THE UNIVERSITY OF WARWICK

Library Declaration and Deposit Agreement

1. **STUDENT DETAILS**

Please complete the following:

Full name: MATTHEW ASHLEY REYNOLDS

University ID number: 0321511

2. **THESIS DEPOSIT**

2.1 I understand that under my registration at the University, I am required to deposit my thesis with the University in BOTH hard copy and in digital format. The digital version should normally be saved as a single pdf file.

2.2 The hard copy will be housed in the University Library. The digital version will be deposited in the University's Institutional Repository (WRAP). Unless otherwise indicated (see 2.3 below) this will be made openly accessible on the Internet and will be supplied to the British Library to be made available online via its Electronic Theses Online Service (EThOS) service.
[At present, theses submitted for a Master's degree by Research (MA, MSc, LLM, MS or MMedSci) are not being deposited in WRAP and not being made available via EthOS. This may change in future.]

2.3 In exceptional circumstances, the Chair of the Board of Graduate Studies may grant permission for an embargo to be placed on public access to the hard copy thesis for a limited period. It is also possible to apply separately for an embargo on the digital version. (Further information is available in the *Guide to Examinations for Higher Degrees by Research*.)

2.4 *If you are depositing a thesis for a Master's degree by Research, please complete section (a) below. For all other research degrees, please complete both sections (a) and (b) below:*

(a) Hard Copy

I hereby deposit a hard copy of my thesis in the University Library to be made publicly available to readers (please delete as appropriate) EITHER immediately ~~OR after an embargo period of .... months/years as agreed by the Chair of the Board of Graduate Studies~~.

I agree that my thesis may be photocopied. YES / ~~NO~~ *(Please delete as appropriate)*

(b) Digital Copy

I hereby deposit a digital copy of my thesis to be held in WRAP and made available via EThOS.

Please choose one of the following options:

✓ EITHER My thesis can be made publicly available online. YES / ~~NO~~ *(Please delete as appropriate)*

OR My thesis can be made publicly available only after.....[date] (Please give date)
YES / NO *(Please delete as appropriate)*

OR My full thesis cannot be made publicly available online but I am submitting a separately identified additional, abridged version that can be made available online.
YES / NO *(Please delete as appropriate)*

OR My thesis cannot be made publicly available online. YES / NO *(Please delete as appropriate)*

JHG 05/2011

3. GRANTING OF NON-EXCLUSIVE RIGHTS

Whether I deposit my Work personally or through an assistant or other agent, I agree to the following:

Rights granted to the University of Warwick and the British Library and the user of the thesis through this agreement are non-exclusive. I retain all rights in the thesis in its present version or future versions. I agree that the institutional repository administrators and the British Library or their agents may, without changing content, digitise and migrate the thesis to any medium or format for the purpose of future preservation and accessibility.

4. DECLARATIONS

(a) I DECLARE THAT:

- I am the author and owner of the copyright in the thesis and/or I have the authority of the authors and owners of the copyright in the thesis to make this agreement. Reproduction of any part of this thesis for teaching or in academic or other forms of publication is subject to the normal limitations on the use of copyrighted materials and to the proper and full acknowledgement of its source.

- The digital version of the thesis I am supplying is the same version as the final, hard-bound copy submitted in completion of my degree, once any minor corrections have been completed.

- I have exercised reasonable care to ensure that the thesis is original, and does not to the best of my knowledge break any UK law or other Intellectual Property Right, or contain any confidential material.

- I understand that, through the medium of the Internet, files will be available to automated agents, and may be searched and copied by, for example, text mining and plagiarism detection software.

(b) IF I HAVE AGREED (in Section 2 above) TO MAKE MY THESIS PUBLICLY AVAILABLE DIGITALLY, I ALSO DECLARE THAT:

- I grant the University of Warwick and the British Library a licence to make available on the Internet the thesis in digitised format through the Institutional Repository and through the British Library via the EThOS service.

- If my thesis does include any substantial subsidiary material owned by third-party copyright holders, I have sought and obtained permission to include it in any version of my thesis available in digital format and that this permission encompasses the rights that I have granted to the University of Warwick and to the British Library.

5. LEGAL INFRINGEMENTS

I understand that neither the University of Warwick nor the British Library have any obligation to take legal action on behalf of myself, or other rights holders, in the event of infringement of intellectual property rights, breach of contract or of any other right, in the thesis.

Please sign this agreement and return it to the Graduate School Office when you submit your thesis.

Student's signature: M. Reynolds .... Date: 12 . 04 . 13 ....

Signalizers in Groups of Lie Type

by

Matthew Reynolds

Thesis

Submitted to The University of Warwick

for the degree of

Doctor of Philosophy

Mathematics Institute

March, 2013

THE UNIVERSITY OF
WARWICK

Contents

Acknowledgments

All good things come from God. All that is good in this thesis comes from God, whilst all shortcomings are mine!

Throughout the PhD process, I was supported by many friends at Warwick and beyond, who all deserve great thanks but are far too many to list here. I owe enormous thanks to my supervisor, Dr. Inna Capdeboscq, for patiently reading numerous versions of this work and offering invaluable advice and support. Completing this thesis would not have been possible without the love and encouragement of my Mum and Dad and my sister Anna. Above all, thank you to Noelia, for her constant love, patience and kindness as we both negotiated the PhD process.

This work was supported by EPSRC.

Declaration

The author declares that the material contained in this thesis is entirely his own work. As is standard practice, the subject matter developed builds on existing theory, and clear citations and references are provided where necessary.

Although material contained herein may be submitted for publication at a later date, the author has not published any work which forms part of this thesis.

No part of this thesis has been submitted, for the purposes of a degree or otherwise, to any other university or educational institution.

Abstract

We classify all $C_G(t)$-signalizers, where G is a finite group of Lie type and t is an automorphism of G of prime order $s > 3$. Our results extend existing work by Korchagina ([Ko], [Ko2]).

Notation

Throughout this work, we adopt the following notation. Let G and H be finite groups, let m and n be integers and let p be a prime.

$H \circ G$	Central product of H and G
$H.G$	Extension of H by G
$H : G$	Split extension of H by G
$\frac{1}{n}G$	Normal subgroup of index n in G
n or C_n	Cyclic group of order n
p^n or E_{p^n}	Elementary abelian group of order p^n
p^{n+m}	Extension of p^n by p^m
$[n]$	Arbitrary group of order n
$Z(G)$	Center of G
$G^{\#}$	Set of nonidentity elements of G
$m_p(G)$	p-rank of G
$^\wedge H$	For $H \leq G$, the homomorphic image of H in $G/Z(G)$
(m, n)	Greatest common divisor of m and n

Chapter 1

Introduction

1.1 Motivation

In the articles *2-signalizers in almost simple groups* [Ko2] and *3-signalizers in almost simple groups* [Ko], Korchagina classifies the 2 and 3-signalizers that occur in the finite simple $\mathscr{K}$-groups. The result is relevant to the revised proof of the Classification Theorem of Finite Simple Groups. We aim to extend this work by classifying s-signalizers in Groups of Lie Type, where s will be an odd prime greater than 3. Thus, the objects we wish to study are the following.

Definition 1.1. *Fix a prime s. Let G be a finite group, take $t \in Aut(G)$ of order s, and X a p-subgroup of G with p prime and $p \neq s$. Suppose that*

(i) $[X, t] = X$*,*

(ii) $C_G(t) \leq N_G(X)$

Then we say (G, t, X) is a triple of type (Hs), and we call X a $C_G(t)$-signalizer.

We wish to classify triples (G, t, X) of type (Hs) for $G \in Lie(r)$ and $s > 3$. We will show below, in Lemma 2.15, it suffices to consider the cases of t being inner-diagonal and t being a field automorphism.

1.2 Statement of Results

We are now ready to state the main result of this thesis.

Theorem 1.2. *Let $G \in Lie(r)$. Suppose that G admits a nontrivial automorphism t of order s, where s is a prime greater than 3. Suppose that X is a $C_G(t)$-signalizer. Then either $X = 1$ or one of the following holds.*

(1) $r \neq s$, $p = r$, $t \in Inndiag(G)$ and there exists a parabolic subgroup $P \leq G$ such that X is contained in the unipotent radical $O_r(P)$ of P, $C_G(t) \leq P$, $C_G(t) \cap O_r(P) = 1$ and $C_G(t)$ is isomorphic to a subgroup of a Levi complement L of P,

(2) $G \cong SU_4(3)$, $t \in Inn(G)$, $s = 5$, $p = 2$, $C_G(t) \cong C_4 \times C_5$ and $X \cong 2_-^{1+4}$,

(3) G is isomorphic to a quotient of $SU_4(3)$ by its central subgroup of order 2, $s = 5$, $C_G(t) \cong C_2 \times C_5$ and $X \cong E_{2^4}$.

(4) $G \cong PSU_4(3)$, $t \in Inn(G)$, $s = 5$, $p = 2$, $C_G(t) \cong C_5$ and $X \cong E_{2^4}$,

(5) $G \cong Sp_{2m}(3)$ (for $m \geq 2$), $t \in Inn(G)$, $s = 5$, $p = 2$, $C_G(t) \cong Sp_{2m-4}(3) \times C_2 \times C_5$ and $X \cong 2_-^{1+4}$,

(6) $G \cong PSp_{2m}(3)$ (for $m \geq 3$), $t \in Inn(G)$, $s = 5$, $p = 2$, $C_G(t) \cong Sp_{2m-4}(3) \times C_5$ and $X \cong 2_-^{1+4}$

(7) $G \cong PSp_4(3)$, $t \in Inn(G)$, $s = 5$, $p = 2$, $C_G(t) \cong C_5$ and $X \cong E_{2^4}$,

(8) $G \cong G_2(3)$, $t \in Inn(G)$, $s = 7$, $p = 2$, $C_G(t) \cong C_7$ and $X \cong E_{2^3}$,

(9) $G \cong {}^2G_2(3)$, $t \in Inn(G)$, $s = 7$, $p = 2$, $C_G(t) \cong C_7$ and $X \cong E_{2^3}$,

(10) $G \cong F_4(2)$, $t \in Inn(G)$, $s = 13$, $p = 3$, $C_G(t) \cong C_{13}$ and $X \cong E_{3^3}$,

(11) $G \cong {}^2E_6(2)$, $t \in Inn(G)$, $s = 13$, $p = 3$, $C_G(t) \cong C_{13}$ and $X \cong E_{3^3}$,

(12) $G \cong {}^2E_6(2)$, $t \in Inn(G)$, $s = 13$, $p = 3$, $C_G(t) \cong C_{13}$ and $X \cong 3^{3+3}$,

(13) $G \cong A_1(2^s)$, t is a field automorphism whose order s divides $p - 1$, $C_G(t) \cong A_1(2)$, 3 divides $2^s + 1$ and X is a cyclic group whose order p^n also divides $2^s + 1$,

(14) $G \cong {}^2B_2(2^s)$, t is a field automorphism whose order s divides $p - 1$, $C_G(t) \cong {}^2B_2(2)$, 5 divides one of $2^s \pm 2^{(s+1)/2} + 1$ and X is a cyclic group whose order p^n also divides $2^s \pm 2^{(s+1)/2} + 1$.

Furthermore, the triples (G, t, X) given in (1)-(14) do indeed exist.

1.3 Structure of Argument

We will prove Theorem 1.2 as follows. Chapter 2 introduces the necessary background group theory, paying particular attention to the finite groups of Lie type. Chapter 3 is concerned with preliminary results addressing the possibility that the characteristic r of G is equal to the order s of t. The main result of Chapter 3 is that all such $C_G(t)$-signalizers are trivial. Thus we divide the remainder of the proof into 2 cases; the case $p = r$ and the case $p \neq r$. Chapter 4 discusses the former case and shows that signalizers with $p = r$ display the uniform behaviour described in Theorem 1.2 (1). Thereafter we begin the analysis in the totally 'coprime' case $r \neq p \neq s$. We divide the proof of this case into the subcases in which t is either an inner-diagonal or a field automorphism. Chapter 5 deals with the former case using inductive arguments on $rank(G)$, whilst Chapter 6 deals with the field automorphisms and concludes the proof.

Chapter 2

Group Theoretic Background

2.1 The Finite Groups Of Lie Type

We dedicate this section to a brief introduction to the main objects of study - the finite groups of Lie type. Our treatment agrees with [GLS3] and with Section 5.1 [KL].

2.1.1 Definitions and Preliminaries

In this section we take it as understood that for an algebraically closed field $\overline{\mathbb{F}}_p$ of characteristic p, an $\overline{\mathbb{F}}_p$-*algebraic group* is a closed subgroup $\overline{K}$ of $GL_n(\overline{\mathbb{F}}_p)$, for some n, with respect to the *Zariski topology* on $GL_n(\overline{\mathbb{F}}_p)$ (the topology given by the condition that the closed sets are the solution sets of systems of polynomial equations in the matrix entries and the function $d : A \to det(A)^{-1}$). Further, a connected algebraic group $\overline{K}$ is said to be *semisimple* if $R(\overline{K}) = 1$, where $R(\overline{K})$ is the *radical* of $\overline{K}$, that is the largest normal subgroup of $\overline{K}$ that is closed, connected (with respect to the topology inherited from $GL_n(\overline{\mathbb{F}}_p)$) and solvable; and $\overline{K}$ is said to be *simple* if $[\overline{K}, \overline{K}] \neq 1$ and the only proper closed normal subgroups of $\overline{K}$ are finite (cf Definition 1.7.1 and Proposition 1.1.6 (b) [GLS3]). Accepting these definitions we may now define our main objects of study, the Finite Groups of Lie type.

Definition 2.1. *(1) If K is a finite group, then a σ-setup for K over $\overline{\mathbb{F}}_p$ (an algebraically closed field of characteristic p) is a pair $(\overline{K}, \sigma)$ such that*

- *$\overline{K}$ is a semisimple algebraic group over $\overline{\mathbb{F}}_p$,*
- *σ is a Steinberg endomorphism of $\overline{K}$ (a surjective endomorphism of $\overline{K}$ such that $C_{\overline{K}}(\sigma)$ is finite),*
- *K is isomorphic to $O^{p'}(C_{\overline{K}}(\sigma))$, the subgroup of $C_{\overline{K}}(\sigma)$ generated by its p-elements.*

(2) A finite group of Lie type in characteristic p is a finite group K possessing a σ-setup $(\overline{K}, \sigma)$ over $\overline{\mathbb{F}}_p$ such that $\overline{K}$ is simple.

We now record an alternative description of Steinberg endomorphisms that clarifies the definition of the finite groups of Lie type. This appears as Definition 2.1.9 and Theorem 2.1.11 [GLS3].

Definition 2.2. *Let q be a power of p. For $x \in GL_n(\overline{\mathbb{F}}_p)$, write $x^{(q)}$ for the matrix obtained by raising each entry of x to the power q, and let $\sigma_q(x) = x^{(q)}$ for all x.*

*An endomorphism σ of an algebraic group $\overline{K}$ is called a **Frobenius endomorphism** if there is a power $\tau = \sigma^m$ of σ, a power q of p and an algebraic group identification of $\overline{K}$ with a closed subgroup of $GL_n(\overline{\mathbb{F}}_p)$ for some n, such that $\tau = \sigma_q|\overline{K}$. In this case, we say that σ has **level** $q^{1/m}$.*

Theorem 2.3. *Let $\overline{K}$ be an algebraic group. If σ is a Frobenius endomorphism of $\overline{K}$ then σ is a Steinberg endomorphism. Conversely, if σ is a Steinberg endomorphism and $\overline{K}$ is simple, then σ is a Frobenius endomorphism.*

Now Definition 2.1 (2) and Theorem 2.3 show that, roughly speaking, a finite group of Lie type is a subgroup of fixed points of a Frobenius endomorphism of a simple algebraic group. Thus a classification of the finite groups of Lie type follows from the classification of simple algebraic groups. The classification of simple algebraic groups is achieved by means of classifying irreducible *Root systems* (Theorem 1.10.4 [GLS3]). We pause now to briefly discuss this concept.

Definition 2.4. *(1) A **Root System** is a nonempty subset Σ of nonzero vectors in a Euclidean Space V with inner product $(\ ,\ )$, such that the following hold.*

- *Σ spans V;*
- *If $r, s \in \Sigma$, then $s - \frac{2(r,s)}{(r,r)} r \in \Sigma$;*
- *If $r, s \in \Sigma$, then $\frac{2(r,s)}{(r,r)} \in \mathbb{Z}$;*
- *If $r, \lambda \cdot r \in \Sigma$ then $\lambda = \pm 1$.*

*(2) A **Fundamental System** Π for Σ is a linearly independent subset of Σ such that every element of Σ can be expressed as a linear combination of elements of Π with coefficients that are either all positive or all negative.*

*(3) A root system Σ is said to be **irreducible** if it admits no partition into mutually orthogonal subsets.*

Now irreducible root systems are classified (up to isomorphism, which we do not discuss here) by Theorem 1.8.7 [GLS3]. Each irreducible root system Σ has a label Σ_l, where l denotes the dimension of the span of Σ. A list of irreducible root systems is: A_m $(m \geq 1)$, B_m $(m \geq 1)$, C_m $(m \geq 1)$, D_m $(m \geq 3)$, E_m $(m = 6, 7, 8)$, F_4, G_2. Among these, we have equalities $A_1 = B_1 = C_1$, and $D_3 = A_3$.

To each simple algebraic group $\overline{G}$ we may associate one of the above irreducible root systems. For each root $\alpha \in \Sigma$ there exists a *root subgroup* X_α, which is parametrised by $\overline{\mathbb{F}}_p$ so that one may write $X_\alpha = \langle x_\alpha(t) : t \in \overline{\mathbb{F}}_p \rangle$. By Theorem 1.10.1 (a) [GLS3], the root subgroups generate $\overline{G}$.

This association gives rise to certain isomorphisms of $\overline{G}$. If ρ is an isometry of the fundamental system Π, then, by Theorem 1.15.2 (a) [GLS3], there is an automorphism γ_ρ such that $\gamma_\rho(x_\alpha(t)) = x_{\rho(\alpha)}(t)$ for all $\alpha \in \pm\Pi$ and all $t \in \overline{\mathbb{F}}_p$. Furthermore, if $\Sigma = B_2$, F_4 or G_2 with $p = 2, 2, 3$ respectively, then by Theorem 1.15.4 (b) [GLS3], there is an angle preserving and length changing bijection $\rho : \Sigma \to \Sigma$, and an automorphism ψ of $\overline{G}$ such that $\psi(x_\alpha(t)) = x_{\rho(\alpha)}(t)$ or $\psi(x_\alpha(t)) = x_{\rho(\alpha)}(t^p)$, depending on whether α is a *long* or *short* root (in the sense that in the fundamental systems for B_2 and G_2, one element has greater length than the other, and in the fundamental system for F_4 there are two longer roots and two shorter roots).

Now if we have a σ-setup $(\overline{K}, \sigma)$, then, by Theorem 2.2.3 [GLS3], we may assume that one of the following situations holds.

(1) $\sigma = \gamma_\rho \varphi_q$ (where $\varphi_q(x_\alpha(t)) = x_\alpha(t^q)$), for some power $q = p^a$ of p. In this case, σ has level q.

(2) $\sigma = \psi \varphi_q$ for some power $q = p^a$ of p. In this case σ has level $p^{a+\frac{1}{2}}$.

The finite groups of Lie type may thus be classified as follows.

- The *untwisted groups of Lie type*: $A_m(q)$, $B_m(q)$ $(m \geq 2)$, $C_m(q)$ $(m \geq 2)$, $D_m(q)$ $(m \geq 3)$, $G_2(q)$, $F_4(q)$, $E_6(q)$, $E_7(q)$, $E_8(q)$ arise from case (1) above, taking ρ to be trivial.
- The *Steinberg (or twisted) groups*: ${}^2A_m(q)$ $(m > 1)$, ${}^2D_m(q)$ $(m \geq 3)$, ${}^3D_4(q)$, ${}^2E_6(q)$ arise from case (1) above with ρ having order $d > 1$.
- The *Suzuki-Ree groups*: ${}^2B_2(2^{2a+1})$, ${}^2F_4(2^{2a+1})$, ${}^2G_2(3^{2a+1})$ arise from case (2) above.

