$.*

(ii) *For $n \geqq 3$, $\mathrm{Sp}(2n, 2)$ is simple, and $\mathrm{Sp}(4, 2) \cong \sum_6$.*

(iii) *For $n \geqq 2$, $\Omega^\pm(2n, 2)$ acts transitively on nonsingular vectors and on nonzero singular vectors.*

(iv) *For $n \geqq 3$, the stabilizer in $\Omega^\pm(2n, 2)$ of a nonsingular vector is isomorphic to $0(2n - 1, 2) \cong \mathrm{Sp}(2n - 2, 2)$.*

(v) *For $n \geqq 3$, the stabilizer $S$ in $\Omega^\pm(2n, 2)$ of a nonzero singular vector is a split extension of $0_2(S)$, elementary abelian of order $2^{2n-2}$, by $S/0_2(S) \cong \Omega^\pm(2n - 2, 2)$.*

We present notation used in Theorem 1. We set

$$E_1 \cong D_8$$
$$E_{n+1} = E_n \circ F_n,\ n = 1, 2, \cdots \quad \text{where} \quad F_n \cong D_8$$
$$V_n = E_n/\langle e\rangle \quad \text{where} \quad \langle e\rangle = E'_n$$

and, in the obvious way, we regard

$$E_1 \subset E_2 \subset \cdots \subset E_n$$
$$V_1 \subset V_2 \subset \cdots \subset V_n .$$

We call $E_n$ an extra-special group of *positive type*, order $2^{2n+1}$. The other isomorphism type, the *negative type*, of extra-special group of order $2^{2n+1}$ is denoted by $T_n$. We have

$$\begin{aligned} &T_1 \cong Q_8 \\ &T_{n+1} \cong T_1 \circ E_n \cong T_n \circ E_1 , \qquad \text{for} \quad n \geqq 1 . \end{aligned}$$

We use the bar convention for image under $E_n \rightarrow V_n$ and for other homomorphic image when specified. We use $*$ to denote preimages. All our central products will have amalgamated central subgroup of order 2.

Some general references for cohomology of groups are [1], [11], [12], and [14].

## 3. Statement of results.

We momentarily identify the two groups $\mathrm{Out}\,(E)$ and $0^{\varepsilon}(2n, 2)$.

$$\mathrm{Out}\,(E) \cong 0^{\varepsilon}(2n, 2) .$$

Also, we identify $E/E'$ with $\mathrm{Inn}\,(E)$, thus making $\mathrm{Inn}\,(E)$ the standard module for $\mathrm{Out}\,(E)$. Let $G$ be a subgroup of $\mathrm{Out}\,(E)$. Consider (*), the extension of $G$ by $\mathrm{Inn}\,(E)$ induced by $\mathrm{Aut}\,(E)$:

$$\begin{tikzcd} & 1 \arrow[r] & \mathrm{Inn}\,(E) \arrow[r] & \mathrm{Aut}\,(E) \arrow[r] & \mathrm{Out}\,(E) \arrow[r] & 1 \\ (*) & 1 \arrow[r] & \mathrm{Inn}\,(E) \arrow[r] \arrow[u, "="'] & B \arrow[r] \arrow[u, hook] & G \arrow[r] \arrow[u, hook] & 1 . \end{tikzcd}$$

THEOREM 0. *Let $W$ be a subspace of* $\mathrm{Inn}\,(E)$, $|W| = 4$, *so that the nontrivial elements of $W$ consists of two singular vectors $x, y$ and one nonsingular vector $z$. Suppose $G$ has a subgroup $K$ satisfying*

(a) *$K$ fixes the vector $z$*:

(b) *$K$ contains an involution $t$ with $x^t = y$, $y^t = x$, $z^t = z$*:

(c) *$K$ has no subgroup of index* 2.

*Then,* (*) *is a nonsplit extension.*

THEOREM 1. *Let $E$ be an extra-special group of order $2^{2n+1}$, $n \geqq 1$. We identify* $\mathrm{Out}\,(E)$ *with the relevant orthogonal group* $0^{\varepsilon}(2n, 2)$, $\varepsilon = \pm$. *Consider the exact sequences of groups*

$$(*) \quad 1 \longrightarrow \mathrm{Inn}\,(E) \longrightarrow \mathrm{Aut}\,(E) \xrightarrow{\pi} 0^{\varepsilon}(2n, 2) \longrightarrow 1 ,$$

$$1 \longrightarrow \mathrm{Inn}\,(E) \longrightarrow A(E) \xrightarrow{\pi} \Omega^{\varepsilon}(2n, 2) \longrightarrow 1 ,$$

*where $A(E)$ is the preimage of $\Omega^{\varepsilon}(2n, 2)$ in* $\mathrm{Aut}\,(E)$ *under $\pi$.*

(a) *If $E$ is of positive type, the sequences of* (*) *are nonsplit* *when* $n \geqq 3$, *split when* $n = 1, 2$.

(b) *If* $E$ *is of negative type, the sequences of* (*) *are nonsplit when* $n \geqq 3$, *split when* $n = 1, 2$.

COROLLARY 1. *The second cohomology groups* $H^2(0^{\pm}(2n, 2), V)$ *and* $H^2(\Omega^{\pm}(2n, 2), V)$ *are nonzero for* $n \geqq 3$, *where* $V$ *is the usual* $2n$*-dimensional space on which* $0^{\pm}(2n, 2)$ *acts. Also,* $H^2(0^{+}(4, 2), V) = 0$ *and* $H^2(\Omega^{+}(4, 2), V) = 0$.

COROLLARY 2. *Let* $E$ *be an extra-special group of order* $2^{2n+1}$ *and let* $Y$ *be cyclic of order* 4. *Then* $\mathrm{Out}\,(E \circ Y) \cong Z_2 \times \mathrm{Sp}\,(2n, 2)$. *The extensions*

$$1 \longrightarrow \mathrm{Inn}\,(E \circ Y) \longrightarrow \mathrm{Aut}\,(E \circ Y) \xrightarrow{\pi} Z_2 \times \mathrm{Sp}\,(2n, 2) \longrightarrow 1\,,$$
$$1 \longrightarrow \mathrm{Inn}\,(E \circ Y) \longrightarrow A(E \circ Y) \xrightarrow{\pi} \mathrm{Sp}\,(2n, 2) \longrightarrow 1\,,$$

*where* $A(E \circ Y)$ *is the centralizer in* $\mathrm{Aut}\,(E \circ Y)$ *of* $Y$, *are nonsplit for* $n \geqq 3$. *Consequently, the second cohomology group* $H^2(\mathrm{Sp}\,(2n, 2), V)$ *is nonzero for* $n \geqq 3$, *where* $V$ *is the standard* $2n$*-dimensional module for* $\mathrm{Sp}\,(2n, 2)$.

