ACADEMIC PRESS
Available online at www.sciencedirect.com
SCIENCE DIRECT
Journal of Algebra 256 (2002) 611–625
JOURNAL OF Algebra
www.academicpress.com

Regular orbits of cyclic subgroups in permutation representations of certain simple groups

Johannes Siemons * and Alexandre Zalesskiĭ

School of Mathematics, University of East Anglia, Norwich NR4 7TJ, UK

Received 4 April 2002
Communicated by Jan Saxl

1. Introduction

In this paper we study regular orbits of cyclic subgroups of finite simple groups. The main result is the following theorem.

Theorem 1.1. *Let G be a known finite simple group, not isomorphic to an alternating group A_n, which admits a doubly transitive permutation representation. Then every cyclic subgroup $H \subset G$ has a regular orbit in any non-trivial permutation representation of G.*

If H acts on Δ then an H-orbit is *regular* if its cardinality is $|H|$. The alternating groups, already in their natural representation, do not have the property of the theorem, hence the exception. The other known simple groups with a doubly transitive permutation representation are $PSL(n,q)$, $Sp(2n,2)$ (two representations), $U_3(q)$, ${}^2B_2(q)$, ${}^2G_2(q)$ and a short list of sporadic examples which are reproduced in Section 5. If one assumes the completeness of the classification of finite simple groups then these are all doubly transitive representations of finite simple groups and the word *known* can be omitted in the theorem. In our paper [8] the Theorem 1.1 was proved for $PSL(n,q)$. Here we consider the remaining doubly transitive groups. The same method can in

* Corresponding author.
E-mail addresses: j.siemons@uea.ac.uk (J. Siemons), a.zalesskii@uea.ac.uk (A. Zalesskiĭ).

0021-8693/02/$ – see front matter
PII: S0021-8693(02)00107-2

principle be extended to other groups of Lie type. Similarly, it may also be interesting to investigate the doubly transitive groups of affine type. However, both problems may require essential additional efforts.

The theorem can be proved using the same ideas as in [8]. For each group one distinguishes the *embedding case* where the result is proved for cyclic $H \subset G$ in doubly transitive representations, and the *factorization case* where the result is proved for cyclic $H \subset G$ acting on a G-set Δ for which $G = G_\omega \cdot G_\delta$ factorizes, with $\delta \in \Delta$ and $\omega \in \Omega$, for some doubly transitive G-set Ω. The details of this are explained again in Section 2. The proof of Theorem 1.1 follows from Theorem 1.1 of [8] for $PSL(n,q)$, from Proposition 3.6 and Theorem 3.7 for $Sp(2n,2)$, from Theorems 4.1, 4.3, 4.4, and 4.5 for $U_3(q)$, ${}^2B_2(q)$, and ${}^2G_2(q)$, and from Theorem 5.1 for the sporadic examples.

2. Preliminaries

The notation in this paper is the usual one. If G is a group and Ω a G-set then $g\omega$ is the image of $\omega \in \Omega$ under $g \in G$ and if $H \subseteq G$ is a subgroup then $H\omega$ is the orbit of ω under H. The stabilizer of ω in G is G_ω and if $\Gamma \subseteq \Omega$ then $g\Gamma := \{g\gamma \colon \gamma \in \Gamma\}$. All G-sets considered here are finite. The number of G-orbits on Ω of size k is denoted by $n_\Omega(G,k)$ or just $n(G,k)$. If K is a field then KG is the group ring over K and $K\Omega$ denotes the natural KG-module with Ω as a basis.

We collect the general results needed for this paper. The first is Theorem 3.1 in [8].

Theorem 2.1. *Suppose that G acts doubly transitively on Ω and also transitively on Δ, where $|\Omega| \geqslant 2$. Let K be a field whose characteristic does not divide the order of G. Then one and only one of the following occurs*:

(i) *There exists an injective KG-homomorphism $\varphi : K\Omega \to K\Delta$.*
(ii) *For any $\omega \in \Omega$ and $\delta \in \Delta$ we have $G = G_\omega \cdot G_\delta$.*

We refer to (i) as the *embedding case* and to (ii) as the *factorization case*. The condition $G = G_\omega \cdot G_\delta$ means that G_δ is transitive on Ω or, equivalently, that G_ω is transitive on Δ. Instrumental in the embedding case is the following, see Theorem 3.6 in [8]:

Theorem 2.2. *Suppose that G acts doubly transitively on Ω and also transitively on Δ, where $|\Omega| \geqslant 2$. Let K be a field, let $H \subset G$ be a cyclic group and put $h := |H|$. If there exists an injective KG-homomorphism $\varphi : K\Omega \to K\Delta$ then $n_\Omega(H,h) \leqslant n_\Delta(H,h)$.*

In [8] we have proved Theorem 1.1 for the projective special linear groups. More precisely:

Theorem 2.3. *Let $PSL(n,q) \subseteq G \subseteq PGL(n,q)$ and let H be a cyclic subgroup of G. Then H has a regular orbit in every non-trivial G-set Ω unless one of the following holds*:

(a) $(n,q) \in \{(2,2),(2,3)\}$, *or*
(b) $(n,q) = (4,2)$, $|\Omega| = 8$ *and* $|H| = 6$ *or* $|H| = 15$.

In the original statement of Theorems 1.1(b) and 1.2(b) in [8] we should have mentioned the possibility $|H| = 6$ for $G = SL(4,2) \cong A_8$. In addition, in Theorem 1.2(b) the exception $H \cong C_3 \times C_3$ should have been stated. These omissions have no effect on any other result in [8].

The strategy of this paper is now clear. For each group G under consideration we first prove the result for any doubly transitive representation (G,Ω). So $1 \leqslant n_\Omega(H,h)$ and hence $n_\Omega(H,h) \leqslant n_\Delta(H,h)$ for any Δ in the embedding case. This exhausts the vast majority of permutation representation of G. For the second part it remains to examine the maximal factorisations of G. These are available in Liebeck et al. [7]. At times G has several doubly transitive representations and the following simple fact cuts down further on the factorisation case: if G_δ is a factor in one doubly transitive representation but not in some other doubly transitive representation then no further work is needed, the result follows by embedding the second representation. We start with the symplectic groups which are the most difficult case to deal with.

3. The symplectic groups $Sp(2n,2)$

In this section we treat the case where G is the symplectic group $Sp(2n,2)$. As we shall use induction, we denote this group by G_n. Let Q_n^+ and Q_n^- denote the quadratic forms defining the orthogonal groups $H_n^+ := O^+(2n,2)$ and $H_n^- := O^-(2n,2)$, respectively, and let $\Omega_n^+ := G_n/H_n^+$, $\Omega_n^- := G_n/H_n^-$. Then Ω_n^+ and Ω_n^- are doubly transitive G_n-sets. If $d_n := |G_n : H_n^+|$ and $c_n := |G_n : H_n^-|$ one may observe that $c_n = 2^{n-1}(2^n - 1)$ and $d_{n-1} = 2^{n-1}(2^n + 1)$. We set $\Omega_n = \Omega_n^+ \cup \Omega_n^-$.