So the finite groups of Lie type are indexed by the symbols ${}^d\Sigma_l(q)$ where Σ_l is an irreducible root system, d is the order of ρ, and q is the level of σ, a power of p. We may now make the following crucial definition.

Definition 2.5. *Let* $G = {}^d\Sigma_l(q)$ *be a finite group of Lie type. Then the* ***(Untwisted) Rank*** *of* G*, written* $rank(G)$ *is*

$$rank(G) = l = dim(Span(\Sigma)).$$

This list of finite groups of Lie type above is also subject to the additional complication that each symbol ${}^d\Sigma_l(q)$ can represent more than one nonisomorphic group (*version*). By Theorem 2.2.6 (a) [GLS3], for each symbol $K = {}^d\Sigma(q)$, there is up to isomorphism a unique largest group K_u (called the *universal* version) and a unique smallest group K_a (called the *adjoint* version). In some cases these are the same, but for the symbols $A_m(q)$, $B_m(q)$, $C_m(q)$, $D_m(q)$, $E_6(q)$, $E_7(q)$, ${}^2A_m(q)$, ${}^2D_m(q)$ and ${}^2E_6(q)$ we must always specify which version we are talking about. In all cases we have the following helpful result, which is parts (b) and (c) of Theorem 2.2.6 [GLS3].

Theorem 2.6. *For any version* K *of a symbol* ${}^d\Sigma_l(q)$*, there are surjective homomorphisms* $K_u \to K \to K_a$ *whose kernels are central. In particular if* K *is simple, then* $K \cong K_a$*. Furthermore,* $Z(K_a) = 1$ *and* $K/Z(K) \cong K_u/Z(K_u) \cong K_a$*.*

We conclude this section with a description of the simple groups of Lie type, which is exactly Theorem 2.2.7 (a) [GLS3].

Theorem 2.7. *Let* K *be a finite group of Lie type. If* K *is adjoint, then* K *is a nonabelian simple group with the following exceptions:* $K = A_1(2)$*,* $A_1(3)$*,* ${}^2A_2(2)$*,* ${}^2B_2(2)$*,* $B_2(2)$*,* $G_2(2)$*,* ${}^2F_4(2)$*,* ${}^2G_2(3)$*. The first four of these are Frobenius groups of respective orders* $3{\cdot}2$*,* $4{\cdot}3$*,* $9{\cdot}8$ *and* $5{\cdot}4$*, and for each of the last four, there is a unique proper normal subgroup, namely the commutator subgroup* $[K, K]$*, which is nonabelian simple with* $|K : [K, K]| = p$*.*

2.1.2 Identifications with some Classical Groups

The symbols $A_m(q)$, ${}^2A_m(q)$, $B_m(q)$, $C_m(q)$, $D_m(q)$ and ${}^2D_m(q)$ are naturally identified with certain classical matrix groups, as follows (compare section 2.7 [GLS3]).

- $A_m(q)$ has universal version isomorphic to the special linear group $SL_{m+1}(q)$ and adjoint version isomorphic to the projective special linear group $PSL_{m+1}(q)$;
- The twisted group ${}^2A_m(q)$ has universal and adjoint versions isomorphic to the unitary and projective unitary groups $SU_{m+1}(q)$ and $PSU_{m+1}(q)$ respectively;
- $B_m(q)$ has adjoint version isomorphic to the $(2m + 1)$-dimensional orthogonal group $\Omega_{2m+1}(q)$;
- $C_m(q)$ has universal and adjoint versions isomorphic to the symplectic and projective symplectic groups $Sp_{2m}(q)$ and $PSp_{2m}(q)$ respectively;

- $D_m(q)$ has adjoint version isomorphic to the $2m$-dimensional projective orthogonal group $P\Omega_{2m}(q)$;
- The twisted group ${}^2D_m(q)$ has adjoint version isomorphic to the $2m$-dimensional orthogonal group $P\Omega^-_{2m}(q)$.

Henceforth we regard the groups $A_m(q)$, ${}^2A_m(q)$, $B_m(q)$, $C_m(q)$, $D_m(q)$ and ${}^2D_m(q)$ as *Classical Groups of Lie type* and the remaining groups of Lie type as *Exceptional Groups of Lie type.*

We will adopt the following standard notation for discussing classical groups.

Notation 2.8. *We sometimes write $A^{\pm}_l(q) = (P)SL^{\pm}_{l+1}(q)$ to refer to $A_l(q) = (P)SL_{l+1}(q)$ and ${}^2A_l(q) = (P)SU_{l+1}(q)$ respectively.*

We pause here to state a very useful result on the Sylow subgroups of $PSL_2(q)$. This can be found as Chapter 5, Lemma 1.1 [G].

Lemma 2.9. *Let $G = PSL_2(q)$, with $q = r^a$, r a prime. Then we have*

(a) A Sylow r-subgroup R of G is elementary abelian of order r^a, R is disjoint from its conjugates and $N_G(R)$ is a Frobenius group with a cyclic complement which acts irreducibly on R;

(b) If p is a prime distinct from r or 2, then a Sylow p-subgroup of G is cyclic;

(c) If r is odd, then a Sylow 2-subgroup of G is dihedral and has order 4 if and only if $q \equiv 3, 5 \mod 8$;

(d) If Q is a nontrivial subgroup of G of odd prime power order, then $N_G(Q)$ does not contain a subgroup isomorphic to A_4.

We close this section by defining some important subgroups of certain classical groups.

Definition 2.10. *A **Singer cyclic subgroup** of $GL_n(q)$ is a cyclic subgroup of $GL_n(q)$ of order $q^n - 1$.*

A Singer cyclic subgroup of $SL_n(q)$ is a cyclic subgroup of $SL_n(q)$ of order $\frac{q^n-1}{q-1}$.

A Singer cyclic subgroup of $GU_n(q)$ (for n odd) is a cyclic subgroup of $GU_n(q)$ of order $q^n + 1$.

A Singer cyclic subgroup of $SU_n(q)$ (for n odd) is a cyclic subgroup of $SU_n(q)$ of order $\frac{q^n+1}{q+1}$.

A Singer cyclic subgroup of $Sp_{2n}(q)$ is a cyclic subgroup of $Sp_{2n}(q)$ of order $q^n + 1$.

A Singer cyclic subgroup of $GO^-_{2n}(q)$ is a cyclic subgroup of $GO^-_{2n}(q)$ of order $q^n + 1$.

A Singer cyclic subgroup of $SO^-_{2n}(q)$ is a cyclic subgroup of $SO^-_{2n}(q)$ of order q^n+1.

A Singer cyclic subgroup of $\Omega^-_{2n}(q)$ is a cyclic subgroup of $Sp_{2n}(q)$ of order $(q^n{+}1)/(2,q{+}1)$.

All such subgroups exist by Table 1 [B].

2.1.3 Automorphisms

We now describe the automorphism groups of the finite groups of Lie type. We begin by recording a definition from [GLS3].

Definition 2.11. *(1) Let $\overline{\mathbb{F}}_p$ be an algebraically closed field of characteristic p. A* ***Torus*** *is an algebraic group which is isomorphic, as an algebraic group, to the direct product of finitely many copies of $GL_1(\overline{\mathbb{F}}_p)$. A* ***subtorus*** *of an algebraic group $\overline{K}$ is a closed subgroup of $\overline{K}$ which is a torus. A* ***maximal torus*** *of $\overline{K}$ is a subtorus of $\overline{K}$ not contained in any other subtorus of $\overline{K}$.*

(2) Let $(\overline{K},\sigma)$ be a sigma setup for the finite group of Lie type K. Then a maximal torus of K is a subgroup of K of the form $\overline{T}\cap K$, where $\overline{T}$ is a maximal torus of $\overline{K}$.

We now follow Theorem 2.5.1 [GLS3] to describe the automorphism groups.

Theorem 2.12. *Let K be a group of Lie type over $\mathbb{F}_q$, where $q=r^a$, and let $(\overline{K},\sigma)$ be a σ-setup for K. Then every automorphism of K is a product $idfg$, where*

(a) $i\in Inn(K)$,

(b) d is a 'diagonal automorphism' of K, that is d is induced by conjugation by an element $h\in N_{\overline{T}}(K)$, where $\overline{T}$ is a maximal torus of $\overline{K}$,

(c) f is a 'field automorphism' of K, that is f arises from an automorphism φ of $\mathbb{F}_q$ and takes each $x_\alpha(t)$ to $x_\alpha(\varphi(t))$,

(d) g is a 'graph automorphism' of K, that is $g=1$ unless K is untwisted, and one of the following holds.

- *Σ has one root length and for some isometry ρ of Σ carrying Π to Π, g takes each $x_\alpha(t)$ to $x_{\rho(\alpha)}(\epsilon_\alpha\cdot t)$, where the ϵ_α are signs, and $\epsilon_\alpha=1$ when $\pm\alpha\in\Pi$, or*
- *$\Sigma=B_2$, F_4 or G_2 with $r=2$, 2, 3 respectively and g takes $x_\alpha(t)$ to $x_{\rho(\alpha)}(t)$ if α is long, and $x_\alpha(t)$ to $x_{\rho(\alpha)}(t^r)$ if α is short, where ρ is the unique angle-preserving and length changing bijection from Σ to Σ carrying Π to Π.*

The following lemma gives us some extra information on inner-diagonal and graph automorphisms that will be useful in what follows. It may be obtained by combining Theorem 2.5.14 [GLS3] and Lemma 4.1.1 [GLS3].

Lemma 2.13. *Let $K \in Lie(r)$ and let $x \in Aut(K)$ be an inner-diagonal or graph automorphism of prime order $r_1 \neq r$. The there exists a σ-setup $(\overline{K}, \sigma)$ of K and overlinex $\in Aut_0(\overline{K})$ (the group of automorphisms of $\overline{K}$ as an algebraic group) commuting with σ such that $\overline{x}$ induces x on K. Moreover, in this case $\overline{x}$ is unique and has order r_1.*

Remark 2.14. *We remark that inner-diagonal automorphisms of a group K of Lie type are further divided into two types, so-called **equal rank type** and **parabolic type**. Roughly speaking, if $\overline{x}$ is an automorphism of the algebraic group $\overline{K}$ which induces x on K as in Lemma 2.13, then x having equal rank type means that the Dynkin diagram of $[C_{\overline{K}}(\overline{x})^0, C_{\overline{K}}(\overline{x})^0]$ has the same number of nodes as that of $\overline{K}$. If x has parabolic type this means that the Dynkin diagram of $[C_{\overline{K}}(\overline{x})^0, C_{\overline{K}}(\overline{x})^0]$ has fewer nodes than that of $\overline{K}$ (see Definition 4.1.8 [GLS3]).*

We close this section with some observations that limit the possibilities for automorphisms of prime order $s > 3$.

Lemma 2.15. *Let $K \in Lie(r)$ and let t be an automorphism of prime order s, where $s \neq r$ and $s > 3$. Then either t is inner-diagonal (a product of an inner automorphism and a diagonal automorphism) or t is conjugate to a field automorphism.*

Proof. By Lemma 2.12, t is a product ifg, where i is inner-diagonal, f is a field automorphism and g is a graph automorphism. In fact, by Theorem 2.5.12 [GLS3], $Aut(K)$ is a split extension of the group $Inndiag(K)$ of inner-diagonal automorphisms by the group $\Phi_K \Gamma_K$ generated by the graph and field automorphisms. Since t has order s we have $(ifg)^s = t^s = 1$. If $g \neq 1$, then since it is a graph automorphism, it has order divisible by 2 or 3. This is a contradiction and so $g = 1$. Hence $(if)^s = 1$ This can be rewritten as

$$i(fif^{-1})(f^2if^{-2})...(f^{s-1}if^{-(s-1)})f^s = 1$$

Moving the last f^s over to the other side gives

$$i(fif^{-1})(f^2if^{-2})...(f^{s-1}if^{-(s-1)}) = f^{-s}$$

Now the left-hand side of this equation is contained in $Inndiag(K)$ whilst the right-hand side is in Φ_K. Since $Inndiag(K)$ and Φ_K intersect trivially, each side is in fact trivial. In particular, $f^s = 1$. If $f = 1$, then $t = i$ and so t is inner-diagonal as required. So assume $f \neq 1$. Then certainly $t \in Inndiag(K)f$. So we are in the conditions of Proposition 4.9.1 (d) [GLS3], which asserts exactly that t is $Inndiag(K)$-conjugate to f. $\square$

Lemma 2.15 tells us that we may divide our analysis into two cases, that of t being inner-diagonal or of t being a field automorphism. Theorem 2.5.12 (c) [GLS3] will simplify our analysis even further by giving the order of $Outdiag(K) := Inndiag(K)/Inn(K)$. We record this result below.

Lemma 2.16. *Let K be a group of Lie type. Then the order of $O := Outdiag(K)$ is given in the following table (or is 1 if K does not appear in the table).*

K	$A_m^{\pm}(q)$	$B_m(q)$,$C_m(q)$,$D_{2m}^{-}(q)$	$D_{2m}(q)$	$D_{2m+1}^{\pm}(q)$	$E_6^{\pm}(q)$	$E_7(q)$
$\lvert O\rvert$	$(m+1, q \mp 1)$	$(2, q-1)$	$(2, q-1)^2$	$(4, q \mp 1)$	$(3, q \mp 1)$	$(2, q-1)$

2.2 Further Background Information

In this section we introduce two topics that need to be understood for the analysis to follow.

2.2.1 The Frattini Subgroup

The first topic to address in this section is that of a very important characteristic subgroup of a finite group G, namely the *Frattini Subgroup* $\Phi(G)$.

Definition 2.17. *Let G be a finite group. The **Frattini Subgroup** $\Phi(G)$ of G is the intersection of all the maximal subgroups of G.*

The following Lemma is part of Lemma 3.15 [GLS2].

Lemma 2.18. *Let X be a finite group and $N \triangleleft X$. Then $\Phi(N) \leq \Phi(X)$.*

We will mainly work with the Frattini subgroup $\Phi(G)$ in the context where G is a p-group. We therefore introduce a standard Lemma, which can be found as Chapter 5, Theorems 1.3 and 1.4 [G] to this end.

Lemma 2.19. *Let P be a finite p-group.*

(i) The Frattini factor group $P/\Phi(P)$ is elementary abelian;

(ii) $\Phi(P) = 1$ if and only if P is elementary abelian;

(iii) If ϕ is a p'-automorphism of P inducing the identity on $P/\Phi(P)$, then ϕ is the identity automorphism of P.

2.2.2 Extra-Special Groups

We are now in a position to discuss a very important class of groups known as *Extra-Special Groups*. Our treatment follows [GLS2].

Definition 2.20. *The p-group P is called **special** if either P is elementary abelian or P is nonabelian with $Z(P) = \Phi(P) = [P,P]$ elementary abelian; and P is called **extra-special** if P is nonabelian, special and $|Z(P)| = p$.*

The extra-special groups are well-understood and we now list some standard results about them, beginning with the following structure theorem, Proposition 10.4 [GLS2].

Theorem 2.21. *Any nonabelian group of order p^3 is extra-special. Conversely, if p is extra-special, then the following conditions hold for some integer n.*

(i) P is a central product of extra-special groups P_1, P_2, ... ,P_n of order p^3;

(ii) $P/Z(P) \cong E_{p^{2n}}$;

(iii) If $|P| = p^3$, then either $p = 2$ and $P \cong D_8$ or Q_8; or p is odd, P has exponent p or p^2 and P is uniquely determined up to isomorphism by its exponent;

(iv) $D_8 \circ D_8 \cong Q_8 \circ Q_8 \ncong D_8 \circ Q_8$.

Write 2_+^{1+2k} to denote the central product $D_8 \circ D_8 \circ ... \circ D_8$ of k copies of D_8 and 2_-^{1+2k} to denote the product $D_8 \circ D_8 \circ ... \circ D_8 \circ Q_8$ of $k-1$ copies of D_8 with 1 copy of Q_8.

Lemma 2.22. *Let Q be an extra-special p-group of order p^{1+2k}. Then the smallest dimension of a faithful representation of Q over a field of order coprime to p is p^k.*

Proof. This follows from Proposition 4.6.3 (i), (ii) [KL]. □

Lemma 2.23. *Let p be a prime and suppose that P is an extra-special group of order p^{1+2n}.*

(i) If p is odd and P is of exponent p, then the subgroup of $Aut(P)/Inn(P)$ consisting of the elements acting trivially on $Z(P)$ is isomorphic to $Sp_{2n}(p)$.

(ii) If $P \cong 2_\pm^{1+2n}$, then $Aut(P)/Inn(P) \cong O_{2n}^{\pm}(2)$.

Proof. This is exactly Proposition 10.5 (iii) and Proposition 10.6 (iv) [GLS2]. □

Chapter 3

The Case $r = s$

The purpose of this chapter is to show that if $G \in Lie(r)$ with (G, t, X) a triple of type (Hs) such that $X \neq 1$, then $r \neq s$. If $p = r$, then since $p \neq s$ by assumption we certainly have $r \neq s$. Therefore we will assume that $p \neq r$ in what follows. We begin the chapter with some technical results. We first recall some theory on the *Generalized Fitting Subgroup* $F^*(X)$ of a finite group X, that we will use extensively in what follows. The following definition is exactly Definition 3.4 [GLS2]

Definition 3.1. *Let X be a finite group.*

(i) A Component of X is a quasisimple subnormal subgroup of X;

(ii) The Layer of X is the subgroup $E(X)$ generated by all the components of X;

(iii) The Fitting subgroup $F(X)$ of X is the largest normal nilpotent subgroup of X;

(iv) The generalized Fitting subgroup $F^*(X)$ of X is given by $F^*(X) = F(X)E(X)$.

The generalized Fitting subgroup $F^*(X)$ is a characteristic subgroup of X and the following result gives two further useful properties.

Proposition 3.2. *Let X be a finite group. Then*

(i) The subgroup $F^*(X)$ contains its centralizer, that is $C_X(F^*(X)) = Z(F(X))$;

(ii) If $N \lhd X$, then $F^*(N) \leq F^*(X)$.

Proof. Part (i) is a Theorem of Bender, 3.6 [GLS2]. Part (ii) can be found as Lemma 3.10 (i) [GLS2]. □

The next result we will need is a corollary of a well known Theorem of Borel and Tits. Here we state both the theorem and its corollary, as both will be needed further later. The following appear as Theorem 3.1.3 (a) and Corollary 3.1.4 [GLS3] respectively.

Theorem 3.3. *Let $G \in Lie(r)$ and let R be a nonidentity r-subgroup of G. Then there is a parabolic subgroup P of G such that $R \leq O_r(P)$ and $N_K(R) \leq P$.*

Corollary 3.4. *Let $G \in Lie(r)$. If X is a subgroup of $Aut(G)$ containing $Inn(G)$ and R is an r-subgroup of G with $R \nleq Z(G)$, then $N_X(R)$ and $N_G(R)$ are r-constrained. Moreover $F^*(N_X(R)) = O_r(N_X(R))$ and $F^*(N_G(R)) = O_r(N_G(R))Z(G)$.*

Our next result is a standard statement that appears as Chapter 5, Theorem 3.16 [G].