THEOREM 2.

$$H^2(0^{-}(4, 2), V) = 0$$

*and*

$$H^2(\Omega^{-}(4, 2), V) = 0\,,$$

*where* $V$ *is the usual* 4*-dimensional module on which* $0^{-}(4, 2)$ *acts.*

THEOREM 3. (J. McLaughlin) $H^2(\mathrm{Sp}\,(4, 2), V) \neq 0$, *where* $V$ *is the usual* 4*-dimensional module. More precisely, the cup-product*

$$H^1(\mathrm{Sp}\,(4, 2), Z_2) \times H^1(\mathrm{Sp}\,(4, 2), V) \longrightarrow H^2(\mathrm{Sp}\,(4, 2), V)$$

*is not the zero pairing.*

THEOREM 4. $H^2(\mathrm{Sp}\,(4, 2)', V) = 0$, $V$ *the standard module.*

THEOREM 5. (a) *Let* $E$ *be an extra-special group of order* $2^{2n+1}$, $n \geqq 1$, *type* $\varepsilon = \pm$. *There is a group* $H$ *having the properties*

$$0_2(H) \cong E,\ Z(H) = Z(0_2(H))$$
$$H/0_2(H) \cong 0^{\varepsilon}(2n, 2),\quad H/Z(H) \cong \mathrm{Aut}\,(E)$$

*and* $H$ *has a faithful, ordinary, irreducible complex representation of degree* $2^n$.

(b) *Let $E$ be as above and let $Y \cong Z_4$. There is a group $H_0$ having the properties*

$$0_2(H_0) \cong E \circ Y, \quad Z(H_0) = Z(E)$$
$$H_0/0_2(H_0) \cong \mathrm{Sp}\,(2n, 2), \quad H_0/Z(H_0) \cong A(E \circ Y)$$

*and $H_0$ has two faithful, ordinary irreducible complex representations of degree $2^n$. These are interchanged by the action of* Aut $(E \circ Y)$ *on $A(E \circ Y)$ and by complex conjugation.*

(c) *Let $F$ be a splitting field for $E$ or $E \circ Z_4$ (e.g. $F = \boldsymbol{Q}$, the rationals, will do for $E_n$, and $\boldsymbol{Q}(\sqrt{-1})$ will do for $T_n$ or $E \circ Z_4$).*

(i) *If $W = H$ or $H_0$, then the $2^n$-dimensional representation, when restricted to $W'$, may be written in $F$.*

(ii) *If $W_0 = H, H'E, H_0$ or $H_0'E$ then every faithful irreducible character of $\chi$ of $W_0$ has the form $\chi = \xi\eta$, where $E$ is contained in the kernel of $\xi$ and $\eta$ is the character of a $2^n$-dimensional representation from* (a) *if $W_0 = H$ or $H'E$, or from* (b) *if $W_0 = H_0$ or $H_0'E$.*

COROLLARY 3. *The exact sequences of Corollary* 2 *are nonsplit for $n = 2$.*

Note that Corollary 3 implies the first assertion of Theorem 3.

4. *Proof of Theorem* 0, *and for $n \geqq 4$, proof of Theorem* 1 (a), (b), *and Corollary* 1. Assume the hypotheses of Theorem 0. Let $W^*$ be the preimage of $W$ in $E$. Then $W^* \cong D_8$. Assume (*) is split. Then, there is a complement to Inn $(E)$ in $B$, which we may as well identify with $G$. Now, $t \in G$ effects an outer automorphism of order 2 on $W^*$. The structure of Aut $(W^*)$ implies that $t$ inverts the maximal cyclic subgroup $U$ of $W^*$. But $K$ acts on $U$, and since $K$ has no subgroup of index 2, $K$ must centralize $U$. This gives a contradiction, since $t \in K$. Therefore, the complement does not exist, and the Theorem is proven.

We can now get the assertions of Theorem 1 (a), (b) and Corollary 1, for $n \geqq 4$. Let $G = \mathrm{Out}\,(E)$ or $\mathrm{Out}\,(E)'$. Choose any $W$ as in the Theorem and let $K$ be the stabilizer of the nonsingular vector in $\mathrm{Out}\,(E)'$; we have $K \cong 0(2n-1, 2) \cong \mathrm{Sp}\,(2n-2, 2)$. Since $n \geqq 4$, $K$ is simple. One can easily find an involution $t$ with the required properties. Theorem 0 now implies the assertions of Theorem 1, and Corollary 1 as well.

If $n = 3$, the arguments are different and will be given in §§5 and 13. Here $K \cong \sum_6$, the symmetric group. The trouble is, since $|K: K'| = 2$, we are not immediately led to a contradiction, for $t$ may not lie in $K'$.

EXAMPLE. It may be easy to check the hypotheses of the Theorem in some cases. Let $G$ be Conway's group 1. Let $\Lambda$ be the Leech lattice, and set $V = \Lambda/2\Lambda$. The quadratic form on $\Lambda$ induces an $\boldsymbol{F}_2$-valued quadratic form on $V$ which is nondegenerate. Also, $G$ preserves the form on $V$. Consider a triangle in $\Lambda$ of type 322. We take for $W$ the union of $0 \in V$ and the image in $V$ of the edges of this triangle. Let $K^*$ be the stabilizer in .0 of the subgroup of $\Lambda$ generated by the edge of type 3; $K^* \cong .3 \times Z(.0)$. Let $K$ be the image of $K^*$ in $G$. It is not difficult to find an involution $t^*$ of .0 which switches the two edges of type 2 in our triangle. Finally, set $t$ equal to the image of $t^*$ in $G$. Since $K$ is simple, all parts of the hypothesis of our Theorem are satisfied. It follows that there is a nonsplit extension of $G$ by $V$ (we have embedded in $G$ in Out $(E)$, $E$ extra special of order $2^{25}$, and identified $V$ with $E/E'$ to get this). Of course, we also get $H^2(.1, \Lambda/2\Lambda) \neq 0$.

## 5. *Proof of Theorem* 1 (b), *Corollary* 1, *the case* $n = 3$.

It suffices to show that

$$1 \longrightarrow \mathrm{Inn}\,(T_3) \longrightarrow \mathrm{Aut}\,(T_3)' \longrightarrow \mathrm{Out}\,(T_3)' \longrightarrow 1$$

is a nonsplit extension. In this case, Out $(T_3)' \cong \Omega^-(6, 2) \cong U_4(2)$.

We assume the extension splits. The considerations of §4 allow us to assume the following: there is a coset $x\langle e\rangle$ of $\langle e\rangle = T_3'$ with $x^2 = e$ and $x^d = xe$ for $d \in K - K'$, where $K \cong \sum_6$ is the stabilizer of $x\langle e\rangle$ in the complement. We may write $T_3 = T_1 \circ F$, where $x \in F \cong E_2$. There is an automorphism $\alpha$ of order 3 which centralizes $F$ and acts nontrivially on $T_1 \cong Q_8$. Let $Q$ be the subgroup of $K'$ which is congruent to $\langle\alpha\rangle$ modulo Inn $(T_3)$. Any subgroup of order 3 in $K \cong \sum_6$ is centralized by some $d \in K\backslash K'$. Thus $\langle Q, d\rangle \cong \boldsymbol{Z}_6$ acts on $T_1 = [T_3, Q]$. But Aut $(T_1) \cong \sum_4$ implies that $d$ centralizes $T_1$. So, choose $y \in T_1$, $|y| = 4$. Then $y^d = y$, whence $(xy)^d = xey = (xy)e$. But $xy = yx$ implies $xy$ is an involution. The stabilizer of the singular vector $xy\langle e\rangle$ in the complement is isomorphic to a perfect group which is an extension of $\Omega^-(4, 2) \cong A_5$ by an elementary abelian group of order $2^4$. Since this perfect group must centralize every element of the coset $xy\langle e\rangle$, we have a contradiction to $(xy)^d = xye$. Thus, the complement does not exist in the case $n = 3$ either.