We start off with an observation on the natural representations of G_n. Let F_q be the field of q elements and let $V = F_2^{2n}$ be the natural G_n-module. We keep the same symbol for the restrictions to H_n^+ and H_n^-. Let V_s^+, V_t^+ (respectively V_s^-, V_t^-) denote the set of singular and non-singular vectors in V with respect to Q_n^+ (respectively Q_n^-). Let $\mathbb{C}$ denote the field of complex numbers. The following observation illustrates the use of Theorem 2.1:

Proposition 3.1. *(G_n, V) and (G_n, Ω_n) are not isomorphic as permutation sets while $\mathbb{C}V$ and $\mathbb{C}\Omega_n$ are isomorphic as $\mathbb{C}G_n$-modules.*

Proof. For the first part note that G_n has an orbit of length $2^n - 1$ on V and no orbit of this length on Ω_n. For the second part note that Ω_n^+ and Ω_n^- are doubly transitive permutation G_n-sets so that $\mathbb{C}\Omega_n^+ = 1_{G_n} + \phi_1$ and $\mathbb{C}\Omega_n^- = 1_{G_n} + \phi_2$ where ϕ_1 and ϕ_2 are irreducible $\mathbb{C}G_n$-modules. Therefore $\dim \phi_1 = d_n - 1$ and $\dim \phi_2 = c_n - 1$. As H_n^+ and H_n^- are not transitive on $V^* =: V \setminus \{0\}$, Theorem 2.1 implies that there are injective homomorphisms $\mathbb{C}\Omega_n^- \to \mathbb{C}V^*$ and $\mathbb{C}\Omega_n^+ \to \mathbb{C}V^*$. In particular, $\mathbb{C}V^*$ contains a direct sum $1_{G_n} \oplus \phi_1 \oplus \phi_2$. As the dimension of the right hand side module is $d_n + c_n - 1 = 2^{2n} - 1$, we have the equality $\mathbb{C}V^* = 1_{G_n} \oplus \phi_1 \oplus \phi_2$. As $\mathbb{C}\Omega_n = 1_{G_n} + \mathbb{C}V^*$, the proposition follows. □

Corollary 3.2. *If $A \subset G_n$ is a cyclic subgroup then (A, V) and (A, Ω_n) are isomorphic permutation sets.*

Proof. This follows from [8, Corollary 2.5] and Proposition 3.1.

3.1. The embedding case for Sp$(2n, 2)$

Here we show that every cyclic subgroup of G_n has regular orbits in the doubly transitive representations on Ω_n^+ and Ω_n^-. We start with the following lemma which is valid for arbitrary classical groups (with the same proof; however, to avoid introducing more notation we record the proof only for $Sp(2n, 2)$). Observe that similar situations (but different from the lemma below) are discussed in Huppert [4, Satz 2] and Aschbacher [1, Section 5].

Lemma 3.3. *Let $X \subset G_n$ be a subgroup such that V is a completely reducible X-module. Let W be a homogeneous component of X on V. Then W is either non-degenerate or totally isotropic. In the second case there is another totally isotropic homogeneous component W' of V such that $W + W'$ is non-degenerate.*

Proof. Recall that a homogeneous component of V is the sum of all irreducible X-submodules isomorphic to some irreducible X-module N, say. So let $\mathrm{Hom}_X(N, W) \neq 0$. Let N^* denote the dual of N. Set $W_0 = W \cap W^{\perp}$, $U = W/W_0$ and $V_0 = V/W_0^{\perp}$. We show first that either $W_0 = 0$ or $W_0 = W$. For suppose the contrary when $V_0 \neq 0$ and $U \neq 0$. Then all irreducible constituents of V_0 are dual to those of W_0 and in particular $\mathrm{Hom}_X(N^*, V_0) \neq 0$. As $W \subseteq W_0^{\perp}$, $\mathrm{Hom}_X(N, V_0) = 0$ so N is not self-dual. Observe that U is a non-degenerate symplectic space and a homogeneous X-module. As every non-degenerate X-submodule of U is self-dual, each irreducible X-submodule U_1 of U is totally isotropic. Hence $U/U_1^{\perp} \cong U_1^*$. As $U_1 \cong N$, this is a contradiction.

Next let $W = W_0$. As $\mathrm{Hom}_X(N^*, V_0) \neq 0$ and V is completely reducible, there exists a homogeneous component W' of V such that $\mathrm{Hom}_X(N^*, W') \neq 0$. Show that $Z = W + W'$ is non-degenerate. Indeed, if $Z_0 = Z \cap Z^\perp \neq 0$ then irreducible constituents of $V/Z_0^\perp$ are dual to those of Z_0 so they are isomorphic to N or N^*. This is a contradiction. □

Lemma 3.4. *Let $A \subseteq G_n$ be an abelian subgroup with cyclic Sylow 2-subgroup S. Suppose that $A \neq S$ and that A does not stabilize a pair of complementary and mutually orthogonal subspaces of V. Then A is cyclic and at least $3 \cdot 2^{2n-2}$ points of V belong to regular A-orbits.*

Proof. Let $A = B \times S$. Let $V = V_1 \oplus \cdots \oplus V_k$ where $V_1, \dots, V_k$ are homogeneous components for B. Clearly, $AV_i = V_i$ for each $i = 1, \dots, k$. Therefore $k \leqslant 2$ by Lemma 3.3 and if $k = 2$ then V_1, V_2 are totally isotropic. In the latter case, under dual bases in V_1 and V_2, the matrices of A have shape $\mathrm{diag}(a, (a^t)^{-1})$ where a runs over $A_1 = A|V_1$. Set $B_1 = B|V_1$ and let $X = \langle B_1 \rangle_{F_2}$ be the enveloping algebra of B_1. As V_1 is homogeneous for B, and hence for B_1, X is a field and so B_1 is cyclic. Therefore B and hence A are cyclic.