Theorem 3.5. *Let Z be a noncyclic abelian p'-group of automorphisms of a p-group X. Then*

$$X = \langle C_X(u) : u \in Z^{\#} \rangle.$$

Lemma 3.6. *Suppose $G \in Lie(r)$. Suppose that (G, t, X) is a triple of type (Hs) with $X \neq 1$ and $p \neq r$. For $u \in G$, write $X_u := C_X(u)$.*

(a) If there exists a subgroup $U \leq C_G(t)$ with $U \cong E_{r^2}$, then there exists $u \in U^{\#}$ such that $[X_u, t] \neq 1$,

(b) Given an r-element u of $C_G(t)$ with $[X_u, t] \neq 1$, we have that $F^*(C_G(u)) = O_r(C_G(u))$ and that $X_u\langle t\rangle$ acts faithfully on $F^*(C_G(u))$.

Proof. Since $U \leq C_G(t) \leq N_G(X)$, U acts on X. Since $p \neq r$, Theorem 3.5 gives $X = \langle X_u : u \in U^{\#}\rangle$. Now if $[X_u, t] = 1$ for every u, then $X = [X, t] = 1$ which is a contradiction, proving (a).

We now focus on the first part of (b). We use Corollary 3.4. Since $\langle u\rangle$ is an r-subgroup of G, we have $F^*(N_G(\langle u\rangle)) = O_r(N_G(\langle u\rangle))$. Now $C_G(u) \lhd N_G(\langle u\rangle)$, and so $F^*(C_G(u)) \leq F^*(N_G(\langle u\rangle))$ by Proposition 3.2 (ii). Hence $F^*(C_G(u)) \leq O_r(N_G(\langle u\rangle))$. Now $O_r(N_G(\langle u\rangle)) \leq O_r(C_G(u))$ since $O_r(N_G(\langle u\rangle))$ is an r-group normalizing $\langle u\rangle$ and $\langle u\rangle$ does not admit a nontrivial r-automorphism. So we have shown that $F^*(C_G(u)) \leq O_r(C_G(u))$. For the opposite inclusion, we note that $O_r(C_G(u))$ is nilpotent since it is a finite r-group. Thus, $O_r(C_G(u)) \leq F^*(C_G(u))$, giving the conclusion.

The second claim in (b) follows directly from the first claim and Proposition 3.2 (i). We have an r'-group $X_u\langle t\rangle \leq C_G(u)$. Further,

$$C_{X_u\langle t\rangle}(F^*(C_G(u))) \leq C_{C_G(u)}(F^*(C_G(u))) \leq F^*(C_G(u)) = O_r(C_G(u))$$

and $O_r(C_G(u))$ is of course an r-group. Hence $C_{X_u\langle t\rangle}(F^*(C_G(u))) = 1$, proving the result. □

Lemma 3.7. *Let p, r, s be primes with $p \neq r$, $p \neq s$. Let X be a nontrivial p-group and t an order s automorphism of X such that $[X, t] = X$. Suppose that $X\langle t\rangle$ acts faithfully on an r-group R and that $(RX\langle t\rangle, t, X)$ has type (Hs). Then $r \neq s$.*

Proof. This is just Lemma 1.8 [Ko] with 3 replaced by a general s. The proof is exactly analogous. $\square$

We are now in a position to prove our first main result.

Proposition 3.8. *Let $G \in Lie(r)$. Suppose that (G, t, X) is a triple of type (Hs) with $X \neq 1$. Then $r \neq s$.*

Proof. The proof is analogous to Proposition 2.1 [Ko]. Suppose $r = s$. Then $G \in Lie(s)$. We aim to show that there exists $U \leq C_G(t)$ such that $U \cong E_{s^2}$. Since $s > 3$, t cannot be a graph automorphism. So we treat the cases of t being inner, innerdiagonal or field.

Case 1: $t \in Inn(G)$.

We may suppose that the action of t is given by conjugation by an order s element of G which, by abuse of notation, we also label t. Then $t \in S$ for some $S \in Syl_s(G)$. Suppose $t \in Z(S)$. Then $S \leq C_G(t)$. Look at $m_s(S) = m_s(G)$. Table 3.3.1 [GLS3] gives us that $m_s(G) \geq 2$, as required, unless $G \cong A_1(s)$.

So suppose $G \cong A_1(s)$. If $p \neq 2$, then X is cyclic by Lemma 2.9 (b). So if X has order p^n, then $Aut(X)$ has order $p^{n-1}(p-1)$. Now t cannot act trivially on X (since if it did, then $X = [X, t] = 1$) and has prime order $s \neq p$, so s divides $p-1$. But on the other hand $|G| = \frac{1}{2}s(s-1)(s+1)$, so either p divides $s-1$ or p divides $s+1$. Either way this leads to a contradiction. Suppose now that $p = 2$. If $G \cong PSL_2(s)$, then Lemma 2.9 (c) gives that X is either cyclic or dihedral. If on the other hand $G \cong SL_2(s)$, then X is either cyclic or generalised quaternion. In both cases, the only possible non-trivial automorphism of odd order of X would have order 3. Since $s > 3$, t must act trivially on X, which is again a contradiction.

Finally, suppose $t \notin Z(S)$. Then $Z(S)$ contains some element $t_1 \neq t$ of order s. Then we may take $U = \langle t, t_1\rangle \cong E_{s^2}$, as required.

Case 2: $t \in Inndiag(G) - Inn(G)$.

In this case the order of t must be coprime to s (by Lemma 2.16), giving a contradiction.

Case 3: t is a field automorphism.

Again using Table 3.3.1 [GLS3], we obtain the required $m_s(C_G(t)) \geq 2$, unless $C_G(t) \cong A_1(s)$.

Suppose $C_G(t) \cong A_1(s)$. In this case $G \cong A_1(s^s)$. But $A_1(s)$ is maximal in $A_1(s^s)$ by Theorem 6.5.1 [GLS3]. Since $C_G(t)$ normalises X, $C_G(t) \leq XC_G(t) \leq G$. Thus because of maximality either $C_G(t) = XC_G(t)$ and so $X \leq C_G(t)$ which is an obvious contradiction as t acts non-trivially on X, or $XC_G(t) = G$ and so $X \lhd G$ which is also a contradiction as G is quasisimple and $[t, Z(G)] = 1$.

So by Cases 1-3, we may assume that there exists $U \leq C_G(t)$ such that $U \cong E_{s^2}$. Now we proceed as in [Ko]. U acts on X and so by Theorem 3.5, if we write $X_u := C_X(u)$, then $X = \langle X_u \in U^\# \rangle$. Now by Lemma 3.6 we may choose $u \in U^\#$ so that $[X_u, t] \neq 1$ and that $X_u\langle t \rangle$ acts faithfully on $F^*(C_G(u)) = O_s(C_G(u))$. As this contradicts Lemma 3.7, we have proved the result. $\square$

Chapter 4

The Case $p = r$

We now deal with triples (G, t, X) of type (Hs) such that $G \in Lie(r)$ and $p = r$. We prove the following result, similar to Proposition 2.2 [Ko].

Proposition 4.1. *Let $G \in Lie(r)$, $t \in Aut(G)$ and $1 \neq X \leq G$ be such that (G, t, X) is a triple of type (Hs) with $p = r$ and $s \geq 5$. Then $t \in Inndiag(G)$ and there exists a parabolic subgroup $P \leq G$ such that X is contained in the unipotent radical $O_r(P)$ of P, $C_G(t) \leq P$, $C_G(t) \cap O_r(P) = 1$ and $C_G(t)$ is conjugate to a subgroup of a Levi complement L of P.*

Proof. Since X is an r-group, Theorem 3.3 tells us that there exists a parabolic subgroup $P \leq G$ such that $X \leq O_r(P)$ and $C_G(t) \leq N_G(X) \leq P$. As we discussed earlier, since $s \geq 5$, either $t \in Inndiag(G)$ or t induces a field automorphism on G.

We first deal with the latter case. Thus assume that t induces a field automorphism on G. Since $G = {}^d\Sigma(q)$ for some d, Σ and q, by Proposition 4.9.1(a) of [GLS3], $O^{r'}(C_G(t)) = {}^d\Sigma(q^{\frac{1}{s}})$ and $C_G(t)/O^{r'}(C_G(t))$ induces diagonal automorphisms on $O^{r'}(C_G(t))$. Moreover, invoking Theorem 1 of [BGL] we conclude that $C_G(t)$ is a maximal subgroup of G unless $C_G(t) \in \{A_1(2), A_1(3), {}^2B_2(2)\}$. Suppose first that $C_G(t) \notin \{A_1(2), A_1(3), {}^2B_2(2)\}$. Then as $C_G(t)$ normalises X, $X \leq C_G(t)$. But then $X \lhd C_G(t)$ and so $X \leq O_r(C_G(t))$ which clearly contradicts the structure of $C_G(t)$. Therefore $C_G(t) \in \{A_1(2), A_1(3), {}^2B_2(2)\}$ and so G is one of the following groups: $A_1(2^s)$, $A_1(3^s)$, ${}^2B_2(2^s)$. Thus $p = r = 2$. In all the cases the only parabolic subgroup is a Borel subgroup B of G. Without loss of generality we may assume that $P = B$ and so $X \leq O_2(B)$. Since $C_G(t) \leq P = B$, $O_2(B) \cap C_G(t) \leq O_2(C_G(t)) = 1$. Hence, $O_2(B) \cap C_G(t) = 1$ and so the image of $C_G(t)$ in $B/O_2(B)$ is isomorphic to $C_G(t)$. This is an obvious contradiction as $B/O_2(B)$ is abelian while $C_G(t)$ is not. Therefore t cannot induce a field automorphism on G and so $t \in Inndiag(G)$.

By Theorem 4.1.9 of [GLS3], either t is of equal rank type or of parabolic type. Now,

$C_G(t) \leq P$. Denote by $U := O_r(P)$. If $C_U(t) \neq 1$, then $C_U(t) \leq O_r(C_G(t)) \neq 1$ which contradicts Theorem 4.2.2 of [GLS3]. Therefore $C_U(t) = 1$, and in particular, $C_X(t) = 1$ as $X \leq U$. Since P is a parabolic subgroup of G, $P = U \rtimes L$, where L is a Levi complement. By applying the Schur-Zassenhaus Theorem, we may see that $C_G(t)$ is conjugate to a subgroup of L. □

Chapter 5

The Case $p \neq r$, t an Inner-Diagonal Automorphism

By the results of Chapters 3 and 4, we may assume from this point forward that if (G, t, X) is a triple of type (Hs) with $G \in Lie(r)$, then the primes p, r, s are pairwise distinct.

5.1 Preliminary Lemmas

We first record some results that will be used repeatedly in the analysis to follow. The following theorem will be employed extensively. It can be found as Chapter 5, Theorems 2.3, 3.5 and 3.6 [G].

Theorem 5.1. *Let X be a p-group and let A be a p'-group of automorphisms of X. Then*

(i) $[[X, A], A] = [X, A]$*;*

(ii) $X = C_X(A)[X, A]$*;*

(iii) If X is abelian, then $X = C_X(A) \times [X, A]$.

In dealing with the groups of Lie type, we will need to work with the different versions of each group $G \in Lie(r)$ simultaneously. Therefore it will be necessary to first establish when we may pass between versions. We denote the universal version of G by G_u and the adjoint version by G_a. In the following, one of the two things happen: either H is a subgroup of G and then $\overline{H}$ denotes the image of H in G_a, or H is a subgroup of G_u and then $\overline{H}$ denotes the image of H in G. Similarly if $g \in G$ (correspondingly G_u), we write $\overline{g}$ to denote the image of g in G_a (correspondingly G). Finally, since every automorphism of G "lifts" to unique automorphisms of G_a and G_u (cf. Theorem 2.5.14 of [GLS3]) if φ

is an automorphism of G, then following the notation of [GLS3] we write φ_a and φ_u for the corresponding automorphisms of G_a and G_u.

Lemma 5.2. *Let $G \in Lie(r)$.*

(i) Let (G, t, X) be a triple of type (Hs). Let u be an automorphism of G_u such that $u = t_u$ and let Y be the largest p-subgroup of G_u such that $\overline{Y} = X$. Then $(G_u, u, [Y, u])$ is also a triple of type (Hs).

(ii) Let (G, t, X) be a triple of type (Hs). Suppose that s does not divide $|Z(G)|$. Then $(G_a, \overline{t}, \overline{X})$ is a triple of type (Hs).

Proof. (i) Note that $o(u) = o(t)$. By Theorem 5.1 (i), we have $[Y, u] = [[Y, u], u]$. It remains to show that $C_{G_u}(u) \leq N_{G_u}([Y, u])$. Take $g \in C_{G_u}(u)$. Since $Y = [Y, u]C_Y(u)$ (by Theorem 5.1 (iii)), it suffices to show that $g \in N_{G_u}(Y)$. Take $y \in Y$. Then, since $\overline{y} \in X$ and $\overline{g} \in C_G(t) \leq N_G(X)$, we have $\overline{gyg^{-1}} \in X$. So there exists $y_1 \in Y$ such that $\overline{gyg^{-1}} = \overline{y_1}$. Hence $gyg^{-1} = y_1 z$ for some $z \in Z(G_u)$. So y_1^{-1} commutes with gyg^{-1}. Since y, y_1 are both p-elements, so is $gyg^{-1}y_1^{-1} = z$. So in fact $z \in Y$. Hence $gyg^{-1} = y_1 z \in Y$ and so $g \in N_{G_u}(Y)$, as required.

(ii) Take $\overline{x} \in \overline{X}$ (where $x \in X$). As $x \in [X, t]$, $\overline{x} \in \overline{[X, t]} = [\overline{X}, \overline{t}]$. Thus $\overline{X} = [\overline{X}, \overline{t}]$. Now take $g \in C_{G_a}(\overline{t})$. Then $g = \overline{h}$ for some $h \in G$. We have $\overline{hth^{-1}} = \overline{t}$. Hence, $[h, t] \in Z(G)$. Thus t commutes with hth^{-1}. Hence, $[h, t]$ is an s-element. Since s does not divide $|Z(G)|$, we have $[h, t] = 1$. So $h \in C_G(t) \leq N_G(X)$. So $g = \overline{h} \in N_{G_a}(\overline{X})$ and so $(G_a, \overline{t}, \overline{X})$ is a triple of type (Hs). □

The consequence of Lemma 5.2 is that we may always start by assuming that G is the universal version, since any triple of type (Hs) in the adjoint version also gives rise to a triple in the universal version. If we wish to assume that G is adjoint, we have to respect the conditions of (ii) above.

We now introduce further preliminary results that will be useful in the analysis to follow. The following appears as Theorem 4.2.2 (a), (b), (d)-(g) [GLS3]. In the statement, $\overline{x}$ is the automorphism of the algebraic group $\overline{G}$ which induces x on G, which exists by Lemma 2.13.

Theorem 5.3. *Let $G \in Lie(r)$ with $G = {}^d\Sigma(q)$ and let $G^* = Inndiag(G)$. Let x be an inner-diagonal automorphism of G of prime order $r_1 \neq r$. Let Δ be the Dynkin diagram of $\overline{G}$ and Δ_x be the Dynkin diagram of $C_{\overline{G}}(\overline{x})$. Then there exist subgroups $T \leq C_G(x)$ and $T^* \leq C_{G^*}(x)$ such that the following hold.*

(a) $L := O^{r'}(C_G(x))$ is a central product $L_1 \circ L_2 \circ ... \circ L_j$ of groups $L_i \in Lie(r)$. Similarly, $L^* := O^{r'}(C_{G^*}(x))$ is a central product $L_1^* \circ L_2^* \circ ... \circ L_j^*$ of groups $L_i^* \in Lie(r)$, where each L_i^* is the image of L_i in G^*.

(b) T and T^* are abelian r'-groups inducing inner-diagonal automorphisms on each L_i (respectively L_i^*).

(c) $C_G(x)/LT$ is an elementary abelian r_1-group and is isomorphic to a subgroup of the kernel K of the covering map $G_u \to G$, where G_u is the universal version of G. Also $C_{G^*}(x)/L^*T^*$ is an elementary abelian r_1-group which is isomorphic to a subgroup of the center of G_u.

(d) We have $L_i = {}^{d_i}\Sigma_i(q^{m_i})$ and $L_i^* = {}^{d_i}\Sigma_i(q^{m_i})$ where

(i) The m_i's are positive integers, and

(ii) Δ_x is the disjoint union of the $\Delta_{x,i}$ for $i = 1, 2, ..., j$, where each $\Delta_{x,i}$ is in turn the disjoint union of m_i copies of the Dynkin diagram of Σ_i.

(e) If x is of parabolic type, then

(i) Δ_x is a subdiagram of Δ, and

(ii) If G is the universal version, then $L = L_1 \times L_2 \times ... \times L_j$ (the direct product)

(f) If x is of equal rank type, then $\Delta_x = \Delta \cup \{\alpha_*\} - \{\alpha\}$, that is the extended Dynkin diagram of $\overline{G}$ with one node erased.

We will employ this result whenever we have some element $z \in G$ or automorphism $z \in G^*$ which centralizes both X and t. Then we have $X\langle t\rangle \leq C_{G^*}(z)$ and we may use the above results to analyse $C_G(z)$. If z is an inner automorphism, we will try to choose $z \in Z(X)$, which gives $r_1 = p$, but this is not always possible.

The next statement highlights a commonly occurring situation that will allow the application of Theorem 5.3.

Lemma 5.4. *Let G be a finite group and let $t \in Aut(G)$. Suppose that every triple (G, t, Y) of type (Hs) with $Y \neq 1$ has Y nonabelian. Fix a particular triple (G, t, X) of type (Hs) (so that in particular X is nonabelian). Then for all $z \in Z(X)$ we have $X\langle t\rangle \leq C_{G\langle t\rangle}(z)$*

Proof. Suppose that $[Z(X), t] \neq 1$. We want to show that $(G, t, [Z(X), t])$ is a triple of type (Hs). Take $X_0 = [Z(X), t]$. We have $X_0 = [X_0, t]$ by Theorem 5.1 (i). Furthermore, since $C_G(t) \leq N_G(X)$ and $Z(X)$ is characteristic in X, $X_0 = [Z(X), t]$ is normalized by $C_G(t)$. So (G, t, X_0) is a triple of type (Hs) as required. This is a contradiction since $X_0 = [Z(X), t]$ is abelian. So we must have $Z(X) \leq C_G(t)$ and thus we see that if $z \in Z(X)$, $X\langle t\rangle \leq C_{G\langle t\rangle}(z)$. $\square$

5.1.1 Some Reductions

In this subsection we will work under the following hypotheses:

(H1) (G, t, X) is a triple of type (Hs) with $G \in \mathcal{L}ie(r)$,

(H2) There exists $z \in G$ such that the following conditions hold:

1. z is of prime order $r_1 \neq r$,
2. $z \notin Z(G)$, and
3. $X\langle t\rangle \leq C_{G^*}(z)$.

First let us suppose that s does not divide $|Z(G_u)|$. Then we may assume that $t \in Inn(G)$ by Lemma 2.16. So we may write $X\langle t\rangle \leq C_G(z)$. Since $z \notin Z(G)$, z induces a nontrivial inner automorphism on G. We may now apply Theorem 5.3 above to z. We will use the notation of this theorem (i.e., T and L, etc. are as in Theorem 5.3 with z instead of x). By part (c), $C_G(z)/LT$ is an elementary abelian r_1-group which is isomorphic to a subgroup of the kernel K of the covering map $G_u \to G$. Since $C_G(z)/LT$ is abelian, we have $X = [X, t] \leq [C_G(z), C_G(z)] \leq LT$. Further, $t \in LT$ since $C_G(z)/LT$ is isomorphic to a subgroup of K and t has order s. If $L = 1$, then $X\langle t\rangle \leq T$ and so $X = [X, t] \leq [T, T] = 1$. Thus suppose that $L \neq 1$. Then $X = [X, t] \leq [LT, LT] \leq L$. By part (a), we have that $L = L_1 \circ L_2 \circ ... \circ L_j$ and by part (b), t induces an inner-diagonal automorphism on each L_i. Write X_i for the projection of X into L_i, $i = 1, \ldots, j$. Then $X \leq X_1 \circ X_2 \circ ... \circ X_j$, each X_i is a p-group and since t acts on each factor L_i of L, we have $X_i = [X_i, t]$ for each i. Finally we have $C_{L_i}(t) = L_i \cap C_G(t) \leq L_i \cap N_G(X) = N_{L_i}(X) \leq N_{L_i}(X_i)$ for each i. Hence we may conclude that each (L_i, t, X_i) is a triple of type (Hs).