## 6. *Proof of Theorem* 2.

LEMMA. *Let $V$ be the usual 4-dimensional $\boldsymbol{F}_2$-space on which $\Omega^-(4, 2)$ acts.*

Then $V$ is a projective and injective $F_2\Omega^-(4, 2)$-module. Consequently, $H^i(\Omega^-(4, 2), V) = 0$ for all $i \geqq 1$.

*Proof.* We claim that $V$ is absolutely irreducible. Let $k$ be a field of characteristic 2 containing the $|G|$th roots of unity, where $G = \Omega^-(4, 2)$. It is well-known that $kG$ has four irreducible modules of dimensions 1, 2, 2, and 4. It suffices to show that $k \otimes V$ has no 1-or 2-dimensional constituent. If there were a 1-dimensional constituent, an element of order 5 in $G$ would have 1 as an eigenvalue on $k \otimes V$, hence also on $V$. This is impossible as $|V| = 16$. Assume no trivial constituent occurs and suppose the 2-dimensional modules are the constituents. But on each of these, an element of order 3 in $G$ has no fixed points, although it stabilizes both singular and nonsingular vectors of $V$, contradiction.

Thus, $V$ is absolutely irreducible. Since $k \otimes V$ has dimension 4, the full 2-part of the order of $G$, $k \otimes V$ lies in a block of defect 0 (see [2], especially (6A)), hence is projective and injective for $kG$. As $V$ is an $F_2G$-summand of $k \otimes V$, $V$ is projective and injective.

Since cohomology vanishes on injectives in positive degree (see [11] or [14]), the last assertion is immediate. The lemma is proven.

Now consider an extension

$$(+)1 \longrightarrow V \longrightarrow E \longrightarrow 0^-(4, 2) \longrightarrow 1$$

of $0^-(4, 2) \cong \sum_5$ by its usual 4-dimensional $F_2$-module. By the lemma, $(+)$ restricted to $\Omega^-(4, 2)$ is split because $H^2(\Omega^-(4, 2), V) = 0$. Furthermore, $H^1(\Omega^-(4, 2), V) = 0$ implies that all subgroups of $E$ isomorphic to $\Omega^-(4, 2)$ are conjugate.

We can now show $H^2(0^-(4, 2), V) = 0$ by applying the Frattini-like argument suggested in [12], page 124. Namely, let $D$ denote a subgroup of $E$ isomorphic to $\Omega^-(4, 2)$. Since all such $D$ are conjugate, $E = VN_E(D)$. Now, $N_E(D) \cap V = 1$ because $\Omega^-(4, 2)$ fixes no vector in $V^\#$. Thus $N_E(D)$ complements $V$ in $E$. Consequently,

$$H^2(0^-(4, 2), V) = 0 .$$

7. *Proof of Theorem* 1, *and Corollary* 1, *the case* $n = 1, 2$. Consider part (a). For $n = 1$ the result holds, as $\mathrm{Aut}\,(D_8) \cong D_8$. For $n = 2$, $\mathrm{Out}\,(E_2) \cong 0^+(4, 2)$ is isomorphic to a wreath product $\sum_3 \wr Z_2$. Now consider any extension

$$1 \longrightarrow \mathrm{Inn}\,(E_2) \longrightarrow B \longrightarrow 0^+(4, 2) \longrightarrow 1$$

with the same action as $\mathrm{Out}\,(E_2)$ on $\mathrm{Inn}\,(E_2)$. Let $P$ be a Sylow 3-subgroup of $B$; $P \subset 0_{2,3}(B)$. By the Frattini argument, $B = \mathrm{Inn}\,(E_2) \cdot N_B(P)$. But $P$ acting faithfully on $\mathrm{Inn}\,(E_2)$ may not have a nontrivial fixed point. Thus, $\operatorname{Inn}(E_2) \cap N_B(P) = C_{\operatorname{Inn}(E_2)}(P) = 1$. Thus, $N_B(P)$ complements $\operatorname{Inn}(E_2)$ in $B$, whence the extension is split. A similar argument shows that any extension of $\Omega^+(4, 2)$ by $\operatorname{Inn}(E_2)$ is split.

Next, consider part (b). For $n = 1$ the result holds, as $\operatorname{Aut}(Q_8) \cong \sum_4$ and $\sum_3 \subset \sum_4$ complements the normal four-group $\operatorname{Inn}(Q_8)$. For $n = 2$, $0^-(4, 2) \cong \sum_5$ and $\Omega^-(4, 2) \cong A_5$. The splitting in this case follows from Theorem 2.

The last assertion of Corollary 1 follows from the above.

8. *Proof of Corollary* 2. To prove Corollary 2, we choose $n \geqq 3$ and work for a contradiction under the assumption that

$$1 \longrightarrow \operatorname{Inn}(E \circ Y) \longrightarrow A(E \circ Y) \longrightarrow \operatorname{Sp}(2n, 2) \longrightarrow 1$$

is split. We claim that $D$, the subgroup of $A(E \circ Y)$ leaving invariant the subgroup $E \subset E \circ Y$ is isomorphic to $\operatorname{Aut}(E)$. Namely, any automorphism of $\operatorname{Aut}(E)$ can be extended to one of $E \circ Y$ by letting it act trivially on $Y$. Furthermore, every element in $D$ is of this form, for if $\alpha, \beta \in D$ induce the same automorphism on $E$, then $\alpha\beta^{-1}$ is trivial on $E$ and on $Y$, hence $\alpha\beta^{-1} = 1$. Clearly, $D \supset \operatorname{Inn}(E \circ Y)$, which may be regarded as $\operatorname{Inn}(E)$ under our identification. Our hypothesis implies that the extension of $D$ by $\operatorname{Inn}(E \circ Y)$ is split. But this contradicts Theorem 1. The corollary is proven.

9. *Proof of Theorem* 3. Let $k$ be a perfect field of characteristic 2, $V$ a finite dimensional vector space over $k$, and $b$ a nonsingular alternating form $V \times V \to k$. Let $G$ be the symplectic group associated with $b$. In this section, we write functions and group actions on the left.

Recall that a derivation (or, a 1-cocycle) from $G$ to $V$ is a function $d\colon G \to V$ satisfying $d(xy) = d(x) + xd(y)$, all $x, y \in G$. If $q$ is a quadratic form on $V$ whose associated bilinear form is $b$ there is a derivation $d\colon G \to V$, where $d(t)$ is defined by the condition

$$b(t(v), d(t)) = \sqrt{q(v) + q(t(v))}\,, \quad \text{for all} \quad v \in V\,.$$

Note that, for fixed $t$, the right side is a linear functional in $v$. Since $b$ is nonsingular, it identifies $V$ with its dual, whence a unique vector $d(t)$ is determined by the above condition.

We show that this $d$ is a derivation. Let $s, t \in G$. By definition of $d$, we have

$$\begin{aligned} b(st(v), d(st)) &= \sqrt{q(v) + q(st(v))}\,, \quad \text{all} \quad v \in V \\ b(s(v), d(s)) &= \sqrt{q(v) + q(s(v))}\,, \quad \text{all} \quad v \in V \\ b(t(v), d(t)) &= \sqrt{q(v) + q(t(v))}\,, \quad \text{all} \quad v \in V\,. \end{aligned}$$

In the second equation, replace the variable $v$ by $t(v)$, and in the third expression, replace $b(t(v), d(t))$ by $b(st(v), sd(t))$. Adding the three new equations, we get $b(st(v), d(st) + d(s) + sd(t)) = 0$ all $v \in V$, whence $d(st) + d(s) + sd(t) = 0$, as required. We shall see that in most cases, $d$ is not a coboundary.