Let $|X| = 2^l$ where $l > 1$ as $B_1 \neq 1$. As X is a field, V_1 can be viewed as a vector space over X (in particular $m = \dim_X V_1 < \dim V_1$) and $L = \mathrm{End}_X(V_1)$ is a subalgebra of $\mathrm{End}_{F_2}(V_1)$ formed by all elements of $\mathrm{End}_{F_2}(V_1)$ that commute with those in X. Therefore $A_1 \subset L$. Let V_X denote V_1 viewed as a vector space over X. Let $V_X = W_1 \oplus \cdots \oplus W_r$ where $W_1, \dots, W_r$ are indecomposable XA-submodules and $d_1 = \dim_X W_1 \geqslant d_i = \dim_X W_i$ for $i > 1$. Assume first that $r = 1$. Then V_X is uniserial XA-module (equivalently, a generator a of A is represented by a single Jordan block). Let U be the largest proper XA-submodule of V_X. Then $\dim_X U = m - 1$ and U contains each proper XA-submodule of V_X. Let $w \in V_X$ and $w \notin U$. We claim that w belongs to a regular A-orbit. Indeed, if $b = a^i \neq 1$ and $bw = w$ then $W = \{v \in V_X\colon\ bv = v\}$ is a proper A-submodule. Hence $w \in W \subseteq U$ which is a contradiction. The number of vectors in $V_X \setminus U$ is equal to $q^m - q^{m-1}$ where $q = |X|$.

Next let $r > 1$. As A is cyclic and $d_1 \geqslant d_i$ for $i = 1, \dots, r$, it follows that A is faithful on W_1 (that is, no $a \in A$ except $a = 1$ acts trivially on W_1). Therefore at least $(q^{d_1} - q^{d_1 - 1})q^{m-d_1} = q^m - q^{m-1}$ vectors of V_X belong to regular A-orbits.

If $V_1 = V$ then $\dim V_1 = 2n$ so $q^m - q^{m-1} = 2^{2n} - 2^{2n-l} \geqslant 2^{2n} - 2^{2n-2} = 3 \cdot 2^{2n-2}$ as $l > 1$ and we are done.

If $V \neq V_1$ then $\dim V_1 = n$. In this case at least $q^m(q^m - q^{m-1})$ vectors of V belong to regular orbits. So $q^m(q^m - q^{m-1}) = 2^n(2^n - 2^{n-l}) = 2^{2n} - 2^{2n-l} \geqslant 3 \cdot 2^{2n-2}$ as above. □

For $1 \leqslant m < n$ consider the subgroup $X_m \subseteq G_n$ isomorphic to $G_m \times G_{n-m}$. This is the stabilizer in G_n of a non-degenerate m-dimensional subspace of V. We are interested in the action of X_m on Ω_n^+ and Ω_n^-.

Lemma 3.5. (1) *As an X_m-set Ω_n^+ is the union of two orbits isomorphic to $\Omega_m^+ \times \Omega_{n-m}^+$ and $\Omega_m^- \times \Omega_{n-m}^-$.*

(2) *As an X_m-set Ω_n^- is the union of two orbits isomorphic to $\Omega_m^+ \times \Omega_{n-m}^-$ and $\Omega_m^- \times \Omega_{n-m}^+$.*

Proof. Let V_m be a non-degenerate m-dimensional subspace of V such that X is the stabilizer of V_m in G. Set $V_{n-m} = V_m^{\perp}$. For $i = m, n-m$ let f_i be a (unique) bilinear form on V_i preserved by X_m. Let Q_i^+ and Q_i^- denote non-degenerate quadratic forms on $2i$-dimensional vector spaces of Witt defect 0 and 1, respectively, with associated bilinear form given by f_i. Then $Q_m^+ + Q_{n-m}^+$ and $Q_m^- + Q_{n-m}^-$ are quadratic forms of Witt defect 0 while $Q_m^+ + Q_{n-m}^-$ and $Q_m^- + Q_{n-m}^+$ are of Witt defect 1, see [6, 2.5.11]. Observe that the stabilizer of $Q_m^+ + Q_{n-m}^+$ in X_m is $H_n^+ \times H_n^+$, and the stabilizer of $Q_m^- + Q_{n-m}^-$ in X_m is $H_n^- \times H_n^-$. Hence X_m has orbits on Ω_n^+ isomorphic to $\Omega_m^+ \otimes \Omega_{n-m}^+$ and $\Omega_m^- \otimes \Omega_{n-m}^-$. As the lengths of these orbits are $d_m d_{n-m}$ and $c_m c_{n-m}$, their union is Ω_n^+. Similarly, the stabilizer of $Q_m^- + Q_{n-m}^+$ in X_m is $H_n^- \times H_n^+$ and the stabilizer of $Q_m^+ + Q_{n-m}^-$ in X_m is $H_n^+ \times H_n^-$. Hence X_m has an orbit on Ω_n^+ isomorphic to $\Omega_m^- \otimes \Omega_{n-m}^+$ and $\Omega_m^+ \otimes \Omega_{n-m}^-$. As the lengths of these orbits are $d_m c_{n-m}$ and $c_m d_{n-m}$, their union is Ω_n^-. □

Proposition 3.6. *Let $A \subseteq G_n$ be an abelian subgroup with cyclic Sylow 2-subgroup S. Then A has a regular orbit on Ω_n^+. If, in addition, the Sylow 3-subgroup of A is cyclic then A has a regular orbit on Ω_n^- unless $n = 1$ or, possibly, $n = 2$ with $|A| = 6$.*

Proof. Suppose first that V is not an orthogonal sum of proper non-degenerate A-modules. If $A = S$ the claim is trivial. Let $A \neq S$. By Lemma 3.4 A is cyclic and at least $3 \cdot 2^{2n-2}$ vectors of V belong to regular A-orbits. By Lemma 3.5 the permutation A-set $\Omega_n^+ \cup \Omega_n^-$ is isomorphic to V. As $3 \cdot 2^{2n-2} > 2^{n-1}(2^n + 1) = c_n = |\Omega_n^+| > |\Omega_n^-|$, not all points of regular A-orbits on $\Omega_n^+ \cup \Omega_n^-$ belong to Ω_n^+ or Ω_n^-.

Next suppose that $V = V_1 \oplus V_2$ where V_1, V_2 are non-degenerate A-modules and $V_2 = V_1^{\perp}$. Let $2m = \dim V_1$. Then $A \subset X_m = \mathrm{Stab}_{G_n}(V_1)$. Set $A_i = A|V_i$ for $i = 1, 2$. The cases with $n \leqslant 4$ can be easily verified by using the tables in [2] or by refining the argument below. So let $n > 4$, and we can assume that $m \leqslant n - m$. By Lemma 3.5, Ω_n^+ viewing as an X_m-set, contains $\Omega_m^+ \times \Omega_{n-m}^+$ hence the result follows by induction on n. Observe that A_2 has a regular orbit on Ω_{n-m}^- (otherwise, $n - m \leqslant 2$ which conflicts with $n > 4$). As Ω_n^- contains $\Omega_m^+ \times \Omega_{n-m}^-$, the result is again obtained by induction. □

3.2. The factorisation case for $Sp(2n, 2)$

It remains to analyse the factorisations of $Sp(2n, 2)$, denoted by G_n as before. These are determined by Liebeck, Praeger and Saxl in [7]. Having in mind the remark made following Theorem 2.2 we need to consider only those factorisations where the maximal subgroup factors both with $O^+(2n, 2)$ and $O^-(2n, 2)$. This only happens when $Sp(2n, 2) = M \cdot O^{\pm}(2n, 2)$ where $M \cong Sp(2k, 2^\ell) \cdot C_\ell$ with $n = k\ell$ and C_ℓ being the cyclic group of prime order ℓ, see Table 1 in [7]. In fact, $M = N_{G_n}(S)$ where $S \cong Sp(2k, 2^\ell)$ is naturally embedded in G_n.