Suppose now that we are in the situation where s does divide $|Z(G_u)|$. We need to be a little more careful: now we may have $t \in Inndiag(G) - Inn(G)$ and so we may only say that $X\langle t\rangle \leq C_{G^*}(z)$. But we may use the results of Theorem 5.3 for G^*. Since we still have that $C_{G^*}(z)/L^*T^*$ is an elementary abelian r_1-group, we may make exactly analogous conclusions provided $s \neq r_1$. If z is an s-element and s does divide $|Z(G_u)|$, then we are unable to make any such statements.

In light of the above discussion we may now state the following result.

Lemma 5.5. *Let $G \in Lie(r)$, $t \in G^* = Inndiag(G)$ and suppose that (G, t, X) is a triple of type (Hs). Further suppose that there exists $z \in G$ of prime order $r_1 \neq r$ such that $z \notin Z(G)$ and $X\langle t\rangle \leq C_{G^*}(z)$. Suppose that either s does not divide $|Z(G_u)|$, or that $r_1 \neq s$ (or both). Then*

(a) X may be embedded inside a central product $L = L_1 \circ L_2 \circ ... \circ L_j$ of groups $L_i \in Lie(r)$ (where $L = O^{r'}(C_G(z))$ or $O^{r'}(C_{G^*}(z))$), whose possible isomorphism types may be calculated explicitly by Theorem 5.3 (d)-(f), such that t acts as an inner-diagonal automorphism

on each L_i.

(b) If we write X_i for the projection of X into L_i, then for each i, either (L_i, t, X_i) is a triple of type (Hs), or $X_i = 1$

We should also note that if $r_1 = 2$, then Tables 4.5.1, 4.5.2 and 4.5.3 [GLS3] give explicit lists of all the possible isomorphism types of $C_{G^*}(z)$ and in particular, L for us!

5.1.2 Further Lemmas

The following result appears as Proposition 11.11 [GLS2].

Lemma 5.6. *Let X be a p-group. Then there exists a subgroup Y of X with the following properties.*

(i) Y is critical in X, that is, Y char X and every p'-group of automorphisms of X acts faithfully on Y;

(ii) Y has nilpotence class at most 2;

(iii) $Y' = \Phi(Y)$ is elementary abelian;

(iv) If Y is not abelian, then it has exponent p or 4 according as p is odd or 2.

Remark 5.7. *Suppose again that (G, t, X) is a triple of type (Hs) with $G \in Lie(r)$. Later we will use Lemma 5.6 for the following common trick: take a subgroup $Y \leq X$ described above (which we know to be nontrivial provided $X \neq 1$) and switch to a new triple of type (Hs), the one involving Y. We will now outline the details.*

First of all notice that part (i) of the above lemma implies that t acts nontrivially on Y. Here are two cases to consider.

(1) First suppose that X is abelian. We have $C_Y(t) \leq C_X(t)$, and so $C_Y(t) = 1$ by Theorem 5.1 (iii). Thus $Y = [Y, t]$ by that same result. We also observe that $C_G(t) \leq N_G(Y)$ since Y is characteristic in X and hence (G, t, Y) is a triple of type (Hs). Now Lemma 5.6 (iii) tells us that $\Phi(Y) = 1$ and hence Y is elementary abelian. Therefore we have $Y \cong E_{p^n}$ for some n and so $Aut(Y) \cong GL_n(p)$. So we will be able to analyse the situation using the fact that s divides $|Aut(Y)|$ and that n is bounded by $m_p(G)$, the p-rank of G.

(2) If X is nonabelian, take $R = [Y, t]$. Then $R = [R, t]$ by Theorem 5.1 (i). Furthermore, since $C_G(t) \leq N_G(X)$ and Y is characteristic in X, R is normalized by $C_G(t)$. Hence, (G, t, R) is a triple of type (Hs).

We now state a technical lemma which will be used when we are in the situation of the above remark with $p = 2$.

Lemma 5.8. *Let X be a 2-group and Y be a subgroup of X satisfying conditions (i)-(iv) of Lemma 5.6. Let t be an automorphism of X of prime order s, $s \geq 5$, and let $R = [Y, t]$. Suppose further that R is nonabelian and $Z(R)$ contains a unique involution α.*

Then R is extraspecial.

Proof. We have $R' \leq \Phi(R) \leq \Phi(Y)$ by Lemma 2.18 as $R \lhd Y$. Since $R \leq Y$ and R is non-abelian while $cl(Y) \leq 2$, $cl(Y) = 2$. Hence, $cl(R) = 2$ and both R' and $\Phi(R)$ are elementary abelian since $R' \leq \Phi(R) \leq \Phi(Y)$. Further $Z(R)$ contains a unique involution and R is nonabelian, so $|R'| = 2$. Moreover, $\Omega_1(Z(R)) = \langle \alpha \rangle$ and so t acts trivially on it. Now Lemma 11.2(iii) of [GLS2] gives us that $[Z(R), t] = 1$.

Assume now that we have $\beta \in Z(R)$ such that $\beta^2 = \alpha$. Then as $\Phi(R)$ is elementary abelian, passing to the Frattini factor group $\overline{R} = R/\Phi(R)$ we have $1 \neq \overline{\beta} \in C_{\overline{R}}(t)$. Since $\overline{R}$ is elementary abelian (as the Frattini factor group of a 2-group) and $\overline{R} = [\overline{R}, t]$, we have $C_{\overline{R}}(t) = 1$ by Theorem 5.1 (iii), which is a contradiction. Hence $Z(R)$ has order 2, so $R' = Z(R)$. If $\Phi(R) > Z(R)$, then as $\Phi(R) \leq Z(Y)$, we get an obvious contradiction. Hence, $R' = \Phi(R) = Z(R)$ and and R is indeed extraspecial. □

In light of the above result, it will prove necessary to have some information on signalizers which are extra-special groups. We may make use of Lemmas 2.22 and 2.23 as follows to obtain the required information.

Lemma 5.9. *Let s be an odd prime and let $l \in \mathbb{N}$ be such that $s = 2^l + c$ where $0 < c < 2^l$. Let R be an extraspecial 2-group represented faithfully in $n < 2^{l+1}$ dimensions and suppose that R has an outer automorphism of order s.*

Then $c = 1$, $s = 2^l + 1$ and $R \cong 2_-^{1+2l}$. Moreover, $(\frac{|O_{2l}^-(2)|}{s}, s) = 1$.

Proof. Since R is extraspecial, we have $R \cong 2_+^{1+2k}$ or $R \cong 2_-^{1+2k}$ for some k. By Lemma 2.22, $2^k \leq n$ and so $k \leq l$. Since $Out(R)$ contains an element of order s, the order $|Out(R)|$ must be divisible by s. By Lemma 2.23, $|Out(R)|$ is equal to

$$|O_{2k}^{\pm}(2)| = 2^{k^2-k+1} \cdot (2^2 - 1) \cdot (2^4 - 1) \cdot ... \cdot (2^{2k-2} - 1) \cdot (2^k \mp 1)$$

So $|Out(R)|$ factorizes as

$$2^{k^2-k+1} \cdot (2-1) \cdot (2+1) \cdot (2^2-1) \cdot (2^2+1) \cdot ... \cdot (2^{k-1}-1) \cdot (2^{k-1}+1) \cdot (2^k \mp 1)$$

Since s is prime, s divides one of the factors in this product. Now $s = 2^l + c$ where $k \leq l$ and so s is larger than all of these factors except possibly the last one. So the only possibility is $c = 1$, $s = 2^l + 1$ and $Out(R) \cong O_{2k}^-(2)$, where $k = l$ so that $R \cong 2_-^{1+2l}$. It also follows that $(\frac{|O_{2l}^-(2)|}{s}, s) = 1$. □

Lemma 5.10. *Let $G = Lie(r)$, let s be a prime of the form $s = 2^l + 1$ for some $l \in \mathbb{N}$, and let $R \cong 2_-^{1+2l}$ be such that $Z(R)$ contains the unique involution in $Z(G)$. Suppose that (G, t, R) is a triple of type (Hs). Then $C_G(t)/C_{C_G(t)}(R) \cong C_s$.*

Proof. Since $C_G(t) \leq N_G(R)$, the group $C_G(t)/C_{C_G(t)}(R)$ embeds into $Out(R) \cong O_{2l}^-(2)$ and contains a central element of order $s = 2^l + 1$, namely the image $\bar{t}$ of t. So we look at the centralizer of $\bar{t}$ in $O_{2l}^-(2)$. By Table 1 [B], a Singer cyclic group C of $O_{2l}^-(2)$ has order $2^l + 1 = s$. Since $s = 2^l + 1$, Lemma 5.9 gives us that s divides $|O_{2l}^-(2)|$ only once. So we may assume that $\bar{t}$ is contained in C. Furthermore by the discussion in [B], $O_{2l}^-(2)$ is contained in $GL_{2l}(2)$ and C is the intersection of $O_{2l}^-(2)$ with a Singer cycle of $GL_{2l}(2)$. Now Proposition 2.8 [CR] says that a Singer cycle of $GL_{2l}(2)$ is self-centralizing. Hence C is also self-centralizing. We conclude that the centralizer of $\bar{t}$ in $O_{2l}^-(2)$ is isomorphic to C_s. Observe that, by Schur's Lemma, the group $C_{C_G(t)}(R)$ consists entirely of scalar matrices. Hence $C_G(t)/C_{C_G(t)}(R) \cong C_s$. □

We observed above that it will often be useful to know the p_1-rank $m_{p_1}(G)$ of G for some prime p_1. The following argument of Section 4.10 [GLS3] allows us to calculate $m_{p_1}(G)$ for p_1 odd if G is a group of Lie type. If $G \in Lie(r)$, then $|G_u|$ factorizes as $q^N \prod_i \Phi_i(q)^{n_i}$ where $\Phi_i(q)$ denotes the cyclotomic polynomial for the ith roots of unity. We define m_0 to be the multiplicative order of q modulo p_1. Then the following holds.

Theorem 5.11. *If $G \in Lie(r)$ and p_1 is an odd prime, then*

(a) $m_{p_1}(G_u) = n_{m_0}$; the exponent of Φ_{m_0} in the factorization of G_u,

(b) $m_{p_1}(G_a) = n_{m_0}$ or $n_{m_0} - 1$,

(c) Suppose that p_1 is a **good** *prime for G (meaning $p_1 > 3$ for all exceptional G and further that $p_1 > 5$ if $G = E_8$). Suppose further that the kernel of the natural map $G_u \to G$ is a p_1'-group. Then any elementary abelian p_1-subgroup of G lies in an elementary abelian p_1-subgroup of G of maximal rank.*

Proof. This is just parts (a), (b) and (e) of Theorem 4.10.3 [GLS3]. □

This theorem has the following vital consequence.

Corollary 5.12. *Let $G \in Lie(r)$, $t \in Inn(G)$ has prime order s, where $s \geq 5$, and s is a good prime for G. Suppose that the kernel of the natural map $G_u \to G$ is an s'-group. If $m_s(G) \geq 2$, then $C_G(t)$ has a subgroup $Z = \langle t, t_1 \rangle \cong E_{s^2}$.*

Proof. This follows directly from Theorem 5.11 (c). □

Let us discuss the implications this corollary might have for our investigation.

Remark 5.13. *Let (G, t, X) be a triple of type (Hs) with $G \in Lie(r)$. Now if we have $m_s(C_G(t)) \geq 2$, then there exists a subgroup $Z \cong E_{s^2}$ acting on X. Hence, by Theorem 3.5, we have $X = \langle C_X(u) : u \in Z^\# \rangle$.*

Then for $u \in Z^\#$, we have $C_X(u)\langle t \rangle \leq C_G(u)$. We may now study $C_G(u)$ by means of Lemma 5.5 to find out the possibilities for the $C_X(u)$ and hence for X. Note that Theorem 3.5 does not require for Z to be an s-group; for example if $C_G(t)$ contains a subgroup isomorphic to $C_{p_1}^2$ for any $p_1 \neq p$ we may apply the theorem.

If $m_{p_1}(C_G)(t) = 1$ for all primes $p_1 \neq p$ (including s), then we will have to use different methods.

We have already seen hints that the cases in which the subgroup X is abelian will require different techniques to when it is nonabelian. We will now reproduce some standard results that will help us to understand what restrictions there are on each of these cases. The following statement is Lemma 9.12 (ii) and (iv) [GLS2].

Lemma 5.14. *Let $G = KB$ be a Frobenius group with Frobenius kernel K and complement B. Suppose that $(r, |K|) = 1$ and let V be a faithful $\mathbb{F}G$-module with $\mathbb{F}$ of characteristic r. Then $dim_{\mathbb{F}}(V) \geq |B|$, and $C_K(C_V(B)) = 1$.*

The following result, which is Theorem 9.2 [I], will also be used repeatedly in what follows.

Lemma 5.15. *Let G be a finite group and let $\gamma : G \to GL_n(\mathbb{F})$ be an irreducible $\mathbb{F}$-representation of G. Then the following are equivalent.*

(a) γ is absolutely irreducible. That is, for every field $\mathbb{E} \geq \mathbb{F}$, γ is irreducible when viewed as an $\mathbb{E}$-representation of G.

(b) The centralizer of $\gamma(G)$ in the ring $M_n(\mathbb{F})$ of $n \times n$ matrices over $\mathbb{F}$ consists of scalar matrices.

Lemma 5.16. *Let $G \in Lie(r)$ and suppose that (G, t, X) is a triple of type (Hs) with $t \in Inndiag(G)$ and $X \neq 1$ abelian. Suppose that G has a faithful n-dimensional representation over a field of characteristic r. Then $n \geq s$.*

Proof. We have $X = [X, t] \times C_X(t)$ by Theorem 5.1 (iii). Hence $C_X(t) = 1$ since $X = [X, t]$. Thus $X\langle t \rangle$ is a Frobenius group. Now $X\langle t \rangle$ has an n-dimensional faithful representation over a field of characteristic r. Since $(|X|, r) = 1$, Lemma 5.14 gives $n \geq |\langle t \rangle| = s$ as required. □

It will turn out that Lemma 5.16 can be combined with the following result to deal with a much more general situation.

Lemma 5.17. *Let p, r and s be three distinct prime numbers. Assume further that p and s are odd and let $q = r^a$ for some $a \geq 1$. Let $X \rtimes \langle t \rangle$ be a group such that X is a p-group, $|\langle t \rangle| = s$ and $[X, t] = X$. Suppose further that $X\langle t \rangle$ has an n-dimensional faithful $\mathbb{F}_q$-module V with $n < s$. Then $X = 1$.*

Proof. Since p is odd, applying Lemma 5.6 gives us that X contains a characteristic subgroup Y of class at most 2, exponent p, with $Y' = \Phi(Y)$ and such that t acts faithfully on Y. Moreover, we may assume that $Y = [Y, t]$ and Y is the smallest non-trivial subgroup of X satisfying all those conditions.

If Y is abelian, then since $n < s$, we may apply Lemma 5.16 to obtain $Y = 1$ and we have a contradiction unless $X = 1$. Therefore we may assume that Y is nonabelian. In particular, both Y' and $Z(Y)$ are non-trivial elementary abelian subgroups of Y of exponent p and $[Y', t] = [Z(Y), t] = 1$ (for otherwise we could apply Lemma 5.16 to $Y'\langle t \rangle$ or $Z(Y)\langle t \rangle$).

Assume first that $Z(Y)$ is noncyclic. Since $Y\langle t \rangle$ acts faithfully on V, so does $Z(Y)$. Thus using Theorem 3.5 we obtain

$$V = \langle C_V(y) : y \in Z(Y) - \{1\} \rangle$$

Choose an element $y_0 \in Z(Y) - \{1\}$ such that $V_0 := C_V(y_0) \neq 1$ and t acts non-trivially on V_0. Then $\dim(V_0) := n_0 < n$ and since $y_0 \in Z(Y)$ and $[y_0, t] = 1$, it follows that V_0 is $Y\langle t \rangle$ - invariant. Clearly, $Y\langle t \rangle$ does not act faithfully on V_0. So, let us factor out the kernel of this action. Denote by $\overline{Y\langle t \rangle}$ the image of $Y\langle t \rangle$. Then $\overline{Y\langle t \rangle} \cong \overline{Y}\langle \overline{t} \rangle$ where $\overline{Y} = Y/C_Y(V_0) \neq 1$ and $\langle \overline{t} \rangle \cong \langle t \rangle$. The minimal choice of Y implies that $\overline{Y} = [\overline{Y}, \overline{t}]$, and as $n_0 < n < s$, we are done by induction on n.

So we may assume that $Z(Y)$ is cyclic. Since Y is of class 2, it follows that $Y' = Z(Y)$. And as $\Phi(Y) = Y'$ and Y has exponent p, we obtain that Y is extra-special. Thus $|Y| = p^{1+2m}$ for some $m \in \mathbb{N}$ and by Lemma 2.22, we have that $n \geq p^m$. Furthermore, since $[Y', t] = 1$ we obtain that t embeds into the subgroup of $Aut(Y)/Inn(Y)$ consisting of elements that act trivially on $Z(Y)$ which, by Lemma 2.23, is isomorphic to $Sp_{2m}(p)$. Since t has order s, this implies that s divides

$$|Sp_{2m}(p)| = p^{m^2} \cdot (p^2 - 1) \cdot (p^4 - 1) \cdot \ldots \cdot (p^{2m} - 1)$$

Since s is prime, it divides some factor in this product. Since $s \neq p$, it must divide $p^i \pm 1$ for some $i \leq m$. Since $p^m + 1$ is even, it follows that $s < p^m = n$, which is a contradiction. Hence $Y = 1$ and so $X = 1$, as required. $\square$

We now obtain the following lemma as a direct consequence of Lemma 5.17.

Lemma 5.18. *Let G be a group of Lie type over $\mathbb{F}_q$ ($q = r^a$), and suppose that G has an n-dimensional faithful $\mathbb{F}_q$-module V with $n < s$. Let X be a p-subgroup of G with p an odd prime and let $t \in Inndiag(G)$ such that (G, t, X) is a triple of type (Hs). Then $X = 1$.*

Taking Lemmas 5.16 and 5.18 together we obtain a very powerful consequence.

Corollary 5.19. *Let $G \in Lie(r)$, and suppose that G has an n-dimensional faithful representation with $n < s$. Let $X \neq 1$ be a p-subgroup of G and let $t \in Inndiag(G)$ such that (G, t, X) is a triple of type (Hs). Then $p = 2$ and X is nonabelian.*

We close this section with a series of results which are mostly generalizations of results found in [Ko]. We will need these in order to deal with groups of large Lie rank (in a sense that will become clear) to complete our inductive proof.