For $x \in V$, $x \neq 0$, let $t_x$ be the transvection at $x$, i.e.,

$$t_x(v) = v + b(v, x)x .$$

Then,

$$\begin{aligned} q(v) + q(t_x(v)) &= q(v + t_x(v)) + b(v, t_x(v)) \\ &= q(b(v, x)x) + b(v, v) + b(v, b(v, x)x) \\ &= b(v, x)^2(1 + q(x)) , \end{aligned}$$

whence

$$d(t_x) = \sqrt{1 + q(x)}\, x .$$

If $d$ were a coboundary, there would be a fixed $m \in V$ with $d(t) = t(m) + m$, all $t \in G$. Assume $|k| > 2$ or $\dim(V) \geqq 4$. Suppose $0 \neq y \in V$, $q(y) = 0$. From above, $y = d(t_y) = t_y(m) + m = b(m, y)y$, whence $b(m, y) = 1$, for all such $y$. Now, suppose $q$ has isotropic subspaces of dimension $1/2 \dim(V)$. If $|k| > 2$, choose $c \in k$, $c \neq 0, 1$, and choose $y \neq 0$ with $q(y) = 0$. Then $q(cy) = 0$, but $b(m, cy) = cb(m, y) = c \neq 1$, contradiction. If $\dim(V) \geqq 4$, there are singular vectors $x, y$ with $q(x) = q(y) = q(x + y) = 0$. Then $b(m, x + y) = b(m, x) + b(m, y) = 1 + 1 = 0 \neq 1$, contradiction. Thus, we may assume by changing $q$ if necessary that $d$ is not a coboundary if $|k| > 2$ or $\dim(V) \geqq 4$.

Now, take $k = \boldsymbol{F}_2$, $V$ of dimension 4. Since $G \cong \sum_6$, we have a nontrivial homomorphism $h: G \to \boldsymbol{F}_2$. Define $f: G \times G \to V$ by

$$f(s, t) = h(t)d(s);\ s, t \in G .$$

We show that this 2-chain is a 2-cocycle. We calculate (in characteristic 2)

$$\begin{aligned} &f(s, t) + f(st, r) + sf(t, r) + f(s, tr) \\ &\quad = h(t)d(s) + h(r)d(st) + h(r)sd(t) + h(tr)d(s) \\ &\quad = h(t)d(s) + h(r)\{d(st) + sd(t)\} + \{h(t) + h(r)\}d(s) \\ &\quad = h(t)\{d(s) + d(s)\} + h(r)\{d(st) + sd(t) + d(s)\} = 0 , \end{aligned}$$

so that $f$ is a 2-cocycle.

We want to show that $f$ is not a 2-coboundary, from which $H^2(\mathrm{Sp}(4, 2), V) \neq 0$ will follow. Suppose there were a $g: G \to V$ so that $f(s, t) = g(st) + sg(t) + g(s)$. Note that $0 = h(1) \cdot d(1) = f(1, 1) = g(1) + g(1) + g(1)$ implies $g(1) = 0$.

Let $0 \neq x \in V$ have $q(x) = 0$. Then $d(t_x) = x$ from above. Also, $t_x \notin G'$, so $h(t_x) = 1$. So,

$$\begin{aligned} x = h(t_x)d(t_x) &= f(t_x, t_x) = g(1) + t_x g(t_x) + g(t_x) \\ &= (t_x + 1)g(t_x) = b(x, g(t_x))x . \end{aligned}$$

Thus, $b(x, g(t_x)) = 1$ and $g(t_x) \notin \langle x \rangle^{\perp}$ (where$^{\perp}$ denotes annihilator with respect to $b$).

Now, take $q$ to be a quadratic form for which there are isotropic subspaces of dimension 2. Let $x$, $y$ be distinct nonzero singular vectors with $b(x, y) = 0$. Then $t_x$ and $t_y$ commute. Now

$$d(t_x) = h(t_y)d(t_x) = g(t_x t_y) + t_x g(t_y) + g(t_x) .$$

We then get

$$\begin{aligned} d(t_x) + t_x g(t_y) + g(t_x) &= g(t_x t_y) = g(t_y t_x) \\ &= d(t_y) + t_y g(t_x) + g(t_y) , \end{aligned}$$

or

$$d(t_x) + (t_x + 1)g(t_y) = d(t_y) + (t_y + 1)g(t_x) ,$$

or

$$(1 + b(x, g(t_y))x = (1 + b(y, g(t_x))y .$$

Therefore, $b(y, g(t_x)) = 1$, since $x$ and $y$ are linearly independent.

Let $W$ be the span of $x$ and $g(t_x)$ in $V$. Then $W^{\perp} \subsetneqq \langle x \rangle^{\perp}$. But $x \notin W^{\perp}$ since $g(t_x) \in W$ and $g(t_x) \notin \langle x \rangle^{\perp}$. It follows easily that $W$ is nonsingular under $b$. Since $V$ has isotropic subspaces of dimension 2, there is a nonzero singular vector $y \in W^{\perp}$. But then $b(y, g(t_x)) = 0$ contradicts the last paragraph.

Therefore, $f$ is not a 2-coboundary, as required. McLaughlin remarks that the cocycle $d$ appeared in a different form in Dickson's work [7]. Now $H^1(\mathrm{Sp}\,(4, 2), V) \neq 0$ and $H^1(\mathrm{Sp}\,(4, 2), Z_2) \cong \mathrm{Hom}\,(\mathrm{Sp}\,(4, 2), Z_2) \cong Z_2$. Our definition of $f \in Z^2(\mathrm{Sp}\,(4, 2), V)$ as $f(s, t) = h(t)d(s)$ is a cup-product construction [1], based on the (obvious) pairing $Z_2 \otimes V \rightarrow V$. Note that the cocycle $f$ restricted to $G'$ is identically zero.

10. *Proof of Theorem* 4. We consider an arbitrary extension

$$(\neq) 1 \longrightarrow V \longrightarrow B \longrightarrow \mathrm{Sp}\,(4, 2)' \longrightarrow 1$$

of $\mathrm{Sp}\,(4, 2)' \cong A_6$ by $V$, the usual 4-dimensional $F_2$-vector space on which $\mathrm{Sp}\,(4, 2)$ acts. We will show $(\neq)$ is split.

We know by Theorem 2, that $(\neq)$ restricted to $\Omega^-(4, 2)$ is split. Let $D$ be a subgroup of $E$ mapping isomorphically onto $\Omega^-(4, 2) \subset$

$\mathrm{Sp}(4, 2)'$. Since $V$ is $F_2$ $D$-projective and injective. (By the Lemma in §6), $V$ is likewise for $F_2D_1$, $D_1$ any subgroup of $D$. If we take $|D_1| = 2$, and remark that all involutions of $\mathrm{Sp}(4, 2)'$ are conjugate, we get that $(\neq)$ is split when restricted to any subgroup of order 2 in $\mathrm{Sp}(4, 2)'$.

Let $I$ be a maximal isotropic subspace of $V$, $|I| = 4$. The stabilizer $K_1$ of $I$ in $\mathrm{Sp}(4, 2)'$ is isomorphic to $\sum_4$. Let $K$ be the preimage of $K_1$ in $B$, and let $R = 0_2(K)$. Note that a Sylow 3-subgroup $P$ of $K$ acts fixed point freely on $R$.