The field of q elements is denoted by F_q. If n is a positive integer let $R := M(2n, F_2)$ denote the ring of all $2n \times 2n$ matrices over F_2. Let σ denote an anti-automorphism of R such that $G_n = \{x \in R\colon\ x\sigma(x) = \mathrm{Id}\} \cong Sp(2n, 2)$.

The aim of this section is to prove the following:

Theorem 3.7. *Let $R = M(2n, F_2)$ with $n > 1$. Let F be a subfield of R such that $\mathrm{Id} \in F$, $\sigma(x) = x$ for all $x \in F$ and such that $\ell = [F : F_2]$ is a prime. Let H be a cyclic subgroup of G_n and set $N := N_{G_n}(F)$. Then there exists some $g \in G_n$ such that $H \cap gNg^{-1} = 1$, except for $n = 2$ with $|H| = 6$.*

We mention that $N_{G_n}(S)$ with $S \cong Sp(2k, 2^\ell)$ is equal to $N = N_{G_n}(F)$, where $F = C_R(S)$ is a field on which σ acts trivially, and that N is determined up to conjugacy for any embedding of S in G_n. The proof of this theorem requires some preparatory results, and these follow now.

Lemma 3.8. *Let σ and R be as above and let $e \neq 0$ be an idempotent such that $\sigma(e) = e \neq \mathrm{Id}$. Set $d = \operatorname{rank} e$, $C = eRe$ and $C_\sigma = \{x \in C\colon\ \sigma(x)x = e\}$. Then C_σ is a group isomorphic to $Sp(d, F)$.*

Proof. Let V be the natural R-module and $W = eV$. Let $v_1, \ldots, v_{2n}$ be a basis of V such that $v_1, \ldots, v_d \in W$. It is well known that σ can be described for $r \in R$ as $\sigma(r) = \Phi r^t \Phi^{-1}$ where Φ is a symmetric matrix with zero diagonal and r^t denotes the transpose of r. As $\sigma(e) = e$ and $e^t = e$ in this case, we have $\Phi e = e\Phi$ and hence $\Phi = \mathrm{diag}(\Phi_1, \Phi_2)$ where Φ_1 stabilizes W. Clearly, eRe consists of matrices of shape $\left(\begin{smallmatrix} A & 0 \\ 0 & 0 \end{smallmatrix}\right)$ where $a \in M(d, F)$. Then $\sigma(a) = \Phi_1 A^t \Phi_1^{-1}$. The matrix Φ_1 is the Gram matrix of a symplectic form on W and hence the group C_σ is a symplectic group $Sp(d, F)$ corresponding to this form. □

Lemma 3.9. *The theorem is true for G_2.*

Proof. As can be seen from [2], the group $Sp(4, 2)$ is isomorphic to S_6 and N is isomorphic to S_5. So G_2/N is the natural permutation set for $S_6 \cong G_2$. Hence the result follows. □

Lemma 3.10. *Let $F = F_{q^2}$ and $X = SU(m,q)$.*

(i) *If $m > 2$ then X is not contained in the normalizer of a proper non-central subring L of $M(m,F)$;*
(ii) *if $m = 2$ then X is conjugate to $SL(2,F_q)$.*

Proof. (ii) is well known. Let V be the natural X-module. From [6, 2.10.6(ii)] it follows that X is absolutely irreducible. Let R be the Jacobson radical of L. If $R \neq 0$ then $RV \neq V$ as R is nilpotent and $xRV = RV$ for all $x \in X$. This is impossible and so $R = 0$. If L is not simple then X permutes the minimal central idempotents of L, so X is imprimitive. This means that there exists a non-trivial homomorphism $X \to \mathrm{Sym}(m)$. As $|PSU(m,F_q)| > (m)!$ we see that X is not simple. Hence $(m,q) = (3,2)$. The latter case does not hold as the order of an imprimitive group in $SL(3,4)$ is at most 54. Therefore, L is simple and so $L \cong M(k,T)$ for some field T and integer k. Observe that $LV = V$ for otherwise $XLV = LX$. Therefore, V is a homogeneous L-module (as all non-trivial irreducible L-modules are isomorphic). We identify T with the subfield of scalar matrices in $M(k,T)$. Then T contains the identity of $M(m,F)$. As T is the centre of L, it is normalized by X. Since $\mathrm{Aut}(T)$ is abelian, we have $X \subseteq C_{M(m,F)}(T)$ unless $(m,q) = (3,2)$ which implies that $|T| = 8$ and $|X| \leqslant 24$. This is absurd. Hence X centralizes T. By Schur's Lemma, $T \subseteq F$. Set $C := C_{M(m,F)}(L)$. As each automorphism of L which is trivial on T is inner, we conclude that $X \subseteq L^*C^*$ where * indicates the group of units in the ring. If $C \neq F$ then X is tensor-decomposable which is not the case. So $C = F$ and $X \subseteq L^*F^*$. As $X = X'$, this implies that $X \subseteq L$. However, X cannot be realized over a subfield of F, see [6, 2.10.10(i)]. This completes the proof of (i). □

Lemma 3.11. *Let $X \subseteq M(2n,F_2)$ with $n > 2$ be a non-central subring such that $gXg^{-1} = X$ for all $g \in G_n$. Then $X = M(2n,F_2)$. If $n = 2$ then this remains true with G_2 being replaced by $G_2' \cong A_6$.*