Lemma 5.20. *(Analogous to Lemma 1.7 [Ko]) Let $K = X\langle t\rangle$ be a Frobenius group with kernel X, a 2-group, and complement t, where $t^s = 1 \neq t$. Let R be an r-group with r odd and $r \neq s$. Suppose K acts by automorphisms on R and that (RK, t, X) is a triple of type (Hs). Then the action of K on R is not faithful.*

Proof. (Lemma 1.7 [Ko]) Assume for contradiction that the action is faithful. Now define $R_0 = [R, X] \leq R$ and $V = [R_0/\Phi(R_0), X] \leq R_0/\Phi(R_0)$. Note that since $R_0/\Phi(R_0)$ is the Frattini factor group of an r-group we may apply Lemma 2.19 (i) to see that V is elementary abelian. Now $\Phi(R_0)$ is a characteristic subgroup of R_0 and so K acts on V. We claim that this action is also faithful. Suppose there is a kernel $K_0 \triangleleft K$ of the action on V. Now suppose there is a 2-element $z \in K_0$. Then since X is a Sylow 2-subgroup of K, some conjugate $y = kzk^{-1}$ of z is in X. Clearly $y \in K_0$ since K_0 is normal in K. Now we have $R/\Phi(R_0) = V \times C_{R_0/\Phi(R_0)}(X)$ by Theorem 5.1 (iii). Since y acts trivially on both factors, we see that y acts trivially on the whole of $R_0/\Phi(R_0)$. So y acts trivially on R_0 by Theorem 2.19 (iii). Using the same argument as before we have $R = R_0 C_R(X)$ by Theorem 5.1 (ii) and hence y acts trivially on R. Now since this action is faithful we have $y = 1$ and so $z = 1$. Hence there are no nontrivial 2-elements contained in K_0. Thus either $|K_0| = 1$ or $|K_0| = s$. If $|K_0| = 1$, then since $\langle t\rangle$ is a Sylow s-subgroup of K, we see that K_0 is a conjugate of $\langle t\rangle$. Now K_0 is normal in K which is a contradiction since K is a Frobenius group with complement $\langle t\rangle$. Thus $K_0 = 1$ and the action of K on V is indeed faithful.

Since the action is faithful, we have $C_V(t) \neq 1$ by Lemma 5.14. Hence $C_{R_0/\Phi(R_0)}(t) \neq 1$. Now if we write $\overline{R_0} = R_0/\Phi(R_0)$, then we have $\overline{C_{R_0}(t)} \neq 1$ by Lemma 11.3 [GLS2] and hence $C_{R_0}(t) \neq 1$. Now $C_{R_0}(t) \leq C_{RK}(t) \leq N_{RK}(X)$ and so $[C_{R_0}(t), X] \leq X$. Since we also have $[C_{R_0}(t), X] \leq R_0 \leq R$ we in fact have $[C_{R_0}(t), X] = 1$. Hence $[C_V(t), X] = 1$ and thus $C_X(C_V(t)) = X$ which contradicts Lemma 5.14. So the action on V cannot be faithful. □

Lemma 5.21. *(Analogous to Lemma 1.9 [Ko]) Let G be a group such that $F^*(N) = O_r(N)$ for every r-local subgroup N of G. Suppose (G, t, X) is a triple of type (Hs) with p odd and r, s, p pairwise distinct and let P be a t-invariant r-local subgroup of G. Then $[X \cap P, t] = 1$.*

Proof. (Lemma 1.9 [Ko]) Let $X_0 = X \cap P$. Then X_0 is t-invariant. For contradiction, assume that $[X_0, t] \neq 1$. We have $[X_0, t] = [[X_0, t], t]$ by Theorem 5.1 (i) and so without loss of generality we may assume that $X_0 = [X_0, t]$. Now we claim that X_0 acts nontrivially on $O_r(P)$. Now $O_r(P) = F^*(P)$ and so if the action is trivial we have $X_0 \leq C_P(F^*(P)) \leq F^*(P)$ by Proposition 3.2 (i). Hence $X \leq O_r(P)$ and so X_0 is an r-group. This is a contradiction and so the action is indeed nontrivial.

Hence we have $C_{O_r(P)}(t) \neq 1$ by Lemma 11.14 (i) [GLS2]. Now $C_{O_r(P)}(t) \leq C_G(t) \cap P \leq N_G(X_0)$. Thus $[C_{O_r(P)}(t), X_0] \leq O_r(P) \cap X = 1$. So $s = r$ by Lemma 11.14 (ii) [GLS2]. This is a contradiction and so $[X_0, t] = 1$ as required. □

Corollary 5.22. *(Analogous to Cor 1.10 [Ko]) Let $G \in Lie(r)$ and suppose (G, t, X) is a triple of type (Hs). Suppose there exists a subgroup $Z \leq C_G(t)$ such that $Z \cong C_r \times C_r$. Then $p = 2$ and X is nonabelian.*

Proof. We have $Z \leq C_G(t) \leq N_G(X)$ so Z acts on X. So we have

$$\langle C_X(u) | u \in Z^{\#} \rangle$$

by Theorem 3.5. Now there exists $u \in Z^{\#}$ such that $[X_u, t] \neq 1$ by Lemma 3.6 (a), and by part (b) of that result we have $X_u\langle t \rangle$ acts faithfully on the group $R = O_r(N_{G\langle t \rangle}(\langle u \rangle))$.

We first show that $p = 2$. Suppose for contradiction that p is odd. Now $N_{G\langle t \rangle}(\langle u \rangle)$ is a t-invariant r-local subgroup of $G\langle t \rangle$ and so we have $[X \cap N_{G\langle t \rangle}(\langle u \rangle), t] = 1$ by Lemma 5.21. Now clearly $X_u \leq X$ and $X \leq N_{G\langle t \rangle}(\langle u \rangle)$ and hence $[X_u, t] = 1$. This contradicts Lemma 3.6 (a) and so we must have $p = 2$.

It remains to show that X is nonabelian. Suppose that it is abelian. Then $X\langle t \rangle$ is a Frobenius group and hence so is $X_u\langle t \rangle$. Now the faithful action on $O_r(N_{G\langle t \rangle}(\langle u \rangle))$ contradicts Lemma 5.20 and hence we must have X nonabelian. □

Remark 5.23. *Suppose that (G, t, X) is of type (Hs) and we are in the situation where we may assume that X is a nonabelian 2-group, whatever the version of G. Then we cannot be in the situation where $G = G_u$, X is nonabelian, but the image of X in G_a is abelian. Therefore, we may assume that $G = G_a$.*

5.1.3 Calculations in Algebraic Groups and their consequences

We now prove a statement about the centralisers of semisimple elements of simple algebraic groups. We will then quickly discuss the consequences of those calculations.

Proposition 5.24. *Let $\overline{G}$ be a simple algebraic group over $\overline{\mathbb{F}}_r$ (r prime, $r \neq s$) with fundamental root system $\Pi = \{\alpha_1, ..., \alpha_l\}$ (where the enumeration comes from the diagrams on page 12 of [GLS3]) and corresponding Dynkin diagram $\Delta_{\overline{G}}$. Let $\bar{t}$ be a nontrivial inner automorphism of $\overline{G}$ of order s and suppose $\bar{t}$ is of parabolic type. Write $\overline{C} = C_{\overline{G}}(\bar{t})$ and $\overline{S} = [\overline{C}^0, \overline{C}^0]$. Let Δ_0 be the Dynkin diagram of $\overline{S}$. Then the following hold:*

(i) If $\overline{G} \cong A_l$, then Δ_0 can be obtained by erasing at most $s-1$ nodes from $\Delta_{\overline{G}}$;

(ii) If $\overline{G} \cong B_l$ or $G \cong C_l$, then Δ_0 can be obtained by erasing at most $\frac{s-1}{2}$ nodes from $\Delta_{\overline{G}}$;

(iii) If $\overline{G} \cong D_l$, then Δ_0 can be obtained by erasing at most $\frac{s+1}{2}$ nodes from $\Delta_{\overline{G}}$;

If we further assume that $s = 5$, then the following hold:

(iv) $\overline{G} \cong E_6$, $\overline{G} \cong E_7$ or $\overline{G} \cong E_8$, then Δ_0 can be obtained by erasing at most 4 nodes from $\Delta_{\overline{G}}$;

(v) If $\overline{G} \cong F_4$, then Δ_0 can be obtained by erasing at most 3 nodes from $\Delta_{\overline{G}}$;

(vi) If $\overline{G} \cong G_2$, then Δ_0 can be obtained by erasing exactly 1 node from $\Delta_{\overline{G}}$.

Proof. (i) Let Π_0 be the fundamental root system of $\overline{S}$. As in Proposition 1.1 [Ko], we may assume that Π_0 is a subset of Π. Let $\mathscr{L}_{\overline{G}}$ be the Lie algebra of $\overline{G}$. Given $\alpha \in \Pi$ and the corresponding $e_\alpha \in \mathscr{L}_{\overline{G}}$ we have, since $\bar{t}$ has order s,

$$\bar{t}.e_\alpha = \omega^{\varepsilon_\alpha} e_\alpha \quad \text{with} \quad \varepsilon_\alpha \in \{0, 1, 2, ..., s-1\}$$

where $\omega \in \overline{\mathbb{F}}$ is an s-th root of unity. We suppose for contradiction that we cannot obtain Δ_0 by erasing fewer than s nodes from $\Delta_{\overline{G}}$. Then we must have some set $\{\beta_1, \beta_2, ..., \beta_s\} \subseteq \Pi - \Pi_0$. We assume that, for each i, $\beta_i = \alpha_{j_i}$ with $\alpha_{j_i} \in \Pi$, and $j_1 < j_2 < ... < j_s$. Without loss of generality, we may assume that if Δ is the smallest connected subdiagram of $\Delta_{\overline{G}}$ containing the β_i's for $i = 1, 2, ..., s$, then every node of Δ other than the β_i's is contained in Π_0. As in Lemma 1.3 [Ko], we see that

$$\begin{array}{rcll} \bar{t}.e_{\beta_i} & \neq & e_{\beta_i} & \text{for } i = 1, 2, ..., s \\ \bar{t}.e_\alpha & = & e_\alpha & \text{for all } \alpha \in \Pi_0. \end{array}$$

Thus we have $\bar{t}.e_{\beta_i} = \omega^{\varepsilon_i} e_{\beta_i}$ with $\varepsilon_i \in \{1, 2, ..., s-1\}$ for $i = 1, 2, ..., s$. Since Π_0 is the fundamental root system of $\overline{S}$, we will obtain a contradiction if we find some root which is not contained in the span of Π_0 but whose corresponding element of $\mathscr{L}_{\overline{G}}$ is fixed by $\bar{t}$. To achieve this we will make the following easy calculation.

Lemma 5.25. *Consider the finite sequence $\varepsilon_1, \varepsilon_2, ..., \varepsilon_s$ where each $\varepsilon_i \in \{1, 2, ..., s-1\}$. Then there exist j, k with $1 \leq j < k \leq s$ such that*

$$\sum_{i=j}^{k} \varepsilon_i \equiv 0 \mod s.$$

That is, some sum of consecutive terms of the sequence is congruent to $0 \mod s$.

Proof. We suppose no such list exists. Then in particular we may suppose $\theta_k = \sum_{i=1}^{k} \varepsilon_i \not\equiv 0 \pmod s$ for all $1 \leq k \leq s$. The θ_k account for s nonzero numbers $(\mod s)$ and so two of these sums must be equal. Thus $\theta_k = \theta_j \pmod s$ for some $k < j$. Now $\theta_j - \theta_k = \sum_{i=k+1}^{j} \varepsilon_i \cong 0 \pmod s$. This contradiction proves the result. □

By the above, we may now assume we have found j, k with $1 \leq j < k \leq s$ such that $\sum_{i=j}^{k} \varepsilon_i \equiv 0 \mod s$. Let Δ_{jk} be the smallest connected subdiagram of $\Delta_{\overline{G}}$ containing β_j and β_k. We have the following.

Δ_{jk} is of type A_n for some n, and Δ_{jk} is a subdiagram of Δ,

$\beta_i \in \Delta_{jk}$ for $j \leq i \leq k$,

$\beta_i \notin \Delta_{jk}$ for $i < j,\ i > k$.

Let $\tilde{\Pi} = \{\tilde{\alpha}_1, ..., \tilde{\alpha}_n\}$ be a fundamental root system for Δ_{jk}. Let $\tilde{\alpha} = \tilde{\alpha}_1 + \tilde{\alpha}_2 + ... + \tilde{\alpha}_n \in \Sigma(\tilde{\Pi})$, the full root system of $\tilde{\Pi}$. Then $\bar{t}.e_{\tilde{\alpha}} = \omega^{f(\tilde{\alpha})} e_{\tilde{\alpha}}$. Now

$$f(\tilde{\alpha}) = \sum_{i=j}^{k} \varepsilon_i \equiv 0 \mod s.$$

Hence $\omega^{f(\tilde{\alpha})} = 1$ and $\bar{t}$ fixes $e_{\tilde{\alpha}}$. But $\tilde{\alpha}$ is clearly not contained in the span of Π_0, giving the required contradiction.

(ii) Continue with all the notation of (i). This time assume for contradiction that we cannot obtain Δ_0 by erasing fewer than $\frac{s+1}{2}$ nodes from $\Delta_{\bar{G}}$. Then we have $\{\beta_1, \beta_2, ..., \beta_{\frac{s+1}{2}}\} \subseteq \Pi - \Pi_0$. Let $\tilde{\Pi} = \{\tilde{\alpha}_1, \tilde{\alpha}_2, ...\tilde{\alpha}_n\}$ be a fundamental system for Δ, where $\beta_i = \tilde{\alpha}_{m_i}$ for each i. Then $m_1 = 1$, $m_{\frac{s+1}{2}} = n$. There are now three cases.

Case 1: Δ has type B_n.

In this case we may proceed immediately with the following Lemma.

Lemma 5.26. *Consider the finite sequence $\varepsilon_1, \varepsilon_2, ..., \varepsilon_{\frac{s+1}{2}}$ where each $\varepsilon_i \in \{1, 2, ..., s-1\}$. Then at least one of the expressions of the forms (1)-(3) below is congruent to $0 \mod s$.*

(1) Sums $\varepsilon_i + \varepsilon_{i+1} + ...\varepsilon_{i+k}$ (with $1 \leq i < \frac{s+1}{2}$, $0 < k \leq \frac{s+1}{2} - i$) of consecutive terms in the sequence,

(2) Any sum $\varepsilon_i+\varepsilon_{i+1}+...+\varepsilon_{i+k}+2\varepsilon_{i+k+1}+...+2\varepsilon_{\frac{s-1}{2}}+2\varepsilon_{\frac{s+1}{2}}$ *(with* $1\le i<\frac{s-1}{2}$, $k\ge 0$*),*

(3) Sums $2\varepsilon_i+...+2\varepsilon_{\frac{s-1}{2}}+2\varepsilon_{\frac{s+1}{2}}$ *(with* $1\le i\le\frac{s-1}{2}$*).*

Proof. Suppose that in fact none of the above sums are congruent to $0 \mod s$. Then, taking everything modulo s, we have that ε_1 may not be congruent to any $-(\varepsilon_2+...\varepsilon_{2+k})$ with $0\le k\le\frac{s-3}{2}$, nor to any $-(\varepsilon_2+...+\varepsilon_{2+k}+2\varepsilon_{2+k+1}+...+2\varepsilon_{\frac{s-1}{2}}+2\varepsilon_{\frac{s+1}{2}}$ with $0\le k\le\frac{s-5}{2}$. Furthermore, there are $s-1$ of these expressions and, by our assumptions, they are all nonzero and distinct. Now this is a contradiction since we are working modulo s. □

By the lemma, one of the expressions of type (1)-(3) is congruent to $0 \mod s$. For each possibility, the following expressions in the $\tilde{\alpha}_i$ are roots of $\overline{G}$ which do not lie in the span of Π_0 but whose corresponding element of $\mathscr{L}_{\bar{G}}$ is fixed by $\bar{t}$ (see the list of roots in Remark 1.8.8 [GLS3]).

(1) $\tilde{\alpha}_{m_i}+\tilde{\alpha}_{m_i+1}...+\tilde{\alpha}_{m_{i+k}}$,

(2) $\tilde{\alpha}_{m_i}+\tilde{\alpha}_{m_i+1}+...+\tilde{\alpha}_{m_{i+k}}+2\tilde{\alpha}_{m_{i+k}+1}+...+2\tilde{\alpha}_{n-1}+2\tilde{\alpha}_n$,

(3) $2\tilde{\alpha}_{m_i}+...+2\tilde{\alpha}_{n-1}+2\tilde{\alpha}_n$.

Case 2: Δ has type C_n.

In this case we need the following lemma.

Lemma 5.27. *Consider the finite sequence* $\varepsilon_1,\varepsilon_2,...,\varepsilon_{\frac{s+1}{2}}$ *where each* $\varepsilon_i\in\{1,2,...,s-1\}$*. Then at least one of the expressions of the forms (1) or (2) below is congruent to* $0 \mod s$*.*

(1) Sums $\varepsilon_i+\varepsilon_{i+1}+...\varepsilon_{i+k}$ *(with* $1\le i<\frac{s+1}{2}$, $0<k\le\frac{s+1}{2}-i$*) of consecutive terms in the sequence,*

(2) Sums $\varepsilon_i+\varepsilon_{i+1}+...+\varepsilon_{i+k}+2\varepsilon_{i+k+1}+...+2\varepsilon_{\frac{s-1}{2}}+\varepsilon_{\frac{s+1}{2}}$*. (with* $1\le i<\frac{s-1}{2}$, $k\ge 0$*),*

(3) Sums $2\varepsilon_i+...+2\varepsilon_{\frac{s-1}{2}}+\varepsilon_{\frac{s+1}{2}}$ *(with* $1\le i\le\frac{s-1}{2}$*).*

Proof. This is analogous to Lemma 5.26. □

Again one of the expressions of type (1)-(3) is congruent to $0 \mod s$. For each possibility, the following expressions in the $\tilde{\alpha}_i$ are roots of $\overline{G}$ which do not lie in the span of Π_0 but whose corresponding element of $\mathscr{L}_{\bar{G}}$ is fixed by $\bar{t}$.

(1) $\tilde{\alpha}_{m_i}+\tilde{\alpha}_{m_i+1}+...+\tilde{\alpha}_{m_{i+k}}$,

(2) $\tilde{\alpha}_{m_i}+\tilde{\alpha}_{m_i+1}+...+\tilde{\alpha}_{m_{i+k}}+2\tilde{\alpha}_{m_{i+k}+1}+...+2\tilde{\alpha}_{n-1}+\tilde{\alpha}_n$,

(3) $2\tilde{\alpha}_{m_i}+...+2\tilde{\alpha}_{n-1}+\tilde{\alpha}_n$.

Case 3: Δ has type A_n.

In this case we define Δ_1 to be the subdiagram of $\Delta_{\bar{G}}$ consisting of β_1 and all nodes to the right of it on $\Delta_{\bar{G}}$. Then Δ_1 is a not necessarily proper subdiagram of $\Delta_{\bar{G}}$ of type C_k where $\frac{s+1}{2} \leq n < k$. We may assume that every node of Δ_1 other than the β_i is contained in Π_0. Let $\Pi_1 = \{\gamma_1, ...\gamma_k\}$ be a fundamental system for Δ_1. Write $\beta_i = \gamma_{s_i}$. Then $s_1 = 1$. Now we make the following calculation.

Lemma 5.28. *Consider the finite sequence $\varepsilon_1, \varepsilon_2, ..., \varepsilon_{\frac{s+1}{2}}$ where each $\varepsilon_i \in \{1, 2, ..., s-1\}$. Then at least one of the expressions of the form (1) or (2) below is equal to $0 \mod s$.*

(1) Sums $\varepsilon_i + \varepsilon_{i+1} + ...\varepsilon_{i+j}$ (with $1 \leq i < \frac{s+1}{2}$, $0 < j \leq \frac{s+1}{2} - i$) of consecutive terms in the sequence,

(2) Sums $\varepsilon_i + \varepsilon_{i+1} + ... + \varepsilon_{i+j} + 2\varepsilon_{i+j+1} + 2\varepsilon_{i+j+2} + ... + 2\varepsilon_{i+j+c}$ (with $1 \leq i < \frac{s-1}{2}$, $j, c \geq 1$).

Proof. Assume none of the expressions are $0 \mod s$. As before, this gives $s-1$ nonzero, distinct values that ε_1 cannot be equal to modulo s. This is a contradiction. $\square$

By the lemma, one of the expressions of type (1) and (2) is congruent to $0 \mod s$. For each possibility, the following expressions in the $\tilde{\alpha}_i$ are roots of $\overline{G}$ which do not lie in the span of Π_0 but whose corresponding element of $\mathscr{L}_{\bar{G}}$ is fixed by $\bar{t}$.