We claim $R/I$ is elementary abelian. Now, $P$ acts fixed point freely on $R/I$ also. Since $V/I$ is central in $R/I$, commutation is biadditive. Since $|R/V| = 2^2$, we have $|(R/I)| \leqq 2$. But since $(R/I)'$ is characteristic in $R/I$ and $P$ acts fixed point freely, $(R/I)' = 1$ follows. Thus, $R/I$ is abelian. As pointed out above, every coset of $V/I$ in $R/I$ contains involutions. Thus, $R/I$ is elementary abelian.

We have $P \subset 0_{2,3}(K)$ and $|K: 0_{2,3}(K)| = 2$. By the Frattini argument, we choose a 2-element $t \in N_K(P)$, $t \in 0_{2,3}(K)$. By the structure of $K_1$, $t^2 \in V$, so $t^2 \in C_V(P) = 1$. Thus $\langle P, t) \cong \sum_3$.

Since $V/I$ is an irreducible $\langle P, t\rangle$-module of dimension 2, the 2-part of $|\langle P, t\rangle|$, $V/I$ is projective and injective over $F_2\langle P, t\rangle$ ([2], (6A)). So take $W \subset 0_2(K)$ so that $W/I$ is a $F_2\langle P, t\rangle$-complement to $V/I$.

Since $I$ is central in $W$, we may repeat the above arguments to get $W$ elementary abelian and we may obtain an $F_2\langle P, t\rangle$ complement $T$ to $I$ in $W$. Clearly $\langle P, t, T\rangle$ intersects $V$ trivially and covers $K/V$.

Thus, $(\neq)$ splits when restricted to $K_1$. Since $|\mathrm{Sp}(4, 2)': K_1|$ is odd, Gaschütz' Theorem implies that $(\neq)$ is split. The theorem is proven.

11. *Proof of Theorem* 5. (a) Let $M = C[E]$ be the complex group algebra of $E$. It is well-known ([9], 5.5.4) that $E$ has precisely one faithful irreducible representation and it has dimension $2^n$. Let $N$ be the simple constituent of $M$ corresponding to this representation. Now, $\mathrm{Aut}(E)$ permutes the irreducible representations of $E$, but $N$ must be left invariant because it is the only faithful one. Thus, $\mathrm{Aut}(E)$ operates as automorphisms on the matrix algebra $N$. By the Skolem-Nöther Theorem, every automorphism of $N$ is inner. ([13], p. 24).

For $\alpha \in \mathrm{Aut}(E)$, let $m(\alpha) \in N$ induce the same automorphism of $N$ as $\alpha$. We have $m(\alpha)m(\beta) = m(\alpha\beta)c(\alpha, \beta)$, for $\alpha, \beta \in \mathrm{Aut}(E)$, where $c(\alpha, \beta)$ is a scalar matrix. Thus

$$\alpha \longmapsto m(\alpha)$$

gives a projective representation of $\mathrm{Aut}(E)$. Conjugation by elements of $E \subset M$ on $N$ has the same effect as the action of the $m(\alpha), \alpha \in \mathrm{Inn}(E)$. Since the representation $E \to N$ is irreducible and faithful, and not projectively equivalent to an ordinary representation of $E/E'$, $\alpha \mapsto m(\alpha)$ is not equivalent to an ordinary representation of $\mathrm{Aut}(E)$.

By Schur ([15] (1907) or [12], 24.3), there is a covering group $K$ of $\mathrm{Aut}(E)$, a subgroup $C \subseteqq Z(K) \cap K'$, and an isomorphism $\phi$ so that the diagram below commutes

$$\begin{tikzcd} K/C \arrow[r, "\phi"] \arrow[d] & GL(2^n, C) \arrow[d] \\ \mathrm{Aut}(E) \arrow[r, "m"] & PGL(2^n, C) . \end{tikzcd}$$

We shall show that, for $n \geqq 5$, $C = 1$ and that $K$ is our desired group $H$. Following this, the case $n \leqq 4$ will be treated.

Let $G = \mathrm{Aut}(E)$ and suppose $n \geqq 5$. Set $A = Z(K)$. Then, $A \subseteqq K'$ and $K/A \cong G$. Let $R = \mathrm{Inn}(E) \lhd G$, and let $\tilde{R}$ be the extension of $R$ induced by $K$. Set $B = A \cap \tilde{R}'$ and let $L = K/B$. Now, $0^{\varepsilon}(2n, 2)$ has trivial multiplier ([17] and preliminary result (11) of [10]). Also, $H^1(0^{\varepsilon}(2n, 2), V) = 0$ for $n \geqq 4$ and $V$ the standard module [16]. Since $V$ is self dual, this last fact implies that $\mathrm{Ext}(V, Z_2) \cong \mathrm{Ext}(Z_2, V) \cong H^1(0^{\varepsilon}(2n, 2), V) = 0$. All this, together with the irreducibility of $G/R$ on $R$, implies that $(A/B) \cap L' = 1$. Since $A \subseteqq K'$, we get $A = B$. Since the multiplier of an elementary abelian group is elementary abelian [12], $B$ is elementary. We wish to show $|B| = 2$.

Suppose $B_1$ is a hyperplane of $B$. Then the squaring map from $R/B_1$ into $B/B_1 \cong Z_2$ induces a quadratic form $q_1$ on $\tilde{R}/B \cong R$ which is preserved by $G/R$. Let $B_1$ and $B_2$ be distinct hyperplanes and $q_1$ and $q_2$ the associated forms. We claim that $q_1$ and $q_2$ are "distinct", i.e., that the following does not happen: for every $x \in R$, $q_1(x) = 1$ if and only if $q_2(x) = 1$. Namely, if the latter does hold, then the squares in $R$ generate a proper subgroup of $B$, contradiction. This shows that if $0^{\varepsilon}(2n, 2)$ preserves a unique quadratic form on $V$, then $|B| \leqq 2$ follows.

Suppose $q$ and $q'$ are quadratic forms with the same associated bilinear form $b$. Then, the groups which preserve $q$ and $q'$ are subgroups of the symplectic group associated with $b$, and they are equal if and only if $q = q'$ (as is well-known). So, to get $|B| \leqq 2$, it suffices to show that $0^{\varepsilon}(2n, 2)$ preserves a unique bilinear form, i.e., that $\dim_{F_2} \mathrm{Hom}_{0^{\varepsilon}(2n,2)}(V \otimes V, F_2) = 1$. But since $V$ is a self dual module, we have (dropping subscripts), $\mathrm{Hom}(V \otimes V, F_2) \cong \mathrm{Hom}(V, \mathrm{Hom}(V, F_2)) \cong \mathrm{Hom}(V, V)$, and the latter object has dimension 1, because (for $n \geqq 2$) $V$ is an absolutely irreducible module (as is easily proven, say, by induction on $n$; or see [18]).

We now have $|B| \leqq 2$. Since $Z(K) \neq 1$, this forces $C = 1$ and shows that the covering group $K = K(n, \varepsilon)$ has the properties required of $H$, for $n \geqq 5$, $\varepsilon = \pm$. We turn to the case $n \leqq 4$. Fix $K_0 = K(m, \delta)$, for $m \geqq 5$, and some sign $\delta$. Choose a nonsingular subspace $W$ of $R = \operatorname{Inn}(E)$, so that the annihilator in $R$ of $W$ has order $2^{2n}$, type $\varepsilon$. Let $\tilde{W}$ be the preimage of $W$ in $K_0$; $\tilde{W}$ is an extra-special group of type $\varepsilon\delta$. Let $J$ be the centralizer of $\tilde{W}$ in $K_0$. We have $J \cap \tilde{W} = Z(\tilde{R}) = Z(\tilde{W})$, $J\tilde{W} = \tilde{R}$, and $J$ induces the identity on $\tilde{W}$ and the full orthogonal group on $J \cap \tilde{R}/J \cap Z(\tilde{R})$. This suffices to show that we may take $J$ to be our $H$ for this pair $n, \varepsilon$.