Proof. For convenience abbreviate G_n to G. Suppose that $X \neq M(2n,2)$. Then X is semisimple. Indeed, if $Y = \mathrm{Rad}\,X$ then YV is a G-module, as $gYV = gYg^{-1}gV \subseteq YV$. If X is not simple then G is imprimitive and so we have a non-trivial homomorphism $G \to \mathrm{Sym}(2n)$. If $2n > 4$ then G is simple and so $|G| \leqslant |\mathrm{Sym}(2n)|$ which is not the case. If $2n = 4$ then G has a simple subgroup $G' \cong A_6$ of index 2. As $|A_6| > 2|GL(2,2)|$, in this case G' is primitive. Thus X is a simple ring and so $X = M(l,F_q)$ for some even q. If $q > 2$ let L denote the centre of X, that is $L \cong F_q$. Then $gLg^{-1} = L$ for all $g \in G$ which means that there is a homomorphism from G into $\mathrm{Gal}(L/F_2)$, which is abelian. If $2n > 4$, this homomorphism has to be trivial and so G centralizes L. If $2n = 4$, the homomorphism must be trivial on $G' \cong A_6$ so that G' centralizes L. By Schur's Lemma G, if $2n > 4$, and G', if $2n = 4$, are not absolutely irreducible. If $2n > 4$, this contradicts [6, 2.10.6]. If $2n = 4$ then A_6 is not isomorphic to a subgroup of $GL(2,r)$ for any even r. So A_6 is absolutely irreducible. Thus, $q = 2$. Clearly, X contains Id, as otherwise $geg^{-1} = e$ for the central idempotent e of X and all $g \in G$. This is not the case by Schur's lemma. Every automorphism of X is known to be inner. Therefore, for each $g \in G$ there exists $y_g \in X$ such that $gxg^{-1} = y_g e y_g^{-1}$ for all $x \in X$. It follows that G has a projective representation $\tau : G \to GL(2n,2)$. It is in fact ordinary as both G and $GL(2n,2)$ have trivial center. It follows from Schur's lemma that τ is non-trivial, and also non-trivial on G' if $2n = 4$. It is well known that G, and G' if $2n = 4$, has no non-trivial representation of degree $l < 2n$. □

Lemma 3.12. *Let $2n > 4$ be even and let $\mathrm{Id} = e_1 + e_2 \in R = M(2n, F_2)$ where e_1 and e_2 are idempotents of R with $\sigma(e_1) = e_2$. Set $C_i := e_i R e_i$ for $i \in \{1, 2\}$, $C := C_R(e_1)$ (hence $C = C_1 \oplus C_2$), and $C_\sigma := C \cap G_n$. Let $M \subseteq R$ be a proper subring.*

(i) *There is $g \in G_n$ such that $e_1(gMg^{-1} \cap C_\sigma) \neq C_1$ and $gMg^{-1} \cap C_\sigma \neq C_\sigma$.*
(ii) *Let l be prime, $M \cong M(2n/l, F_{2^l})$ and $N = N_{GL(2n,2)}(M)$. Then $e_1(gNg^{-1} \cap C_\sigma) \neq e_1 C_\sigma$.*

Proof. For convenience abbreviate G_n to G. As $e_2 = \mathrm{Id} - e_1$, we have that $e_1e_2 = e_2e_1 = 0$. By Lemma 3.11 there is some $g \in G$ such that $e_1 \notin gMg^{-1}$. So we can assume that $e_1 \notin M$. Set $M_\sigma = M \cap G$ and $C_\sigma = C \cap G$. Clearly, $C_\sigma = \{x + \sigma(x^{-1})\}$ where x runs over $C_1^* = GL(n,2)$. Hence $e_1 G_\sigma = C_1^*$. Observe that $e_1 M_\sigma \neq C_1^*$. Indeed, as $e_1(x + \sigma(x^{-1})) = x$, the equality $e_1 M_\sigma = C_1^*$ implied that $M_\sigma = C_\sigma \cong C_1^*$. Therefore, $y \mapsto e_1 x$ and $y \mapsto e_2 x$ for $y \in C_\sigma = M_\sigma$ are dual representations of $C_1^* = GL(n,2)$. As $n > 2$ they are non-equivalent. Therefore $\langle M_\sigma \rangle$ is not a simple ring. Then it is easy to see that $\langle M_\sigma \rangle = C$ whereby $e_1 \in C \subseteq M$, contradicting the above. Thus, $e_1 M_\sigma \neq C_1^*$ and $C_\sigma \neq M_\sigma = M \cap C_\sigma$ as $C_1^* = e_1 C_\sigma$. This proves (i). As N/M_σ is of prime order l, it is abelian. Hence if $e_1 C_\sigma \subseteq e_1(C_\sigma \cap gNg^{-1})$ then $e_1 C_\sigma \subseteq e_1 M_\sigma$. This is not true as $C_\sigma \cong GL(n,2)$ is simple. □

Lemma 3.13. *Let $X \subset R$ be a subring and let I, J be ideals of X such that $I + J = X$.*

(i) *Suppose that $I \cap J \neq J$ and X/I is simple. Then $J/(I \cap J) \cong X/I$.*
(ii) *Let $e \in R$ be an idempotent with $e \neq 0, \mathrm{Id}$ and $X \subseteq C_R(e)$. Suppose that eX is a simple non-commutative ring and that $(\mathrm{Id} - e)X$ is commutative. Then $eX \subseteq X$.*

Proof. The first part is obvious. To prove (ii) set $\eta : X \to eX$ with $\eta(x) = ex$, $\eta' : X \to (1 - e)X$ with $\eta'(x) = (1 - e)x$ for $x \in X$, and let $I := \operatorname{Ker} \eta$,

$J := \operatorname{Ker}\eta'$. Then $I \cap J = 0$ and $J \subseteq eX$ as $x = ex + (1-e)x = ex$ for $x \in J$. Also, $J \neq 0$ as X/J is commutative and X is not. By (i) $J \cong X/I \cong eX$ and as $J \subseteq eX$ we have $eX = J$ as desired. $\square$

We now have the prerequisites to prove the main theorem of this section.

Proof of Theorem 3.7. By Lemma 3.9, we assume that $n > 2$. Set $M := C_R(F)$ so that $M \cong M(2n/l, F)$ and F is the centre of M. For convenience again abbreviate G_n to G. Then $M_\sigma =: G \cap M = C_G(F) = \{x \in M\colon\ x\sigma(x) = \mathrm{Id}\}$ is isomorphic to $Sp(2n/l, F)$ and $N/C_G(F)$ is isomorphic to $\mathrm{Gal}(F/F_2)$. In particular, $N/C_G(F)$ is cyclic of order l. Set $A := \langle H\rangle_{F_2}$. So A is a commutative ring. We split the argument into five parts.

(i) Suppose first that A is a field. Then $|H|$ is odd. As $\sigma(h) = h^{-1} \neq h$ for $h \in H$, we observe that σ acts non-trivially on the subfield $\langle h\rangle$ of A for each $h \neq 1$. Since $\sigma^2 = 1$ it follows that $[\langle h\rangle : F_2]$ is even, and $\langle h\rangle$ contains a unique subfield L_h isomorphic to F_4. The same is true for A and so $L_h = L$ does not depend on h. Let $t \in L$ be an element of order 3. As $H_g := H \cap gNg^{-1} \neq 1$ for each $g \in G$, we observe that each H_g contains t, and hence $t \in N_1 := \bigcap_{g\in G} gNg^{-1}$. Clearly, N_1 is normal in G and $|N_1| > 2$ which is impossible as $2n > 4$.