(1) $\gamma_{s_i} + \gamma_{s_i+1} + ... + \gamma_{s_{i+j}}$,

(2) $\gamma_{s_i} + \gamma_{s_i+1} ... + \gamma_{s_{i+j}} + 2\gamma_{s_{i+j}+1} + 2\gamma_{s_{i+j}+2} + ... + 2\gamma_{k-1} + \gamma_k$.

Now since we obtained the required contradiction in all three cases, we must have that $\Pi - \Pi_0$ can contain at most $\frac{s-1}{2}$ simple roots, as required.

(iii) Continue with all the notation of (i). This time assume that we cannot obtain Δ_0 by erasing less than $\frac{s+3}{2}$ nodes from $\Delta_{\bar{G}}$. Now we have $\{\beta_1, \beta_2, ..., \beta_{\frac{s+3}{2}}\} \subseteq \Pi - \Pi_0$. There are again 2 cases.

Case 1: Δ has type D_n.

We have the following lemma.

Lemma 5.29. *Consider the finite sequence $\varepsilon_1, \varepsilon_2, ..., \varepsilon_{\frac{s+3}{2}}$ where each $\varepsilon_i \in \{1, 2, ..., s-1\}$. Then at least one of the expressions of the forms (1) or (2) below is congruent to $0 \mod s$.*

(1) Sums $\varepsilon_i + \varepsilon_{i+1} + ...\varepsilon_{i+k}$ (with $1 \leq i < \frac{s+1}{2}$, $0 < k \leq \frac{s+1}{2} - i$) of consecutive terms in the sequence,

(2) Sums $\varepsilon_i + \varepsilon_{i+1} + ... + \varepsilon_{i+k} + 2\varepsilon_{i+k+1} + ... + 2\varepsilon_{\frac{s-1}{2}} + \varepsilon_{\frac{s+1}{2}} + \varepsilon_{\frac{s+3}{2}}$ (with $1 \leq i < \frac{s-1}{2}$, $k \geq 0$),

(3) Sums $2\varepsilon_{i+k+1} + ... + 2\varepsilon_{\frac{s-1}{2}} + \varepsilon_{\frac{s+1}{2}} + \varepsilon_{\frac{s+3}{2}}$ (with $1 \leq i \leq \frac{s-1}{2}$).

Proof. This is analogous to Lemma 5.26. $\square$

As usual, one of the expressions of type (1)-(3) is congruent to $0 \mod s$. For each possibility, the following expressions in the $\tilde{\alpha}_i$ are roots of $\overline{G}$ which do not lie in the span of Π_0 but whose corresponding element of $\mathscr{L}_{\bar{G}}$ is fixed by $\bar{t}$ (see the list of roots in Remark 1.8.8 [GLS3]).

(1) $\tilde{\alpha}_{m_i} + \tilde{\alpha}_{m_i+1} ... + \tilde{\alpha}_{m_{i+k}}$,

(2) $\tilde{\alpha}_{m_i} + \tilde{\alpha}_{m_i+1} + ... + \tilde{\alpha}_{m_{i+k}} + 2\tilde{\alpha}_{m_{i+k}+1} + ... + 2\tilde{\alpha}_{n-2} + \tilde{\alpha}_{n-1} + \tilde{\alpha}_n$,

(3) $2\tilde{\alpha}_{m_i} + ... + 2\tilde{\alpha}_{n-2} + \tilde{\alpha}_{n-1} + \tilde{\alpha}_n$.

Case 2: Δ has type A_n.

As in part (b) we define Δ_1 to be the subdiagram of $\Delta_{\bar{G}}$ consisting of β_1 and all nodes to the right of it on $\Delta_{\bar{G}}$. Then Δ_1 has type D_k where $\frac{s+3}{2} \leq n < k$. We may assume that every node of Δ_1 other than the β_i is contained in Π_0. Let $\Pi_1 = \{\gamma_1, ...\gamma_k\}$ be a fundamental system for Δ_1. Write $\beta_i = \gamma_{s_i}$. Then $s_1 = 1$. Now we make our usual calculation.

Lemma 5.30. *Consider the finite sequence $\varepsilon_1, \varepsilon_2, ..., \varepsilon_{\frac{s+1}{2}}$ where each $\varepsilon_i \in \{1, 2, ..., s-1\}$. Then at least one of the expressions of the form (1) or (2) below is congruent to $0 \mod s$.*

(1) Sums $\varepsilon_i + \varepsilon_{i+1} + ...\varepsilon_{i+j}$ (with $j \geq 1$) of consecutive terms in the sequence.

(2) Sums $\varepsilon_i + \varepsilon_{i+1} + ... + \varepsilon_{i+j} + 2\varepsilon_{i+j+1} + 2\varepsilon_{i+j+2} + ... + 2\varepsilon_{i+j+c}$. (with $i, j, c \geq 1$ and $i + j + c \leq \frac{s-1}{2}$)

Proof. Assume none of the expressions are congruent to $0 \mod s$. As before, this gives $s-1$ nonzero, distinct values that ε_1 cannot be congruent to modulo s. This is a contradiction. □

By the lemma, one of the expressions of type (1) and (2) is congruent to $0 \mod s$. For each possibility, the following expressions in the $\tilde{\alpha}_i$ are roots of $\overline{G}$ which do not lie in the span of Π_0 but whose corresponding element of $\mathscr{L}_{\bar{G}}$ is fixed by $\bar{t}$ (see the list of roots in Remark 1.8.8 [GLS3]).

(1) $\gamma_{s_i} + \gamma_{s_i+1} + ... + \gamma_{s_{i+j}}$,

(2) $\gamma_{s_i} + \gamma_{s_i+1} ... + \gamma_{s_{i+j}} + 2\gamma_{s_{i+j}+1} + 2\gamma_{s_{i+j}+2} + ... + 2\gamma_{k-2} + \gamma_{k-1} + \gamma_k$.

Since we obtained the required contradiction in both cases, we must have that $\Pi - \Pi_0$ can contain at most $\frac{s+1}{2}$ simple roots, as required.

(iv) Again continue with the notation of (i). We now assume that $s = 5$. This time we suppose for contradiction that we cannot obtain Δ_0 by erasing less than 5 nodes from $\Delta_{\bar{G}}$. Then we must have $\{\beta_1, \beta_2, \beta_3, \beta_4, \beta_5\} \subseteq \Pi - \Pi_0$. By Lemma 5.25, we may assume we have found j, k with $1 \leq j < k \leq 5$ such that $\sum_{i=j}^{k} \varepsilon_i \equiv 0 \mod 5$. As in (a), let Δ_{jk} be the smallest connected subdiagram of $\Delta_{\bar{G}}$ containing all the β_i with $j \leq i \leq k$. We have the following.

The type of Δ_{jk} is one of $\{A_n, D_n, E_6, E_7, E_8\}$ (for $n \geq 5$), and Δ_{jk} is a subdiagram of Δ,

$\beta_i \in \Delta_{jk}$ for $j \leq i \leq k$,

$\beta_i \notin \Delta_{jk}$ for $i < j,\ i > k$

Let $\tilde{\Pi} = \{\tilde{\alpha}_1, ..., \tilde{\alpha}_n\}$ be a fundamental root system for Δ_{jk}. Let $\tilde{\alpha} = \tilde{\alpha}_1 + \tilde{\alpha}_2 + ... \tilde{\alpha}_n \in \Sigma(\tilde{\Pi})$, the full root system of $\tilde{\Pi}$. Then $\bar{t}.e_{\tilde{\alpha}} = \omega^{f(\tilde{\alpha})} e_{\tilde{\alpha}}$. But

$$f(\tilde{\alpha}) = \sum_{i=j}^{k} \varepsilon_i \equiv 0 \mod 5$$

Hence $\omega^{f(\tilde{\alpha})} = 1$ and $\bar{t}$ fixes $e_{\tilde{\alpha}}$. But $\tilde{\alpha}$ is clearly not in the span of Π_0, giving the required contradiction.

(v) This time we assume that we cannot obtain Δ_0 by erasing less than 4 nodes from $\Delta_{\bar{G}}$. So we have $\Pi - \Pi_0 = \{\alpha, \beta, \gamma, \delta\}$, the full fundamental system of $\bar{G} = F_4$. Again we want to find a root which is which is not in the span of Π_0 but whose corresponding element of $\mathscr{L}_{\bar{G}}$ is fixed by $\bar{t}$. We will use the following calculation.

Lemma 5.31. *Consider the finite sequence $\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4$ where each $\varepsilon_i \in \{\pm 1, \pm 2\}$. Then at least one of the following expressions is congruent $0 \mod 5$.*

(a) $\varepsilon_1 + \varepsilon_2 + 2\varepsilon_3 + 2\varepsilon_4$,

(b) $\varepsilon_1 + 2\varepsilon_2 + 2\varepsilon_3 + 2\varepsilon_4$,

(c) $\varepsilon_1 + \varepsilon_2 + \varepsilon_3 + \varepsilon_4$,

(d) $\varepsilon_1 + \varepsilon_2$,

(e) $\varepsilon_2 + 2\varepsilon_3 + 2\varepsilon_4$,

(f) $\varepsilon_2 + \varepsilon_3 + \varepsilon_4$,

(g) $\varepsilon_1 + \varepsilon_2 + 2\varepsilon_3 + 2\varepsilon_4$,

(h) $\varepsilon_3 + \varepsilon_4$.

Proof. Suppose none of (a)-(h) are congruent to $0 \mod 5$. Then (a)-(d) give four inequalities for ε_1 and (e)-(h) show that the right hand sides of these are all nonzero and distinct, giving the usual contradiction. $\square$

By the lemma, one of the expressions (a)-(h) is congruent to $0 \mod 5$. For each possibility, the following expressions in are roots of $\overline{G}$ which do not lie in the span of Π_0 but whose corresponding element of $\mathscr{L}_{\bar{G}}$ is fixed by $\bar{t}$ (see the list of roots in Remark 1.8.8 [GLS3]).

(a) $\alpha + \beta + 2\gamma + 2\delta$,

(b) $\alpha + 2\beta + 2\gamma + 2\delta$,

(c) $\alpha + \beta + \gamma + \delta$,

(d) $\alpha + \beta$,

(e) $\beta + 2\gamma + 2\delta$,

(f) $\beta + \gamma + \delta$,

(g) $\alpha + \beta + 2\gamma + 2\delta$,

(h) $\gamma + \delta$.

(vi) This time suppose that we cannot obtain Δ_0 by erasing less than 2 nodes from $\Delta_{\bar{G}}$. Then we have $\{\beta_1, \beta_2\} \subseteq \Pi - \Pi_0$. That is, the full fundamental system $\{\alpha, \beta\}$. Making the usual calculation, it is easily seen that if $\varepsilon_1, \varepsilon_2 \in \{\pm 1, \pm 2\}$, then one of the following expressions is congruent to 0 modulo 5.

(a) $\varepsilon_1 + \varepsilon_2$,

(b) $2\varepsilon_1 + \varepsilon_2$,

(c) $3\varepsilon_1 + \varepsilon_2$,

(d) $3\varepsilon_1 + 2\varepsilon_2$.

Then in each case we may easily give a root which is not in the span of Π_0 but whose corresponding element of $\mathscr{L}_{\bar{G}}$ is fixed by $\bar{t}$, giving the required contradiction.

(a) $\alpha + \beta$,

(b) $2\alpha + \beta$,

(c) $3\alpha + \beta$,

(d) $3\alpha + 2\beta$. □

Proposition 5.24 has the following important corollaries.

Corollary 5.32. *(Analogous to Corollary 1.5 [Ko]) Let r be a prime, $r \neq s$ and let $q = r^a$. Let G be one of the following groups: $A^{\pm}_m(q)$ $(m \geq s+1)$, $B_m(q)$ $(m \geq \frac{s+3}{2})$, $C_m(q)$ $(m \geq \frac{s+3}{2})$ or $D^{\pm}_m(q)$ $(m \geq \frac{s+5}{2})$. If t is an inner-diagonal automorphism of G of order s, then there exists $Z \leq C_G(t)$ such that $Z \cong C_r \times C_r$.*

Proof. We may apply Lemma 2.13 to find a σ-setup $(\overline{G}, \sigma)$ of G and the unique $\bar{t} \in Aut(\overline{G})$ which induces t on G. We have that $\bar{t}$ is inner and has order s. Now we look at $L := O^{r'}(C_G(t))$. We may analyse L by means of Theorem 5.3 (a),(e) [GLS3]. We see that L is a central product $L_1 \circ L_2 \circ ... \circ L_j$ of groups $L_i = {}^d\Sigma_{m_i}(q^{a_i}) \in Lie(r)$. Further, the Dynkin diagram of $C_{\overline{G}}(\bar{t})$ is the disjoint union of diagrams Δ_i for $i = 1, 2, ..., j$ where each Δ_i is in turn a disjoint union of a_i copies of the Dynkin diagram of L_i. By Proposition 5.24 we obtain the Dynkin diagram of $\overline{S} = [C_{\overline{G}}(\bar{t}), C_{\overline{G}}(\bar{t})]$ by erasing at most $s - 1$ nodes from the diagram of $\overline{G}$, and hence that diagram has at least two nodes. In particular, $j \geq 1$. If $j \geq 2$, then certainly $m_r(L) \geq 2$. If $j = 1$, then $m_r(L) \geq 2$ by Table 3.3.1 [GLS3], unless $L \cong A_1^{\pm}(r)$. Then by our earlier observation we must have $\overline{S} = \overline{A_1}$ which contradicts the fact that the Dynkin diagram of $\overline{S}$ has at least 2 nodes. □

Corollary 5.33. *Let $q = r^a$, where $r \neq 5$ and suppose that $G \cong E_l(q)$ for $l = 6, 7, 8$ or $G \cong {}^2E_6(q)$. If t is an inner-diagonal automorphism of G of order 5, then there exists $Z \leq C_G(t)$ such that $Z \cong C_r \times C_r$*

Proof. This is exactly analogous to Corollary 5.32. □

5.2 The Case $G = A_m^{\pm}(q)$

In this section, we address the case $G = A_m^{\pm}(q)$ with $q = r^a$. Recall that the primes p,r,s are assumed to be pairwise distinct and that $s \geq 5$. We begin with a general result about inner-diagonal automorphisms of G.

Lemma 5.34. *Let $G = A_m(q)$ and let x be an inner-diagonal automorphism of G of prime order $r_1 \neq r$. Then x is not of equal rank type.*

Proof. Let $\overline{x}$ be the automorphism of the algebraic group $\overline{G} = A_m$ inducing x on G and let Δ_x be the Dynkin diagram of $C_{\overline{G}}(\overline{x})$. If x is of equal rank type, then by Theorem 5.3 (f), Δ_x has type A_m. This is a contradiction since x is a nontrivial automorphism. □

We now obtain our main results.

Lemma 5.35. *Let $G \cong A_1^{\pm}(q)$. Let X be a p-subgroup of G and let $t \in Inndiag(G)$ be such that (G, t, X) is a triple of type (Hs). Then $X = 1$.*

Proof. By Lemma 5.2, we may assume that G is universal. Corollary 5.19 tells us that X must be a nonabelian 2-group. Hence $r \neq 2$. Since $SU_2(q) \cong SL_2(q)$, we may assume $G \cong SL_2(q)$. For contradiction, suppose $X \neq 1$.

The subgroup X is contained in some $Y \in Syl_2(G)$. The Sylow subgroup Y is a generalized quaternion group. Hence X is either cyclic or is also generalized quaternion group. This is a contradiction since no such 2-group admits a non-trivial action of an automorphism of order $s > 3$. Hence $X = 1$. □

Lemma 5.36. *Let $G \cong A_m^{\pm}(q)$, where $m < s - 2$. Let X be a p-subgroup of G and let $t \in Inndiag(G)$ be such that (G, t, X) is a triple of type (Hs). Then $X = 1$.*

Proof. We work by induction on m, taking Lemma 5.35 as the basis case of our induction. So we assume that if (G, t, Y) is a triple of type (Hs) with $G \cong A_{m'}^{\pm}(q')$ for some $m' < m$ and some q' (q' being a power of r), then $Y = 1$.

Suppose that $X \neq 1$. By Lemma 5.2, we may assume $G \cong SL_n(q)$ or $G \cong SU_n(q)$, where $n = m + 1$. We see that X must be a nonabelian 2-group by Corollary 5.19. Furthermore, as $s > n$, we may use Lemma 2.16 to conclude that t induces an inner automorphism on G. Since $|Z(G)| = (n, q \pm 1)$, by abuse of notation, we assume that t is an element of G.

By Lemma 5.6, X contains a critical subgroup Y such that Y has class at most 2, $Y' = \Phi(Y)$ is elementary abelian and Y has exponent 2 or 4. Set $R = [Y, t]$. Then, as noted in Remark 5.7 (2), (G, t, R) is a triple of type (Hs). We know $R \neq 1$ since Y is critical in X.

If R is abelian, then we have a contradiction with Lemma 5.16. So we may assume that R is nonabelian.

First suppose that $Z(R)$ contains an involution z which is not contained in $Z(G)$. Then, by Lemmas 5.4 and 5.5, we obtain $R \leq L = L_1 \circ L_2 \circ \circ L_j$, where $L_i \cong A^{\pm}_{m_i}(q^{a_i})$ and each (L_i, t, R_i) is a triple of type (Hs), where R_i denotes the projection of R onto L_i. Further, by Theorem 5.6 (d)-(f) and Lemma 5.34, each L_i has Lie rank $m_i < m$, since $z \notin Z(G)$. So by the inductive hypothesis, we obtain $R_i = 1$ for each i. Then $R = 1$ which is a contradiction. Therefore we may assume that $Z(R)$ contains a unique involution, namely the unique order 2 element α of $Z(G)$.

By Lemma 5.8, R is extra-special. So either $R \cong 2^{1+2k}_{+}$ or $R \cong 2^{1+2k}_{-}$. Since $C_G(t)$ acts on R, there is an embedding $C_G(t)/C_{C_G(t)}(R) \hookrightarrow Out(R) := Aut(R)/Inn(R)$. Further, by Lemma 2.23 (ii), we have $Out(2^{1+2k}_{\pm}) \cong O^{\pm}_{2k}(2)$. Since there is an embedding $C_G(t)/C_{C_G(t)}(R) \hookrightarrow Out(R)$, R has an outer automorphism of order s. Choose l such that $s = 2^l + c$ for $0 < c < 2^l$. Since G is represented in $n = m + 1 < s - 1$ dimensions, we may apply Lemma 5.9. So we have $c = 1$ and $R \cong 2^{1+2l}_{-}$. Hence, by Lemma 2.22, $n \geq 2^l = s - 1$. So $m = n - 1 \geq s - 2$ which is a contradiction. Thus $R = 1$ and so $X = 1$. $\square$

Alternative Proof

We work by induction on m, taking Lemma 5.35 as the basis case of our induction. So we assume that if (G, t, Y) is a triple of type (Hs) with $G \cong A^{\pm}_{m'}(q')$ for some $m' < m$ and some q' (q' a power of r), then $Y = 1$.

Suppose that $X \neq 1$. By Lemma 5.2, we may assume $G \cong SL_n(q)$ or $G \cong SU_n(q)$, where $n = m + 1$. Suppose X is abelian. By Theorem 5.1 (iii), we have $X = C_X(t) \times [X, t]$. Since $X = [X, t]$, we may conclude that $C_X(t) = 1$. In particular, $F := X\langle t\rangle$ is a Frobenius group. Since the natural representation of G has dimension n and the Frobenius complement of F has order s, applying Lemma 5.14 gives $n \geq s$. This is a contradiction since $n = m + 1 < s - 1$.