For $n \geqq 5$, it is clear that $K(n, \varepsilon)$ has an irreducible, faithful complex representation of degree $2^n$. For $n \leqq 4$, we argue using the notation of the last paragraph. The representation of degree $2^m$, when restricted to $\tilde{W}$, is the direct sum of $2^n$ equivalent faithful irreducible representations of $\tilde{W}$, each of dimension $2^{m-n}$. Thus, $J = C_{K_0}(\tilde{W})$ acts in $2^n$ dimensions, and this action is easily seen to be faithful and irreducible.

(b) Every irreducible representation of $E \circ Y$ may be expressed as a product of such of $E$ and of $Y$. ([9], 3.7.1). Now, $E$ has precisely one irreducible faithful representation of dimension $2^n$, and $Y$ has two such, each of degree 1. Thus $E \circ Y$ has precisely two faithful irreducible representations, each of dimension $2^n$.

By imitating the argument of part (a), $A(E \circ Y)$ permutes the irreducible constituents of $\boldsymbol{C}[E \circ Y]$, hence permutes the two constituents $N_1, N_2$ corresponding to faithful representations. But since $A(E \circ Y)$ centralizes $Y$, it leaves each $N_i$ invariant. As in (a), this gives a projective representation of $A(E \circ Y)$ of the required degree and the group $H_0$ is constructed in a similar way (we need the fact that $\operatorname{Sp}(2n, 2)$ has trivial multiplier for $n \geqq 4$ [17]).

It is clear from the construction that these two representations are related by the action of $\operatorname{Aut}(E \circ Y)$ on the normal subgroup $A(E \circ Y)$. Also, complex conjugation interchanges these two representations, since each restricted to $E$ has rational trace.

(c) Our argument may be refined as follows. Let $F$ be a splitting field for $X = E$ (resp. $E \circ Y$). We may replace $\boldsymbol{C}[X]$ by $F[X]$ to get a projective representation of $W = \operatorname{Aut}(X)$ (resp. $A(X)$) over $F$, i.e., our map $m$ can be made to satisfy $m(\alpha)m(\beta) = c(\alpha, \beta)m(\alpha\beta)$, where the $m(\ )$ are matrices with entries in $F$ and $c(\alpha, \beta) \in F$. Thus, the image $m(W)$ in $PGL(2^n, \boldsymbol{C})$ actually lies in $PGL(2^n, F) \subseteqq PGL(2^n, \boldsymbol{C})$. Then, from the diagram, $\phi(W) \subseteqq \boldsymbol{C}^\times \cdot GL(2^n, F)$, where $\boldsymbol{C}^\times$ is identified with the scalar matrices.

Now, we have $\phi(W') = \phi(W)' \subseteqq (\boldsymbol{C}^\times \cdot GL(2^n, F))' = SL(2^n, F)$. Thus, on $2^n$-dimensional linear representation for $W'$ may be written in the field $F$.

Now, let $W_0$ be $H$ or $H'E$. If $\psi$ denotes the character of the unique faithful representation of $E$, then, evidently, if $\chi$ is irreducible character of $W_0$ for which $\chi|_E$ is faithful, $\chi|_E$ is a multiple of $\psi$. For such $\chi$, a theorem of Clifford states that $\chi = \xi\eta$, where $\xi, \eta$ are projective characters of $W_0$ and $E \subseteq \ker(\xi)$, $\eta(1) - \psi(1)$. In fact, the proof of (a) and the proof in [5] (page 351) shows that we may take $\xi$ and $\eta$ to be characters of ordinary representations, and we may even take $\eta$ to be the character of the $2^n$-dimensional representation we have constructed. If we let $\xi$ be a variable running over the irreducible characters of $W_0/E$, we can see that all the $\xi\eta$ are distinct and form the set of faithful irreducible characters of $W_0$ by using the fact that $|W_0|$ is the sum of the squares of the degrees of the irreducible characters of $W_0$.

Similar arguments prove the statement for $W_0 = H_0$ or $H_0'E$. There are two choices for $\eta$ to consider in this case, however.

12. *Proof of Corollary* 3. It suffices to prove the second extension does not split. Suppose it does. Let $G \subset A(E \circ Y)$, $G \cong \mathrm{Sp}(4, 2) \cong \sum_6$. By Theorem 5(b), there is a group $H_0$ and an exact sequence

$$1 \longrightarrow Z_2 \longrightarrow H_0 \xrightarrow{\pi} A(E \circ Y) \longrightarrow 1 .$$

Let $G_0$ be the preimage of $G$ in $H_0$. Since $H_0$ has a faithful complex representation of degree 4, so does $G_0$.

Since $\sum_6$ has no faithful ordinary irreducible representations of degree less than 5 [5], $G_0$ is isomorphic to a covering group of $\sum_6$ (see [12], 24.3).

We identify $E \circ Y$ with $0_2(H_0)$. Denote images modulo $Y$ by bars. Note that Inn $(E \circ Y)$ inherits from $E \circ Y$ an alternating form stabilized by $G$. Let $I$ be a subgroup of $E \circ Y$ containing $Y$ isomorphic to $Z_2 \times Z_2 \times Z_4$. Then $\bar{I}$ is a maximal isotropic subspace of Inn $(E \circ Y)$ and $|\bar{I}| = 4$. The stabilizer $K$ in $G$ of $\bar{I}$ is isomorphic to $\sum_4 \times Z_2$. Let $K_0$ be the preimage in $G_0$ of $K$. Since the Sylow 2-subgroups of $G_0'$ are quaternion of order 16, we have $K_0' \cong SL(2, 3)$. Note, $|0_2(K_0)| = 16$.

Now, $K_0$ acts on $I$ while centralizing $Y$. Since $K_0$ induces $SL(2, 2)$ on $\bar{I}$, $0_2(K_0)$ stabilizes the chain $I \supset Y \supset 1$. We claim that $0_2(K_0)$ stabilizes the chain $I \supset E' \supset 1$. First, notice that every coset of $Y$ in $I$ contains an element of order 2. Now, let $w \in 0_2(K_0)$, $u \in I$, and write $u = vy$, where $y \in Y$ and $v^2 = 1$. Since $I$ is abelian, and $0_2(K_0)$ centralizes $Y$, we have $[u, w] = [vy, w] = [v, w]^y[y, w] = [v, w]$ and

$[u, w]^2 = [v, w]^2 = [v^2, w] = 1$. Thus, $[I, 0_2(K_0)]$ is contained in $E'$, the subgroup of order 2 of $Y$. This proves the claim. Commutation induces a map $0_2(K_0) \rightarrow \mathrm{Hom}\,(I/Y, E')$, and the latter group has order 4. So, the kernel $R$ of this map has order at least 4. Note that $R \cap I \subseteqq 0_2(K_0) \cap I = E'$. Let $R_1$ be an abelian subgroup of $R$ of order at least 4. Then, $\langle R_1, I\rangle$ is an abelian group of order

$$|R_1 \cap I|^{-1}|R_1||I| \geqq \frac{1}{2}\cdot 4\cdot 16 = 25 .$$

Since $R/R \cap E'$ is elementary abelian, $\langle R_1, I\rangle/E'$ is elementary abelian of order at least $2^4$, whence $\langle R_1, I\rangle$ contains a subgroup $L$ which is elementary abelian of order $2^4$.