(ii) Now we assume that there exist idempotents e_1 and e_2 in $C_R(H)$ such that $\sigma(e_1) = e_2$ and $e_1 + e_2 = \mathrm{Id}$. Set $C = C_R(e_1)$. Clearly, $C = C_1 \oplus C_2$ where $\sigma(C_1) = C_2$, $C_i \cong M(n, F_2)$ and where e_i is the identity of C_i for $i = 1, 2$. Set $C_\sigma := C \cap G$ and $N_C =: N \cap C_\sigma$. By Lemma 3.12 we have that $e_1 N_C \neq C_1^*$. By Theorem 1.1 of [8] there is some $y \in C_1^*$ such that $e_1 H \cap y e_1 N_C y^{-1} = 1$, except possibly when $n = 4$ and $e_1 N_C \cong A_7$. As A_7 is simple and N_C/M_σ is cyclic, this implies $e_1 M_\sigma = e_1 N_C \cong A_7$. However, A_7 is absolutely irreducible in $GL(4, 2)$ and so it is not contained in any proper subring. If $T = \mathrm{diag}(y, \sigma(y^{-1}))$ then $H \cap tHt^{-1} = 1$, completing the proof of the theorem in the case under discussion.

(iii) Suppose that A is local. Let H_1 be a maximal subgroup of odd order in H. The theorem is trivial if $H_1 = 1$. So suppose that $H_1 \neq 1$. Then $B := \langle H_1\rangle$ is a semisimple ring by Maschke's Theorem and hence B is a field as A is local. Set $C = C_R(B)$, $C_\sigma = G \cap C$, $B_\sigma := B \cap G$. Then $C \cong M(k, B)$ where $k \cdot [B : F_2] = 2n$. By (ii) we can assume that $B \cap N = 1$, hence $H_1 \cap N = 1$. Then $C_\sigma \neq N \cap C_\sigma$, as otherwise $\mathrm{Id} \neq H_1 \subseteq B \cap G \subseteq C \cap G = C_\sigma = N \cap C_\sigma \subseteq N$, which is false.

Recall that $H \subseteq C_\sigma$ and that $H \cap gN_C g^{-1} \neq 1$ for each $g \in C_\sigma \subseteq G$. Let $1 \neq h \in H \cap gN_C g^{-1}$. Then $|h|$ is a 2-power, as otherwise $1 \neq h^a \in H_1$ for some a. Therefore, if t denotes the unique involution in H, we have that $t \in gN_C g^{-1}$ for each $g \in C_\sigma$. Hence $t \in \bigcap_{g\in C_\sigma} gN_C g^{-1} =: D$ and D is normal in C_σ. As $C \cong M(k, B)$ and as $\sigma|_B \neq \mathrm{Id}$, we have $C_\sigma \cong U(k, B)$. Since D contains t, we conclude that D contains a subgroup isomorphic to $SU(k, B)$. Clearly, $M \cap C$ is not central in C as otherwise D is abelian because $N/(N \cap M)$

is cyclic. In addition, N normalizes M, hence $N \cap C$ normalizes $M \cap C$ so that $M \cap C$ is normalized by $SU(k, B)$. If $k > 2$ then, by Lemma 3.10, it follows that $M \cap C = C$. Therefore $H_1 \subseteq B_\sigma \subseteq C_\sigma \subseteq M \cap G \subseteq N$, which is false. So we are left with $k = 2$.

Thus we have shown that if $H \cap gNg^{-1} \neq 1$ for all $g \in G$ then $k = 2$, $[B : F_2] = n$ and $SU(2, B) \cong SL(2, q)$ where $q = 2^n$. Observe that all involutions in $SL(2, q)$ are conjugate (as q is even) and so t normalizes some subgroup $Y \subseteq SU(2, B)$ of order $q - 1$. Set $E := H_1 Y$. Then E is cyclic as $|H_1|$ divides $q + 1$ and as H_1 is central in $C_\sigma \cong U(2, q)$. Clearly, Y stabilizes an isotropic 1-subspace of the natural $SU(2, B)$-module $\mathcal{M}$, so $C \cong M(2, B)$ contains non-trivial idempotents e_1, e_2 which centralize Y, and such that $\sigma(e_1) = e_2$ and $e_1 + e_2 = \mathrm{Id}$. (In $M(2, B)$ we have $Y = \{\mathrm{diag}(\alpha, \alpha^{-1})\}$ where $\alpha \in F_{q^2}$, $\alpha^{q-1} = 1$ and $e_1 = \mathrm{diag}(1, 0)$, $e_2 = \mathrm{diag}(0, 1)$ with respect to a Witt basis of $\mathcal{M}$.) Furthermore, e_1 and e_2 centralize H_1, and hence E. Therefore by (ii) there is some $g \in G$ such that $E \cap gNg^{-1} = 1$.

With this information for $k = 2$ we rearrange the argument above, assuming from the very beginning of (iii) that $C_G(H_1)$ contains a subgroup Y of order $q - 1$ such that $(H_1 Y) \cap N = 1$. Here also $H_1 \cap N = 1$ and so all of the above argument remains valid. However, now N_C cannot contain a subgroup isomorphic to $SU(2, q)$ as all subgroups of order $q - 1$ in $C_G(H_1) = U(2, B)$ are contained in $SU(2, q)$. So $Y \cap N = 1$ implies $N \cap SU(2, B) \neq SU(2, B)$. Therefore, there exists some $x \in SU(2, B)$ such that $t \notin x N_C x^{-1}$. Then $H \cap xNx^{-1} = 1$.

(iv) Here we assume that A contains an idempotent e such that $\sigma(e) = e$. We use induction on n and also on the order of H therefore assuming the theorem being true for all proper subgroups of H. Replacing e by $\mathrm{Id} - e$ we can assume that $|eH| \geqslant |(\mathrm{Id} - e)H|$ and we do this but one exception: if $|eH| = 5$ and $|(\mathrm{Id} - e)H| = 6$ or conversely, we prefer to have $|eH| = 5$.

Let H_2 be the kernel of $H \to eH$. Then $|H_2| < |H|$ as equality would mean that $eH = e$. By minimality of H there exists some $g \in G$ such that $H_2 \cap gNg^{-1} = 1$. Hence we can assume that $H_2 \cap N = 1$. Now it suffices to show that there is $x \in G$ such that $ex = x$ and $xeHx^{-1} \cap eNe = \mathrm{Id}$. To use induction here, we need eNe to normalize a proper non-central subring of eRe.