Therefore we may assume that X is nonabelian. Applying Lemma 5.6 gives us that X contains a characteristic subgroup Y of class at most 2, exponent p or 4, with $Y' = \Phi(Y)$ and such that t acts faithfully on Y. Moreover, we may assume that $Y = [Y, t]$ and Y is the smallest non-trivial subgroup of X satisfying all those conditions.

If Y is abelian, then since $n < s$, we may apply Lemma 5.16 to obtain $Y = 1$ and we have a contradiction unless $X = 1$. Therefore we may assume that Y is nonabelian. Then Y is of exponent p for p odd and of exponent 4 if $p = 2$. Moreover, $[Y', t] = [Z(Y), t] = 1$ for otherwise we could apply Lemma 5.16 to $Y'\langle t\rangle$ or $Z(Y)\langle t\rangle$. Finally, both Y' and $Z(Y)$ are non-trivial elementary abelian subgroups of Y of exponent p. This is true for odd p

as $exp(Y) = p$. As for $p = 2$, $Y' = \Phi(Y)$ is of exponent 2 by Lemma 5.6, while $Z(Y)$ is of exponent 2 for otherwise $C_{Y/\Phi(Y)}(t) \neq 1$ (as the image of $Z(Y)$ in $Y/\Phi(Y)$ would be non-trivial and t would centralise it) while $Y/\Phi(Y) = [Y/\Phi(Y), t]$ (as $Y = [Y, t]$).

Assume first that $Z(Y)$ is noncyclic. Since $Y\langle t\rangle$ acts faithfully on V, so does $Z(Y)$. Thus using Theorem 3.5 we obtain

$$V = \langle C_V(y) : y \in Z(Y) - \{1\}\rangle$$

Choose an element $y_0 \in Z(Y) - \{1\}$ such that $V_0 := C_V(y_0) \neq 1$ and t acts non-trivially on V_0. Then $\dim(V_0) := n_0 < n$ and since $y_0 \in Z(Y)$ and $[y_0, t] = 1$, it follows that V_0 is $Y\langle t\rangle$ - invariant. Clearly, $Y\langle t\rangle$ does not act faithfully on V_0. So, let us factor out the kernel of this action. Denote by $\overline{Y\langle t\rangle}$ the image of $Y\langle t\rangle$. Then $\overline{Y\langle t\rangle} \cong \overline{Y}\langle \overline{t}\rangle$ where $\overline{Y} = Y/C_Y(V_0) \neq 1$ and $\langle \overline{t}\rangle \cong \langle t\rangle$. The minimal choice of Y implies that $\overline{Y} = [\overline{Y}, \overline{t}]$, and as $n_0 < n < s$, we are done by induction on n.

So we may assume that $Z(Y)$ is cyclic. Since Y is of class 2, it follows that $Y' = Z(Y)$. And as $\Phi(Y) = Y'$ and Y has exponent p, we obtain that Y is extra-special. Thus $|Y| = p^{1+2m}$ for some $m \in \mathbb{N}$ and by Lemma 2.22, we have that $n \geq p^m$. Furthermore, since $[Y', t] = 1$ we obtain that t embeds into the subgroup of $Aut(Y)/Inn(Y)$ consisting of elements that act trivially on $Z(Y)$ which, by Lemma 5.9 , is isomorphic to $Sp_{2m}(p)$ for p odd and $O^{\pm}_{2m}(2)$ if $p = 2$. Let us consider the case when p is odd. Since t has order s, this implies that s divides

$$|Sp_{2m}(p)| = p^{m^2} \cdot (p^2 - 1) \cdot (p^4 - 1) \cdot \ldots \cdot (p^{2m} - 1)$$

Since s is prime, it divides some factor in this product. Since $s \neq p$, it must divide $p^i \pm 1$ for some $i \leq m$. Since $p^m + 1$ is even, it follows that $s < p^m = n$, which is a contradiction. Hence $Y = 1$ and so $X = 1$. Therefore we may assume that $p = 2$. Using the factorisation of $|O^{\pm}_{2m}(2)|$ we obtain a similar numerical contradiction.

Lemma 5.37. *Let $G \cong A^{\pm}_{s-2}(q)$. Let X be a p-subgroup of G and let $t \in Inndiag(G)$ be such that (G, t, X) is a triple of type (Hs). Then either $X = 1$ or one of the following holds.*

(i) $G \cong SU_4(3)$, $s = 5$, $C_G(t) \cong C_4 \times C_5$ and $X \cong 2^{1+4}_{-}$, or

(ii) G is isomorphic to a quotient of $SU_4(3)$ by its central subgroup of order 2, $s = 5$, $C_G(t) \cong C_2 \times C_5$ and $X \cong E_{2^4}$.

(iii) $G \cong PSU_4(3)$, $s = 5$, $C_G(t) \cong C_5$ and $X \cong E_{2^4}$.

Furthermore, the triples (G, t, X) described in (i)-(iii) do indeed exist.

Proof. As in the proofs of Lemmas 5.35 and 5.36, by applying Lemma 5.2 we may assume that G is universal (so that either $G \cong SL_{s-1}(q)$ or $G \cong SU_{s-1}(q)$). Since $|Z(G)| = (s-1, q \pm 1)$ and $s > s-1$, using Lemma 2.16, we may assume that t is an element of G. Moreover, by Corollary 5.19, X is a nonabelian 2-group. Exactly as in the proof of Lemma 5.36, X contains the critical subgroup Y of Lemma 5.6, we take $R = [Y, t]$ and we may assume that R is nonabelian. Continuing with that argument, if $Z(R)$ contains an involution z which is not contained in $Z(G)$, then as above we obtain, by Lemmas 5.4 and 5.5, $R \leq L = L_1 \circ L_2 \circ \circ L_j$, where $L_i \cong A^{\pm}_{m_i}(q^{a_i})$ and each (L_i, t, R_i) is a triple of type (Hs). Further, by Theorem 5.3 (d)-(f) and Lemma 5.34, $m_i < s-2$ for each i. Hence, by Lemma 5.36, each $R_i = 1$. So we may assume that $Z(R)$ contains a unique involution and so, by Lemma 5.8, R is extra-special. Then $R \cong 2^{1+2k}_{\pm}$ for some k and there is an embedding $C_G(t)/C_{C_G(t)}(R) \hookrightarrow Out(R) \cong O^{\pm}_{2k}(2)$. Choose l such that $s = 2^l + c$ where $0 < c < 2^l$. By Lemma 5.9, $c = 1$, $s = 2^l + 1$ and $R \cong 2^{1+2l}_{-}$. This time we do not obtain a contradiction with Lemma 2.22 since the natural module for G has dimension $s - 1 = 2^l$. Instead we may apply Lemma 5.10 to see that $C_G(t)/C_{C_G(t)}(R) \cong C_s$.

We now obtain bounds on the order of $C_G(t)$. Certainly $|C_G(t)| \leq s \cdot |C_{C_G(t)}(R)|$. Furthermore $C_{C_G(t)}(R) \leq C_G(R)$, and by definition any element of $C_G(R)$ commutes with the irreducible subgroup R of G. So by Schur's Lemma, $C_G(R)$ consists entirely of scalar matrices, that is elements of $Z(G)$, and we may conclude that it has order $(q \pm 1, s-1)$, according to whether $G \cong SL_{s-1}(q)$ or $G \cong SU_{s-1}(q)$. So certainly $|C_G(t)| \leq s(s-1)$.

A lower bound on $|C_G(t)|$ may be obtained as follows. By Fermat's little theorem, s divides

$$q^{s-1} - 1 = q^{2^l} - 1 = (q-1) \cdot (q+1) \cdot (q^2+1) \cdot (q^4+1) \cdot \ldots \cdot (q^{2^{l-1}}+1).$$

Since s is prime, s divides one of the factors in this product.

If s divides $q-1$ or s divides $q^{2^{l'}} + 1$ for $l' < l-1$, then since each of these polynomial expressions in q appears more than once in the factorization of $|G|$ into irreducible cyclotomic polynomials, Theorem 5.11 (a) gives $m_s(G) \geq 2$. In this case $m_s(C_G(t)) \geq 2$ by Corollary 5.12. This is a contradiction since we showed above that $|C_G(t)| \leq s(s-1)$. So in fact s must divide $q^{2^{l-1}} + 1$.

Now a Singer cyclic subgroup of $SL_{s-1}(q)$ has order $c_+ = (q^{s-1}-1)/(q-1)$. Further, by Theorem 2.2 [BG], $SU_{s-1}(q)$ has a cyclic subgroup of order $c_- = (q^{s-1}-1)/(q+1)$. Since we also showed above that there is no element u such that $u^s = t$, we may assume that t is contained in a cyclic subgroup S of G of order $c_{\pm}$ according to whether $G = SL_{s-1}(q)$ or $G = SU_{s-1}(q)$. Hence $S \leq C_G(t)$ and so $(q^{s-1}-1)/(q \pm 1) = |S| \leq |C_G(t)| \leq s(s-1)$. We now check whether this is possible.

Claim 5.38. *(i) If $n \geq 5$ and $q \geq 3$, then $(q^{n-1}-1)/(q-1) > n(n-1)$,*

(ii) If $n > 5$, n odd and $q \geq 3$, then $(q^{n-1}-1)/(q+1) > n(n-1)$,

(iii) If $q > 3$ then $(q^4 - 1)/(q + 1) > 20$.

Proof. (i) We work by induction on n. Certainly $(3^4 - 1)/2 = 40 > 20 = 5 \cdot 4$, which proves the result for $n = 5$. Now suppose the result holds for $n = k$. Then $q^{(k+1)-1} - 1 = q^k - 1 = q(q^{k-1} - 1) + q - 1 > q \cdot k(k-1)(q-1) + q - 1$ by the inductive hypothesis. Since $q \geq 3$, we have $q \cdot k(k-1) + 1 > k(k+1)$ which proves the result for $n = k + 1$.

(ii) Again we work by induction on n. Certainly $(3^6 - 1)/2 > 42$ which gives the result for $n = 7$. Suppose the result holds for $n = k$. Then $q^{(k+2)-1} - 1 = q^{k+1} - 1 = q^2(q^{k-1} - 1) + q^2 - 1 > q^2 \cdot k(k+1)(q-1) + q^2 - 1$ by the inductive hypothesis. Since $q \geq 3$, we have $q^2 \cdot n(n+1)(q-1) + q^2 - 1 > (n+2)(n+1)$ which proves the result for $n = k + 2$.

(iii) Certainly $(4^4 - 1)/(4 + 1) = 51 > 20$ which gives the result for $q = 4$. Since $(q^4 - 1)/(q + 1)$ is an increasing function of q, the full result now follows. □

Recall that $p = 2$ so $q \geq 3$. If $s > 5$, then $|S| = (q^{s-1} - 1)/(q \pm 1) > s(s-1)$ by Claim 5.38. This is a contradiction since we showed above that $|S| \leq s(s-1)$. Hence we may assume that $s = 5$. If $G = SL_4(q)$ then $|S| = (q^4 - 1)/(q - 1)$. By Claim 5.38 (i), $|S| > 20$ and this is a contradiction as before. So we may assume that $G = SU_4(q)$. If $q > 3$ then $|S| = (q^4 - 1)/(q + 1) > 20$ by Claim 5.38 (iii) and we again have a contradiction. Hence $q = 3$. Recall that $5 = s = 2^l + 1$, so $l = 2$. Hence $R \cong 2_-^{1+4}$. So a priori we may have a triple (G, t, R) of type (Hs) with $G \cong SU_4(3)$, $s = 5$ and $R \cong 2_-^{1+4}$. In this case, looking at the list of maximal subgroups given in Chapter 5 [K3] gives that $N_G(X)$ must be contained in a maximal subgroup $M \cong 2_-^{1+4}.Sp_4(2) \cong N_G(R)$ of G. So we have $X = R$.

It remains to show that such triples do indeed exist. By the lists in Chapter 5 [K3], $G = SU_4(3)$ has a maximal subgroup $M \cong 2_-^{1+4}.Sp_4(2)$. Thus G has a subgroup $X \cong 2_-^{1+4}$ which is normalized by a 5-element t. By [ATLAS], an order 5 element of $PSU_4(3)$ has centralizer isomorphic to C_5. Hence $C_G(t) \cong C_4 \times C_5$. Since we certainly have $Z(G) \leq N_G(X)$ we see that $C_G(t) \leq N_G(X)$. Finally the only elements of X which are centralized by t lie in $Z(X)$, so $X = [X, t]$ and we have a triple $(SU_4(3), t, X)$ of type $(H5)$. Passing to the relevant quotient groups we obtain triples of the types given in parts (ii), (iii) of the statement. □

We now discuss the case $m \geq s - 1$. Since we found triples of type $(H5)$ in $A_3^-(3)$ we will now separate the cases $(s, q) \neq (5, 3)$ and $(s, q) = (5, 3)$.

Lemma 5.39. *Let $G \cong A_{s-1}^{\pm}(q)$, where $(s, q) \neq (5, 3)$. Let X be a p-subgroup of G and let $t \in Inndiag(G)$ be such that (G, t, X) is a triple of type (Hs). Then $X = 1$.*

Proof. By Lemma 5.2, we may assume that G is universal. We have $G = SL_s^{\varepsilon}(q)$, with $\varepsilon = 1$ if $G \cong SL_s(q)$ and $\varepsilon = -1$ if $G \cong SU_s(q)$. Note that, by Lemma 2.16, the group

$Outdiag(G)$ of outer-diagonal automorphisms of G has order $(s, q-\varepsilon)$, so t does not necessarily induce an inner automorphism on G.

There are two cases to consider.

Case 1: X is abelian.

Assume first that t is induced by a genuine element of order s. Then by abuse of notation we may assume that $t \in GL_s^{\varepsilon}(q)$. Consider the group $K := X \rtimes \langle t \rangle$. By using Lemma 5.6 if needed we may reduce to the case when X is an elementary abelian subgroup. Since $X = [X, t]$, Theorem 5.1 implies that $C_X(t) = 1$ and so K is a Frobenius group with kernel X and complement $\langle t \rangle$. As $K \leq G$, K acts faithfully on the natural module V of G. Since Frobenius complement of K has order s while $dim_{\mathbb{F}}(V) = s$, K must act irreducibly on V. We may now use Clifford's Theorem (cf. Theorem 9.7 of [GLS2]) to conclude that X acts completely reducibly on V. Moreover, $V = V_1 \oplus \ldots \oplus V_f$ where each V_i is a Wedderburn component of the $\mathbb{F}X$-module V, K transitively permutes V_i's and $XC_K(X) = X$ is contained in the kernel of this permutation action. Since $K/X \cong \langle t \rangle \cong C_s$, it follows immediately that either $f = s$, $dim_{\mathbb{F}}(V_i) = 1$ for $i = 1, \ldots, s$ and t transitively permutes V_i's, or $f = 1$ and so X acts irreducibly on V.

In the former case it follows immediately that K is contained in the setwise stabiliser N of a frame $\{V_1, \ldots, V_s\}$ in V. In fact X is contained in a pointwise stabiliser of the frame, and so $N_G(X) \leq N$. Recall that N is isomorphic to the monomial subgroup of G, i.e., N contains a normal subgroup $N_0 \cong E_{q-\varepsilon}^{s-1}$ and $N/N_0 \cong S_s$, a permutation group on s letters. In particular it follows that $t \in G$ and since $C_G(t) \leq N_G(X)$, $C_G(t)/C_{C_G(t)}(X) \cong C_s$ while $C_{C_G(t)}(X) \leq Z(G)$. Thus $|C_G(t)| \leq s^2$.

Now, if s divides $q - \varepsilon$, t is diagonalisable and so $C_G(t)$ contains a subgroup $C \cong C_{q-\varepsilon}^{s-1}$. In particular, $s^2 \geq (q-\varepsilon)^{s-1}$. We will now prove the following statement.

Claim 5.40. *If $q \geq 4$ and $n \geq 5$, then $(q-1)^{n-1} > n^2$.*

Proof. Since $q \geq 4$, we certainly have $(q-1)^{n-1} \geq 3^{n-1}$. Therefore it suffices to prove that $3^{n-1} \geq n^2$ for all $n \geq 5$. We prove this by induction on n. Certainly $3^{5-1} = 81 \geq 25 = 5^2$ and so the result holds for $n = 5$. Now suppose the result holds for $n = k$ and look at the case $n = k+1$. Then by the inductive hypothesis we have

$$3^{n-1} = 3^k = 3 \cdot 3^{k-1} \geq 3k^2$$

Since $k \geq 5$ we certainly have $3k^2 \geq (k+1)^2 = n^2$ and so the result holds for $n = k+1$. This completes the proof. $\square$

Since $s \geq 5$ and s divides $q - \varepsilon$, we must have $q \geq 4$. Hence the above claim leads to an obvious contradiction with our earlier evaluation of $|C_G(t)|$. Thus s does not divide $q - \varepsilon$.

In particular, $t \in G$.

If $m_s(C_G(t)) \geq 2$, then there exists $Z = \langle t, t_1 \rangle \cong C_s^2$ acting on X. Then, by Theorem 3.5, $X = \langle C_X(u) | u \in Z^{\#} \rangle$. Choose $C_X(u)$ as large as possible for $u \in Z^{\#}$. Certainly $C_X(u)\langle t \rangle \leq C_G(u)$. Then by Lemma 5.5 we obtain $C_X(u) \leq L = L_1 \circ L_2 \circ \ \circ L_j$, where $L_i \cong A^{\pm}_{m_i}(q^{a_i})$, and each projection $(L_i, t, C_X(u)_i)$ is of type (Hs). Further, by Theorem 5.3 (d) -(f) and Lemma 5.34, each L_i has Lie rank $m_i < s-1$. Hence we may apply Lemmas 5.36 and 5.37 to conclude that each $C_X(u)_i = 1$. Hence $C_X(u) = 1$. Since we chose $C_X(u)$ as large as possible, we must have $X = 1$. Therefore we may assume that $m_s(C_G(t)) = 1$.

Now s divides $q^{s-1} - 1$ by Fermat's little theorem. Since s is prime, s divides one of the irreducible cyclotomic polynomials $\Phi_i(q)$, where i divides $s - 1$.

Suppose first that $G = SL_s(q)$. If $i < s-1$, then $\Phi_i(q)$ has exponent greater than 1 in the factorization of $|G|$ and so by Theorem 5.11 (a), we have $m_s(G) \geq 2$. Hence $m_s(C_G(t)) \geq 2$ by Corollary 5.12. This is a contradiction since we showed above that $m_s(C_G(t)) = 1$. Hence s must divide $\Phi_{s-1}(q)$. We may conclude that t is contained in a Singer cycle $S_+ \cong C_{m_+}$ of a subgroup $H \cong SL_{s-1}(q)$ of G, where $m_+ = (q^{s-1} - 1)/(q - 1)$.

The situation for $G = SU_s(q)$ is a little more complicated. Write $s - 1 = 2k$ so that $q^{s-1} - 1 = (q^k - 1) \cdot (q^k + 1)$. Suppose first that k is even. If s divides $q^k - 1$, then an argument analogous to the $SL_s(q)$ case shows that $m_s(C_G(t)) \geq 2$, which is again a contradiction. If s divides $q^k + 1$, then s divides $\Phi_{2j}(q)$ for some factor j of k. Then we see that s divides $q^{2j} - 1$ and so, if $j < k$, we may again see that $m_s(C_G(t)) \geq 2$. So s must divide $\Phi_{s-1}(q)$. Now suppose k is odd. If s divides $q^k + 1$, then we may immediately conclude that $m_s(C_G(t)) \geq 2$. So s divides $q^k - 1$ and hence divides some $\Phi_i(q)$ such that i divides k. Then s divides $q^{2i} - 1$. Hence, if $i < k$ we have $2i < s - 1$ and so we may see again that $m_s(C_G(t)) \geq 2$, which is a contradiction as before. So in this case we require that s divides $\Phi_k(q) = \Phi_{\frac{s-1}{2}}(q)$. In either case, we may use Theorem 2.2 [BG] to conclude that t is contained in a cyclic subgroup $S_- \cong C_{m_-}$ of order $m_- = (q^{s-1} - 1)/(q + 1)$.