We claim that in our representation of degree 4, every element of $H_0$ acts with determinant 1. Since $G_0$ covers $H_0/H_0' \cong Z_2$, it suffices to prove the statement for elements of $G_0$. Suppose there are elements of $G_0$ acting with determinant $-1$. Since $G$ contains an elementary abelian group of order 8, the Sylow 2-subgroups of $G_0$ are not (generalized) quaternion. But, as those of $G_0'$ are, there is an involution $u \in G_0\backslash G_0'$. If the matrix representing $u$ is diagonalized, it has $\pm 1$'s on the diagonal. Since $u$ acts with determinant $-1$, these eigenvalues are

$$\{1, -1, -1, -1\} \quad \text{or} \quad \{-1, 1, 1, 1\} .$$

Now $(u)\pi \in G$ has centralizer $\langle (u)\pi\rangle \times M$, $M \subset G'$, $M \cong \sum_4$. Let $M_1$, resp. $M_2$, denote the preimage in $G_0$ of $M$, resp. $M'$. Since $(u)\pi$ centralizes $M$, $u$ induces a central automorphism of $M_1$, but centralizes $M_2 \cong SL\,(2, 3)$.

Since $M_2$ commutes with $u$, $M_2$ preserves the eigenspaces of $u$. This forces $M_2$ to have a 1-dimensional constituent, whence $M_2'$ acts trivially on this constituent. However, $E' \subset M_2'$ and $E'$ acts as the scalar $-1$ in this 4-dimensional representation, contradiction.

We have just shown that every element of $H_0$ acts with determinant 1. The same must hold for $L \subset H_0$. But it is impossible for an elementary abelian group of order $2^4$ to act faithfully with determinant 1 in 4 dimensions.

This final contradiction proves that the complement $G$ does not exist. The corollary is established.

13. *Proof of Theorem* 1 (a), *the case* $n = 3$. Let $H$ be the group of Theorem 5(a), associated with $E = E_3$. Set $H_1 = H'$. We identify $E$ with $0_2(H_1) = 0_2(H)$. We have $E' = Z(H_1) = Z(H)$, $H_1/E \cong \Omega^+(6, 2) \cong A_8$, $H_1/E' \cong A(E)$.

Suppose that

$$(*)\quad 1 \longrightarrow E/E' \longrightarrow H_1/E' \longrightarrow H_1/E \longrightarrow 1$$

is the split extension. Take $H_2 \subset H_1$ so that $H_1 = EH_2$ and $E \cap H_2 = E'$. Then $H_2 \cong \boldsymbol{Z}_2 \times A_8$ or $\hat{A}_8$, the covering group of $A_8$.

Let $a(t) \in H_2$ be a representative for $t \in H_2/E'$. We assume $a(1) = 1$. In the case $H_2 \cong A_8 \times \boldsymbol{Z}_2$, we take all the $a(t)$ to lie in $H_2'$. Every $g \in H_1$ may be expressed uniquely as a product $g = xa(t)$, $x \in E$, $a(t) \in H_2$. If $g^2 = 1$, exactly one of the possibilities below must hold:

$$\begin{array}{llll}
(\mathrm{i}) & x = 1 & a(t) = 1 & \\
(\mathrm{ii}) & x = 1 & |a(t)| = 2 & \\
(\mathrm{iii}) & x = e & a(t) = 1 & \\
(\mathrm{iv}) & x = e & |a(t)| = 2 & \\
(\mathrm{v}) & |x| = 2,\ x \notin \langle e \rangle & x^t = x & a(t) = 1 \\
(\mathrm{vi}) & |x| = 2,\ x \notin \langle e \rangle & x^t = x & |a(t)| = 2 \\
(\mathrm{vii}) & |x| = 2,\ x \notin \langle e \rangle & x^t = xe & a(t)^2 = e \\
(\mathrm{viii}) & |x| = 4 & x^t = x & a(t)^2 = e \\
(\mathrm{ix}) & |x| = 4 & x^t = xe & |a(t)| = 2\,.
\end{array}$$

For any group $G$ that follows, let $s(G) = |\{y \in G \mid y^2 = 1\}|$. We count $s(H_1)$ in two different ways. First, we analyze the contribution types (i) through (ix) to $s(H_1)$. In particular, we show that the contribution of each of types (i) and (iii) is 1 and that of each other type is a multiple of 5. We point out that for all $x \in E$, and all $a(t) \in H_2$, we have that $C_{H_2}(xa(t)) \subseteqq N_{H_2}(\langle a(t), e\rangle)$, and in case $H_2 \cong A_8 \times \boldsymbol{Z}_2$, we have $N_{H_2}(\langle a(t), e\rangle) = C_{H_2}(a(t))$.

Assume $H_2 \cong A_8 \times \boldsymbol{Z}_2$; then $H_2' = \{a(t) \mid t \in H_2/\boldsymbol{Z}(H_2)\}$. For types (i) and (iii), we get one $g$ each. For each of (ii) and (iv), we get as many $g$ as involutions in $A_8$; the total is $2\{3\cdot5\cdot7 + 2\cdot3\cdot5\cdot7\}$. For (v), (vi), and (vii), note that there are $2\cdot35$ involutions $x \in E\backslash\langle e\rangle$. Let $m$ be the number of $a(t) \in H_2$ centralizing $x$ with $|a(t)| = 2$. There are no $g$ of type (vii) since $H_2' \cong A_8$. Thus, the contribution of types (v), (vi) and (vii) is $70\{1 + m\}$. No $g$ of type (viii) occurs since $H_2' \cong A_8$. For (ix), note that there are $2\cdot28$ elements of order 4 in $E$. The involutions $a(t) \in H_2$ inverting $x$ lie in $D$, the subgroup of $H_2'$ stabilizing $x\langle e\rangle$. Since $D \cong \mathrm{Sp}\,(4, 2) \cong \sum_6$, every nonidentity 2-element in $D$ has $D$-conjugacy class of size divisible by 5. Since the set of $a(t)$ inverting $x$ is a union of $D$-conjugacy classes, the number of such $a(t)$ is divisible by 5.

Adding up these contributions, we get $s(H_1) = 2(\mathrm{mod}\ 5)$ in the case $H_2 \cong A_8 \times \boldsymbol{Z}_2$.

Assume $H_2 \cong \hat{A}_8$. Using Schur's generators and relations for $A_8$ [15] (1911), we find that an involution in $A_8$ is represented in $\hat{A}_8$ by an element of order 4 if and only if it can be written as the product of two disjoint transpositions. For types (i), (iii), we get one $g$ each. For each of (ii), (iv), we get 3.5.7 involutions. The contribution of types (v), (vi) and (vii) is a multiple of 70. For each of (viii) and (ix), the contribution is a positive multiple of 5.

So, adding the contribution, we get $s(H_1) \equiv 2 \pmod 5$ in the case $H_2 \cong \hat{A}_8$ as well.