Set $C := eRe \cong M(r, 2)$ where $r := \mathrm{rank}(e)$, let $A_2 = (\mathrm{Id} - e)A$. As $e \in A$, clearly, $A_2 \subset A$ and $A = eA \oplus A_2$. Set $C_0 := C + A_2$. Clearly $eC_0 = C$ and $(1 - e)C_0 = A_2$. Hence C and A_2 are ideals of C_0, and $H \subseteq C_0$. Let $M_0 := M \cap C_0$ and so $H \cap M = H \cap M_0$. Observe that $M_0 \cap C \neq C$, for otherwise M_0 would contain a matrix of rank 1 and this is not the case. Moreover, $eM_0 \neq C$. Indeed, suppose to the contrary that $eM_0 = C$. By Lemma 3.13, we have $C \subseteq M_0$ and this contradicts $M_0 \cap C \neq C$.

Set $L := eM_0 \neq C$ and $N_0 = N \cap C_0 \cap G$. Then $eN_0 \neq e(C \cap G) =: C_\sigma$ as $eN_0 = C_\sigma$ implied that C_σ normalizes L. By Lemma 3.8 $C_\sigma = Sp(r, 2)$. As $r > 2$, by Lemma 3.11, L is central in C. Then eN_0 would be abelian (as $N' \subseteq M$), which is impossible. If $r \geqslant 4$ and $|eH| \neq 6$, we can use the induction assumption that Theorem 1.1 is true for $r < 2n$ to conclude that there exists some $h \in C_\sigma = Sp(r,2)$ such that $eH \cap heN_C h^{-1} = 1$, unless $r = 4$ and $eN_C = A_6$. In the latter situation, as A_6 is simple and eN_C normalizes L, by Lemma 3.11, we conclude that $L = C$. Let $r = 4$ and $|eH| = 6$. Then H is of exponent 6 by the above, hence of order 6 as it is cyclic. The group algebra F_2H has only one nontrivial idempotent. It follows that $|(\mathrm{Id} - e)H| \leqslant 2$. Then one can easily reduce the question to the case $n = 3$ and use [2]. (Alternatively, the case with $|H| = 6$ can be settled by using Lemma 4.2 below.)

(v) Let e be a minimal idempotent in A. By the above we are left with the situation when $\sigma(e) \neq e$ which implies that $\sigma(e)e = 0$. Then $e_1 := e + \sigma(e)$ is an idempotent of A and $\sigma(e_1) = e_1$. If $e_1 = \mathrm{Id}$ then the theorem is true by (ii), otherwise, it is true by (iv). □

4. The groups $U_3(q)$, ${}^2B_2(q)$, and ${}^2G_2(q)$

We turn to the permutation representations of the unitary groups $U_3(q)$, the Suzuki groups $Sz(q) = {}^2B_2(q)$ and the Ree groups $R(q) = {}^2G_2(q)$. First we note a fact that can be found in [7]:

Theorem 4.1. *None of the groups $U_3(q)$, ${}^2B_2(q)$, and ${}^2G_2(q)$ admits a non-trivial factorisation.*

It will therefore be sufficient to consider only the doubly transitive representations. It turns out that each case is a simple application of the following trivial lemma:

Lemma 4.2. *Let $H \subset G$ be finite groups. Let Ω be a G-set such that H has no regular orbit on Ω. Let $S_1, \ldots, S_m$ be the minimal non-trivial subgroups of H. Then $|\Omega| \leqslant \sum_{i=1}^m |\operatorname{fix}(S_i)|$.*

Proof. If $\alpha \in \Omega$ then $H_\alpha \neq 1$ and so α is fixed by some non-trivial minimal subgroup $S \subseteq H_\alpha$. □

The basic description of the unitary group $U_3(q) = PSU(3, q^2)$, with q some power of a prime p, is the following, see [3,5]. The group has one doubly transitive representation on $q^3 + 1$ points. The order is $(q^3 + 1)q^3(q^2 - 1)d^{-1}$ where $d = (q + 1, 3)$. The stabilizer B of a point is the normalizer of a Sylow p-subgroup S and B is a split extension of S by a cyclic group C. Clearly, C is the stabilizer of 2 points, of order $q^2 - 1$.

Theorem 4.3. *In the doubly transitive permutation action of $U_3(q)$ of degree $q^3 + 1$ with $q > 2$ every cyclic subgroup H has a regular orbit.*

Proof. Suppose the theorem is false and let $S_1, \dots, S_m \subseteq H$ be as in Lemma 4.2. Clearly, if p_i is the order of S_i then we may assume that p_1 divides q and $p_2, \dots, p_m$ divide $q^2 - 1$. Then S_1 fixes exactly one point and $\mathrm{fix}(S_i) \leqslant q + 1$ as can be seen from page 242 of [5]. As a rough estimate for m we may use $m \leqslant 1 + \ln(q^2 - 1)$. Lemma 4.2 now gives the contradiction $q^3 + 1 \leqslant 1 + \ln(q^2 - 1) \cdot (q + 1)$. $\square$

The basic description of the Suzuki group $Sz(q) = {}^2B_2(q)$ with $q = 2^{2m+1}$ taken from [3] is the following. The group acts doubly transitively on $q^2 + 1$ points such that the stabilizer of any three points is the identity. Its order is $(q^2 + 1)q^2(q - 1)$. The stabilizer B of one point is the normalizer of a Sylow 2-subgroup S and B is a split extension of S by a cyclic group C. In other words, B is a Frobenius group with kernel S and complement C which is the stabilizer of two points, of order $q - 1$.

Theorem 4.4. *In the doubly transitive permutation representation of $Sz(q)$ of degree $q^2 + 1$ with $q > 2$ every cyclic subgroup H has a regular orbit.*

Proof. Suppose the theorem is false and let $S_1, \dots, S_m \subseteq H$ be as in Lemma 4.2. Clearly, if p_i is the order of S_i then we may assume that $p_1 = 2$ and that $p_2, \dots, p_m$ divide $q - 1$. Then S_1 fixes exactly one point and $\mathrm{fix}(S_i) = 2$. We have, as before, $m \leqslant 1 + \ln(q - 1)$ and Lemma 4.2 gives the contradiction $q^2 + 1 \leqslant 1 + 2\ln(q - 1)$. $\square$

The Ree group $R(q) = {}^2G_2(q)$ with $q = 3^{2m+1}$ is doubly transitive on $q^3 + 1$ points, see again [3], and this is the only doubly transitive action. Its order is $(q^3 + 1)q^3(q - 1)$. The stabilizer B of one point is the normalizer of a Sylow 3-subgroup S and B is a split extension of S by a cyclic group C. Clearly, C is the stabilizer of 2 points, of order $q - 1$.