Next, we count $s(H_1)$ in a different way, using a theorem of Frobenius and Schur, [8], §3. Namely, if $G$ is a finite group, then $s(G) = \sum \nu(\chi)\chi(1)$, where the sum ranges over the irreducible characters $\chi$ of $G$,

$$\nu(\chi) = \frac{1}{|G|} \sum \chi(y^2) \text{ (sum over all } y \in G\text{), and where } \nu(\chi) = 1$$

if and only if $\chi$ is afforded by a real representation, $\nu(\chi) = -1$ if and only if $\chi$ is real but not afforded by a real representation, $\nu(\chi) = 0$ otherwise.

The proper normal subgroups of $H_1$ are $E = 0_2(H_1)$ and $E'$. We have

$$s(H_1) = \lambda + \mu$$

where

$$\lambda = \sum_{E' \subseteqq \ker \chi} \nu(\chi)\chi(1) \quad \text{and} \quad \mu = \sum_{1 = \ker \chi} \nu(\chi)\chi(1)$$

so that $\lambda = s(H_1/E')$.

Consider those $\chi$ occuring in $\mu$. Since $\chi|_E$ is a sum of characters faithful on $E$, the arguments of §11 show that $\chi = \xi\eta$, where $\eta$ is the character of the 16-dimensional representation constructed in §11, and $\xi$ is any irreducible character of $H_1$ with kernel containing $E$.

Now, by the results of §11, $\eta$ is afforded by a rational (hence, real) representation, and so $\nu(\eta) = +1$. A study of [8], §3, shows that we can get $\nu(\chi) = \nu(\xi\eta) = \nu(\xi)$. Therefore,

$$\begin{aligned} \mu &= \sum_{\ker \chi = 1} \nu(\chi)\chi(1) = \sum_{\ker \xi \supseteqq E} \nu(\xi)\xi(1)\eta(1) \\ &= \eta(1) \sum_{\xi} \nu(\xi)\xi(1) = 16\, s(H_1/E) = 16\, s(A_8) \\ &= 16\, \{1 + 3\cdot5\cdot7 + 2\cdot3\cdot5\cdot7\} = 16\,(316)\,. \end{aligned}$$

We now have the value of $\mu$. We next calculate the value of $\lambda = s(H_1/E')$ under the assumption that (*) splits.

Denote images under $H_1 \to \bar{H}_1 = H_1/E'$ by bars. We have $\bar{H}_1 = \bar{E}\bar{H}_2$, a semidirect product. Note that $\bar{H}_2 \cong A_8$ has two classes of involutions, represented by, say, $h$ and $k$. We choose notation so that, in the usual representation of $A_8$ on 8 letters, $h$ fixes no letter and $k$ fixes four. Then $|C_{\bar{H}_2}(h)| = 2^6 \cdot 3$, $|C_{\bar{H}_2}(k)| = 2^5 \cdot 3$. In particular, $h$ is central in a Sylow 2-subgroup and $k$ is not.

We claim that, for any involution $y \in \bar{H}_2$, $|C_{\bar{E}}(y)| = 2^4$. Let $v \in \bar{E}$ be a nonzero isotropic vector. Replacing $h$ by a conjugate if necessary, we may assume $h \in 0_2(S)$, where $S$ is the subgroup of $\bar{H}_2$ stabilizing $\langle v \rangle$. Since $0_2(S)$ is elementary abelian of order 16, it does not act regularly on the 8 letters. Thus, we may assume $k \in 0_2(S)$ as well.

Let $\bar{E}_0$ be the annihilator of $\langle v \rangle$ in $\bar{E}$ under the bilinear form. Then $0_2(S)$ acts trivially on $\bar{E}_0/\langle v \rangle$. Thus, any $y \in 0_2(S)^\#$ centralizes a hyperplane of $\bar{E}_0$, whence $|C_{\bar{E}}(y)| \geqq 2^4$. On the other hand, $\bar{H}_2$ contains no elements which act as orthogonal transvections on $\bar{E}$. Thus, $|C_{\bar{E}}(y)| = 2^4$.

Setting $y = h$ or $k$, we get our claim.

We can now calculate $s(\bar{H}_1)$. Every $g \in \bar{H}_1$ can be written $g = xy$, $x \in \bar{E}$, $y \in \bar{H}_2$. We have $g^2 = 1$ if and only if $x^2 = y^2 = [x, y] = 1$. We have shown that if $y \in \bar{H}_2$ is an involution, $|C_{\bar{E}}(y)| = 2^4$. Since the classes of involutions of $\bar{H}_2$ are represented by $h$ and $k$ we have

$$\begin{aligned} s(\bar{H}_1) &= |\bar{E}| + 2^4\{3.5.7 + 2.3.5.7\} = 16\{4 + 105 + 210\} \\ &= 16\,(319)\,. \end{aligned}$$

It follows that $s(H_1) = \lambda + \mu = 16\,(319 + 316) = 16(835)$.

From our first count, we have $s(H_1) \equiv 2 (\text{mod } 5)$, but here we have shown that $s(H_1) \equiv 0\,(\text{mod } 5)$. This contradiction shows that (*) is not split. Therefore, Theorem 1(a) holds in the case $n = 3$ as well.

This completes the proofs of all the Theorems.

## References

1. M. F. Atiyah and C. T. C. Wall, *Cohomology of Groups*, from J. W. S. Cassel and A Fröhlich, Algebraic Number Theory, Thompson Book Company, Washington D. C., 1967.
2. R. Brauer, *Zur Darstellungstheoric der Gruppen endlicher Ordnung*, Math. Zeit., **63** (1956), 406-444.
3. R. Carter, *Simple groups and simple Lie algebras*, J. London Math. Soc., **40** (1965), 193-240.
4. J. Conway, *A group of order* 8, 315, 553, 613, 086, 720, 000, J. London Math. Soc., **1** (1969), 79-88.
5. C. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, Interscience, 1966.
6. J. Dieudonné, *La Géometriè des Groupes Classiques*, Springer-Verlag, Berlin, 1963.
7. L. E. Dickson, *Groups of Steiner in problems of contact*, Trans. Amer. Math. Soc., (1902), 38-45 and 377-382.
8. W. Feit, *Characters of Finite Groups*, W. A. Benjamin, Inc., New York, 1967.
9. D. Gorenstein, *Finite Groups*, Harper and Row, New York (1968).
10. R. Griess, *Schur Multipliers of Finite Simple Groups of Lie Type*, Trans. Amer. Math., (to appear).

11. K. W. Gruenberg, *Cohomological Topics in Group Theory*, Springer-Verlag, Berlin, 1970.

12. B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin, 1967.

13. N. Jacobson, *The Theory of Rings*, American Mathematical Society, Providence, 1943.

14. S. MacLane, *Homology*, Springer-Verlag, Berlin, 1967.

15. I. Schur, *Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen*, J. reine u. angew. Math., **127** (1904), 20-50, and **132** (1907), 85-137; *Über die Darstellung der symmetrischen und der alternienden Gruppe durch gebrochene lineare Substitutionen*, J. reine u. angew. Math., **139** (1911), 155-250.

16. H. K. Pollatsek, *Cohomology groups of some linear groups over fields of characteristic* 2, Illinois J. Math., **15** (1971), 393-417.

17. R. Steinberg, (unpublished).

18. ———, *Representations of algebraic groups*, Nagoya J., **22** (1963), 33-56.

Received May 25, 1972 and in revised form March 8, 1973.

UNIVERSITY OF MICHIGAN