Theorem 4.5. *In the doubly transitive action of $R(q)$ of degree $q^3 + 1$ with $q > 3$ every cyclic subgroup H has a regular orbit.*

Proof. Suppose the theorem is false and let $S_1, \dots, S_m \subseteq H$ be as in Lemma 4.2. If p_i is the order of S_i then we may assume that $p_1 = 3$ and that $p_2, \dots, p_m$ divide $q - 1$. Then S_1 fixes exactly one point and $\mathrm{fix}(S_i) \leqslant 2q + 1$ as can be seen easily from page 251 in [3]. As $m \leqslant 1 + \ln(q - 1)$, Lemma 4.2 gives the contradiction $q^3 + 1 \leqslant 1 + \ln(q - 1) \cdot 2(q + 1)$. $\square$

5. Sporadic doubly transitive representations

Apart from the doubly transitive representations of $PSL(n,q)$, $Sp(2n,2)$, $U_3(q)$, ${}^2B_2(q)$, and ${}^2G_2(q)$ discussed in [8] and Sections 3 and 4 above, all other known permutation actions belong to a small list of sporadic examples:

(1) $PSL(2,11)$ of degree 11, two representations;
(2) $PSL(2,8)$ of degree 28;
(3) A_7 of degree 15, two representations;
(4) $PSL(2,11)$ of degree 11, two representations;
(5) M_{11} of degree 11;
(6) M_{11} of degree 12;
(7) M_{12} of degree 12, two representations;
(8) M_{22} of degree 22;
(9) M_{23} of degree 23;
(10) M_{24} of degree 24;
(11) HS of degree 176, two representations;
(12) Co_3 of degree 276.

Three of the first four groups have already been dealt with in [8, Theorem 1.1] and we may ignore A_7. To complete the proof of the main theorem it suffices therefore to look at the remaining cases:

Theorem 5.1. *Let G be any of the groups M_{11}, M_{12}, M_{22}, M_{23}, M_{24}, HS or Co_3 and let Ω be any non-trivial G-set. Then every cyclic subgroup $H \subset G$ has a regular orbit on Ω.*

Proof. This can be checked from the information given in the Atlas [2]. Elements of composite order $|H|$ involve at most two primes, say p and q, except in Co_3 which has elements of order 30. To verify the statement for the representations stated as items 5–12 in the list above it is sufficient to use Lemma 4.2 together with the fact that all pairs of p- and q-elements together fix an insufficient number of elements. The same argument applies for the elements of order 2, 3, and 5 in the Conway group. This completes the embedding case.

The factorizations of G are available in Table 6 of [7] and in the Atlas. In each case we are looking at a factorisation $G = G_\omega \cdot G_\delta$ where G_ω is the one-point-stabilizer in one of the presentions 5–12 in the list. We may make use of the comment following Theorem 2.2 earlier and so we have to consider only the following cases:

(1) For $G = M_{12}$ and $G_\omega = M_{11}$ we have $G_\delta = L_2(11)$, $G_\delta = 2 \times S_5$, $G_\delta = 4^2.D_{12}$ or $G_\delta = A_4 \times S_3$;
(2) For $G = M_{23}$ and $G_\omega = M_{22}$ we have $G_\delta = 23.11$;

(3) For $G = M_{24}$ and $G_\omega = M_{23}$ we have $G_\delta = M_{12}.2$, $G_\delta = 2^6.3.S_6$, $G_\delta = L_2(23)$, $G_\delta = 2^6(L_3(2) \times S_3)$ or $G_\delta = L_2(7)$;
(4) For $G = HS$ and $G_\omega = U_3(5).2$ we have $G_\delta = M_{22}$.

Now we repeat the same argument as before for the action of G on the cosets Δ of G_δ in G. In all cases where the character of G on Δ is given in the Atlas the Lemma 4.2 gives the result immediately. The remaining cases are

(1) $G = M_{12}$ with $G_\delta = A_4 \times S_3$ and $|\Delta| = 1320$;
(2) $G = M_{23}$ with $G_\delta = 23.11$ and $|\Delta| = 40320$;
(3) $G = M_{24}$ with $G_\delta = L_2(23)$ and $|\Delta| = 40320$, or with $G_\delta = L_2(7)$ and $|\Delta| = 1457280$.

These can be ruled out by easy character estimates. Let $\pi = 1 + n_1\chi_1 + \cdots + n_r\chi_r$ with $n_i > 0$ be the character of G on Δ. For $G = M_{12}$ we have to consider only elements of order $|H| = 6$. Here $\sum n_i \leqslant \frac{1320-1}{16}$ while the number of fixed points of 2- and 3-elements is $f_2 \leqslant 1 + 7\sum n_i$ and $f_3 \leqslant 1 + 3\sum n_i$. This contradicts $f_2 + f_3 \geqslant 1320$. For $G = M_{23}$ we have to consider elements of order $|H| = 6$, 14 or 15 but here all 2-, 3-, 5-, and 7-elements are fixed-point-free. For $G = M_{24}$ we have to consider elements of order $|H| = 6$, 10, 12, 14, 15 or 21. If $G_\delta = L_2(23)$ one may estimate $f_2 \leqslant 1 + 36\sum n_i$, $f_3 \leqslant 1 + 8\sum n_i$ and $f_5 = f_7 = 0$, thus contradicting Lemma 4.2. Finally, if $G_\delta = L_2(7)$ one has $f_2 \leqslant 1 + 36\sum n_i$, $f_3 \leqslant 1 + 16\sum n_i$ and $f_5 = 0$ and $f_7 \leqslant 1 + 4\sum n_i$. The result follows from Lemma 4.2 except for elements of order 6 where a slight variation of the same argument will work. □

References

[1] M. Aschbacher, On the maximal subgroups of the finite classical groups, Invent. Math. 76 (1984) 469–514.
[2] J. Conway, R. Curtis, R.A. Parker, R.M. Wilson, Atlas of Finite Simple Groups, Oxford University Press, London, 1985.
[3] J.D. Dixon, B. Mortimer, Permutation Groups, in: Graduate Texts in Math., Vol. 163, Springer-Verlag, Berlin, 1996.
[4] B. Huppert, Singer-Zyklen in klassischen Gruppen, Math. Z. 117 (1970) 141–150.
[5] B. Huppert, Endliche Gruppen, Springer-Verlag, Berlin, 1967.
[6] P. Kleidman, M.W. Liebeck, Subgroup Structure of Classical Groups, in: London Math. Soc. Lecture Notes, Vol. 129, Cambridge Univ. Press, Cambridge, 1990.
[7] M.W. Liebeck, C.E. Praeger, J. Saxl, The maximal factorizations of the finite simple groups and their automorphism groups, Mem. Amer. Math. Soc. 86 (1990) 151.
[8] J. Siemons, A. Zalesskii, Intersections of matrix algebras and permutation representations of $PSL(n,q)$, J. Algebra 226 (2000) 451–478.