It follows that $s^2 \geq (q^{s-1} - 1)/(q - \varepsilon)$. Since $q \geq 4$ and $s \geq 5$, the following statement gives us an immediate contradiction.

Claim 5.41. *If $q \geq 4$ and n is odd, $n \geq 5$, we have $(q^n - \varepsilon)/(q - \varepsilon) > n^2$.*

Proof. We use induction on n. Assume first $\varepsilon = 1$. Certainly $q^5 - 1 > 25(q - 1)$ for $q \geq 4$ which proves the result for $n = 5$. Now assume the result holds for $n = k$. Then $q^{k+2} - 1 = q^2(q^k - 1) + q^2 - 1 > q^2 \cdot k^2(q-1) + q^2 - 1$ by the inductive hypothesis. Factorizing, this quantity this is equal to $(q-1)(q^2k^2 + q + 1)$. Then since $q^2k^2 + q + 1 > 16k^2 + 3 > (k+2)^2$ for $q \geq 4$, $k \geq 5$, the required result holds. If $\varepsilon = -1$ the proof is analogous. $\square$

Therefore we are reduced to the case when $f = 1$, i.e., X acts faithfully and irreducibly on V. It follows that X is a cyclic group of order p and p does not divide $q^i - \varepsilon$ for $i < s$. Thus X is contained in a Singer cyclic subgroup S of G and $C_G(X) = S$. Since $t \in N_G(X)$ of order s, from the structure of the normaliser of a Singer cyclic subgroup, it follows that t acts on S as a field automorphism and $N_G(X) = S\langle t \rangle$. In particular, $|C_G(t) \cap C_G(X)| \leq (q - \varepsilon)$. Therefore $|C_G(t)| \leq s(q - \varepsilon)$. Again using the numerical evaluations for $|C_G(t)|$ that we used above, we easily get a numerical contradiction.

Therefore we are reduced to the case when the automorphism t of G is induced by an element $t_0 \in GL_s^\varepsilon(q)$ of order s^2 such that $t_0^s \in Z(G)$. In particular, $|Z(G)| = s$ and $\langle t_0^s \rangle = Z(G)$. In this case take $K_0 = X \rtimes \langle t_0 \rangle$. Since $(ps, r) = 1$, V is completely reducible. Assume that there exists an $\mathbb{F}K_0$ submodule $V_0 \leq V$ with $\dim_\mathbb{F} V_0 < dim_\mathbb{F} V$. Now t_0^s acts by scalars on V and hence on V_0. It follows that K_0 is isomorphic to a subgroup of $GL^\varepsilon(V_0)$ which is a contradiction as $n_0 < s$. Thus K_0 acts irreducibly on V. We may now apply Clifford's Theorem to the action of K_0 on V. This time it follows that either K stabilises a frame as before (in particular, $X\langle t_0^s \rangle$ stabilises the frame point wise) or X acts irreducibly on V.

In the former case arguing as before we obtain that $|C_G(t_0)| \leq s^2$. If $s^2 \mid (q - \varepsilon)$, then t_0 is diagonalisable and we may apply the same argument as before. Hence assume that s^2 does not divide $(q - \varepsilon)$. Since $q - \varepsilon$ appears with exponent $s - 1$ in the factorization of $|G| = |SL_s^\varepsilon(q)|$ into irreducible polynomials in q, Theorem 5.11 (a) gives $m_s(G) = s - 1$. Now suppose s divides $(q^k - (\varepsilon)^k)/(q - \varepsilon)$ for some $k < s$. Then s divides some cyclotomic polynomial $\Phi_i(q)$ that appears with exponent smaller than $s - 1$ in the factorization of $|G|$. Theorem 5.11 (a) would then give $m_s(G) < s - 1$, which is a contradiction. So s does not divide $(q^k - (\varepsilon)^k)/(q - \varepsilon)$ for $k < s$. Since s^2 does not divide $q - \varepsilon$, s^2 does not divide $(q^k - (\varepsilon)^k)$ for $k < s$. By Table 1 [B], a Singer cyclic subgroup of $GL_s^\varepsilon(q)$ has order $q^s - \varepsilon$. Since we showed above that s^2 does not divide $(q^k - \varepsilon^k)$ for $k < s$, we may assume that t_0 is contained in a Singer cyclic subgroup C of $GL_s^\varepsilon(q)$. Take $C_0 = C \cap G \leq C_G(t)$. Then C_0 has order $(q^s - \varepsilon)/(q - \varepsilon)$. It follows that $s^2 \geq (q^s - \varepsilon)/(q - \varepsilon)$ which as we saw is a contradiction for $s \geq 5$.

Thus we are in the latter case and so as before we may assume that $X \cong C_p$ acts irreducibly on V. Arguing as before we obtain that $|C_G(t_0)| \leq s(q - \varepsilon)$. Again using the numerical evaluations for $|C_G(t_0)|$ that we used above, we easily get a numerical contradiction.

Case 2: X is nonabelian.

Since $(p, s) = 1$, $X \cap Z(G) = 1$. We may now apply Lemmas 5.4 and 5.5, to obtain that $X\langle t \rangle \leq C_G(z)$ for some $z \in Z(X)$ and so $X \leq L = L_1 \circ L_2 \circ \; \circ L_j$, where $L_i \cong A_{m_i}^{\pm}(q^{a_i})$. By Theorem 5.3 (d)-(f) and Lemma 5.34, each L_i has Lie rank $m_i < s - 1$. So applying Lemmas 5.36 and 5.37, we obtain $X = 1$. This finishes the proof. □

Before deriving results for the remaining linear and unitary groups, we pause to prove the following general claim.

Claim 5.42. *Let G be a group of Lie type over $\mathbb{F}_q$ where $q = r^a$ and suppose that G has a faithful representation in dimension $n < rs$. Suppose that (G, t, X) is of type (Hs) with $X \neq 1$ (where p, r and s are pairwise coprime) and that $O^{r'}(C_G(t)) \cong A_1(r)$. Then X is nonabelian.*

Proof. Assume for contradiction that X is abelian. Then by Theorem 5.1 (iii), $X\langle t\rangle$ is a Frobenius group. Take $u \in C_G(t)$ of order r. Since $C_G(t) \leq N_G(X)$, u acts on X. If $C_X(u) \neq 1$, then $K = C_X(u)\langle t\rangle$ is a Frobenius group. By Lemma 3.6 (b), K acts faithfully on $O_r(C_G(u))$. If $p = 2$, this contradicts Lemma 5.20. If p is odd, then by Lemma 5.21 we obtain $[C_X(u), t] = [X \cap C_G(u), t] \leq [X \cap N_G(\langle u\rangle), t] = 1$, which is also a contradiction, since $C_X(u)\langle t\rangle$ is supposed to be a Frobenius group. Hence we must have $C_X(u) = 1$. So $X\langle tu\rangle$ is a Frobenius group with a complement of order rs. This contradicts Lemma 5.14. Therefore X is nonabelian. □

Lemma 5.43. *Let $G \cong A_s^{\pm}(q)$, where $(s, q) \neq (5, 3)$. Let X be a p-subgroup of G and let $t \in Inndiag(G)$ such that (G, t, X) is a triple of type (Hs). Then $X = 1$.*

Proof. By Lemma 2.16, we may assume that t acts as an inner automorphism on G.

We argue as in the proof of Lemma 2.11 [Ko]. By Lemma 2.13, there exists an order s automorphism $\bar{t}$ of the algebraic group $\overline{G} \cong A_s$ over $\overline{\mathbb{F}}_r$ which induces t on G. The Dynkin diagram of $\overline{G}$ has s nodes. By Theorem 5.3, $L = O^{r'}(C_G(t))$ is a central product $L_1 \circ L_2 \circ ... \circ L_j$ of groups $L_i \cong A_{m_i}^{\pm}(q^{a^i})$ such that the Dynkin diagram of $C_{\overline{G}}(\bar{t})$ is the disjoint union of diagrams Δ_i for $i = 1, 2, ..., j$ where each Δ_i is in turn a disjoint union of a_i copies of the Dynkin diagram of L_i. By Proposition 5.24 (i), the Dynkin diagram for $C_{\overline{G}}(\bar{t})$ has at least 1 node, and hence $L \neq 1$. In particular $m_r(L) \geq 1$.

If $m_r(L) \geq 2$, then by Corollary 5.22, X is a nonabelian 2-group. In particular, as discussed in Remark 5.23, we may assume that $G = G_a$. Then by Lemmas 5.4 and 5.5, we have $X\langle t\rangle \leq M_1 \circ M_2 \circ ... \circ M_j$, where each $M_i \cong A_{m_i}^{\pm}(q^{a^i})$ and each projection (M_i, t, X_i) has type (Hs). By Lemma 5.34, each M_i has rank $m_i < s$ and we obtain $X = 1$ by Lemmas 5.35- 5.39.

So we may assume that $m_r(L) = 1$. By Table 3.3.1 [GLS3], we obtain $q = r$ and $L = A_1(r)$. In particular, $G \cong A_s^{\pm}(r)$. By Lemma 5.2, we may assume that $G = G_u$. So G has a natural module of dimension $n = s + 1$. Since $s + 1 < rs$, we are in the conditions of Claim 5.42. Therefore X is nonabelian.

Suppose that p is odd. Applying Lemma 5.6 gives us that X contains a characteristic subgroup Y of class at most 2, exponent p, with $Y' = \Phi(Y)$ and such that t acts faithfully on Y. Moreover, we may assume that $Y = [Y, t]$ and Y is the smallest non-trivial subgroup of X satisfying all those conditions. Furthermore, as Y is a characteristic subgroup, all of this implies that (G, t, Y) is a triple of type (Hs).

If Y is abelian, then since Y is a characteristic subgroup of X and $Y = [Y, t]$, we may apply Claim 5.42 to obtain $Y = 1$ and we have a contradiction unless $X = 1$. Therefore we may assume that Y is nonabelian. Further, both Y' and $Z(Y)$ are non-trivial elementary abelian subgroups of Y of exponent p and $[Y', t] = [Z(Y), t] = 1$ (for otherwise, since Y is a characteristic subgroup of X, and Y', $Z(Y)$ are characteristic in Y, we would be able to apply Claim 5.42 to (G, t, Y') or $(G, t, Z(Y))$).

Assume first that $Z(Y)$ is noncyclic. Then since $Z(G)$ is cyclic, $Z(Y)$ contains a p-element z not contained in $Z(G)$. So we have $Y\langle t\rangle \le C_G(z)$ and we may apply Lemmas 5.5, and 5.35-5.39 to obtain $Y = 1$.

So we may assume that $Z(Y)$ is cyclic. Since Y is of class 2 and exponent p, it follows that $Y' = Z(Y)$. As $\Phi(Y) = Y'$ and Y has exponent p, we obtain that Y is extra-special. Thus $|Y| = p^{1+2m}$ for some $m \in \mathbb{N}$ and by Lemma 2.22, we have that $n = s + 1 \ge p^m$. Furthermore, since $[Y', t] = 1$, we obtain that t embeds into the subgroup of $Aut(Y)/Inn(Y)$ consisting of elements that act trivially on $Z(Y)$ which, by Lemma 5.9 (i), is isomorphic to $Sp_{2m}(p)$. Since t has order s, this implies that s divides

$$|Sp_{2m}(p)| = p^{m^2} \cdot (p^2 - 1) \cdot (p^4 - 1) \cdot \ldots \cdot (p^{2m} - 1)$$

Since s is a prime, it divides some factor in this product. Since $s \neq p$, it must divide $p^i \pm 1$ for some $i \le m$. Since $s \ge p^m - 1$, we have $s = p^m - 1$ or $s = p^m + 1$. This is a contradiction since s and p are both odd.

Therefore we may assume that $p = 2$. By Lemma 5.6, X contains a critical subgroup Y. Let $R = [Y, t]$. As discussed in Remark 5.7, (G, t, R) is a triple of type (Hs). By Claim 5.42, R is nonabelian. If $Z(R)$ contains an involution not contained in $Z(G)$, then $R\langle t\rangle \le C_G(z)$ and we may apply Lemmas 5.5 and 5.35- 5.39 to obtain $Y = 1$. So we may assume that $Z(R)$ contains a unique involution and by Lemma 5.8, R is extra-special.

Choose l such that $s = 2^l + c$, where $0 < c < 2^l$. Suppose first that $c + 1 < 2^l$. Then G has a faithful representation in $n = s + 1 < 2^{l+1}$ dimensions. Since R admits an order s automorphism and has a faithful representation in dimension smaller than 2^{l+1}, Lemma 5.9 gives $c = 1$ and $R \cong 2_-^{1+2l}$. Hence $s = 2^l + 1$. So by Lemma 5.10, we have $C_G(t)/C_{C_G(t)}(R) \cong C_s$. However, we have $O^{r'}(C_G(t)) \cong A_1(r)$. Since $A_1(r)$ does not contain a central element of order s, the whole of $O^{r'}(C_G(t))$ centralizes R. Hence $R\langle t\rangle \le C_G(z)$ for some involution z (passing to the quotient group $\bar{G} = G/Z(G)$ to avoid the case $z \in Z(G)$ if necessary). Then we apply Lemmas 5.5 and 5.35- 5.39 to obtain $R = 1$, which is a contradiction.

So we may assume that $c+1 = 2^l$. In this case the natural faithful representation of G has dimension $s+1 = 2^{l+1}$. Since either $R \cong 2_+^{1+2k}$ or $R \cong 2_-^{1+2k}$, where $k \leq l+1$, and R admits an automorphism of order $s = 2^{l+1} - 1$, we obtain $R \cong 2_+^{1+2(l+1)}$, $Aut(R) \cong O_{2l+2}^+(2)$ and hence $C_G(t)/C_{C_G(t)}(R) \cong C_s$. Then may again apply Lemmas 5.5 and 5.35- 5.39 to obtain $R = 1$, which is a contradiction. $\square$

Lemma 5.44. *Let $G \cong A_m^{\pm}(q)$, where $m \geq s$ and $(s, q) \neq (5, 3)$. Let X be a p-subgroup of G and let $t \in Inndiag(G)$ such that (G, t, X) is a triple of type (Hs). Then $X = 1$.*

Proof. We work by induction on m, taking Lemma 5.43 as the basis case of our induction. So we assume that $m \geq s+1$ and that if (G, t, X) is a triple of type (Hs) with $G \cong A_{m'}^{\pm}(q')$ for $m' < m$ and $q' \neq 3$, then $X = 1$.

By Corollary 5.32, there exists $Z \leq C_G(t)$ such that $Z \cong C_r \times C_r$. Hence X is a nonabelian 2-group by Corollary 5.22. In particular, as we observed in Remark 5.23, we may assume that $G = G_a$. So by Lemmas 5.4 and 5.5 we have $X\langle t\rangle \leq C_G(z)$ for some involution $z \in Z(X)$ and so $X \leq L = L_1 \circ L_2 \circ ... \circ L_j$, where $L_i = A_{m_i}^{\pm}(q^{a_i})$ and each projection (L_i, t, X_i) is of type (Hs). By Theorem 5.3 (d)-(e) and Lemma 5.34, each L_i has Lie rank $m_i < m$. Since $(s, q) \neq (5, 3)$, we clearly have $(s, q^{a_i}) \neq (5, 3)$. Applying Lemmas 5.36- 5.43 and the inductive hypothesis, we obtain $X_i = 1$ for each i. Hence $X = 1$. $\square$

We conclude our discussion by considering the remaining cases $(s, q) = (5, 3)$.

Lemma 5.45. *Let $G \cong GU_4(3)$, let t be an inner-diagonal automorphism of G of order 5. Suppose that (G, t, X) is a triple of type $(H5)$. Then $X = 1$*

Proof. Since $|G| = 4 \cdot |SU_4(3)|$, we may assume that $t \in SU_4(3)$. Also $X = [X, t] \leq G' \cong SU_4(3)$. So by Lemma 5.37, either $X = 1$ or $X \cong 2_-^{1+4}$. If $X \cong 2_-^{1+4}$, then there exists an element $g \in G - SU_4(3)$ of order 4 with $g \in C_G(t)$ but $g \notin N_G(X)$. This is a contradiction and hence $X = 1$. $\square$

Lemma 5.46. *Let $G \cong A_m^{\pm}(3)$ with $m \geq 4$ and let t be an inner-diagonal automorphism of G of order 5 such that (G, t, X) is a triple of type $(H5)$. Then $X = 1$.*

Proof. We may assume that G is universal by Lemma 5.2. We work by induction on m.

If $m = 4$ we argue as follows. If X is abelian, then the argument of case 1b of Lemma 5.39 applies to give $X = 1$. Hence we may assume that X is nonabelian.

By Lemmas 5.4 and 5.5, we have $X \leq L$, where L is a direct product of linear or unitary groups L_i. Further, by Lemma 5.34, each L_i has Lie rank smaller than 4. By Table 4.5.2 [GLS3] and Lemmas 5.36 and 5.37 we obtain either $X = 1$ or $L \cong SU_4(3)$. In the latter case, we may see by Table 4.5.2 [GLS3] and Lemma 5.4 that in fact $L = O^{r'}(C_G(z))$, where z is an involution, $C_G(z) \cong GU_4(3)$ and $X\langle t\rangle \leq C_G(z)$. Then since $(C_G(z), t, X)$ is a triple of type $(H5)$, we have $X = 1$ by Lemma 5.45.

Now suppose the result holds for $m < l$ and take $m = l$. Then by Corollaries 5.22 and 5.32 and the argument of Lemma 5.43, we may assume that X is a nonabelian 2-group. Hence by Lemmas 5.4 and 5.5 we have $X \leq L = O^{3'}(C_G(z)) = L_1 \circ L_2 \circ ... \circ L_j$, where $z \in Z(X)$ is an involution, each L_i is a linear or unitary group and each projection (L_i, t, X_i) is of type (Hs). By Theorem 5.34, each L_i has Lie rank smaller than m. So by Lemmas 5.36- 5.43 and our inductive hypothesis we have, for each i, either $X_i = 1$ or $L_i \cong A_3^-(3)$.

In the latter case we may see by Tables 4.5.1 and 4.5.2 [GLS3] that the corresponding projection X_i of X may in fact be embedded into $H \cong GU_4(3)$ or $PGU_4(3)$ such that (H, t, X_i) is a triple of type (Hs). Hence $X = 1$ by Lemma 5.45. $\square$

By combining the above lemmas, we obtain the main result of this section.

Proposition 5.47. *Let $G \cong A_m^{\pm}(q)$ where $m \geq 1$. Let X be a p-subgroup of G and let $t \in Inndiag(G)$ such that (G, t, X) is a triple of type (Hs). Then either $X = 1$ or*

(i) $G \cong SU_4(3)$, $s = 5$, $C_G(t) \cong C_4 \times C_5$ and $X \cong 2_-^{1+4}$, or

(ii) G is isomorphic to a quotient of $SU_4(3)$ by its central subgroup of order 2, $s = 5$, $C_G(t) \cong C_2 \times C_5$ and $X \cong E_{2^4}$.

(iii) $G \cong PSU_4(3)$, $s = 5$, $C_G(t) \cong C_5$ and $X \cong E_{2^4}$.

Furthermore, the triples given in (i)-(iii) do indeed exist.

5.3 The Case $G = C_m(q)$

In this section we discuss the case $G = C_m(q)$. We work in analogue with the discussion of $G = A_m^{\pm}(q)$. Hence, we begin with a general result on automorphisms of G.

Lemma 5.48. *Let $G = C_m(q)$ and let x be an inner-diagonal automorphism of G of prime order $r_1 \neq r$. Let $\overline{x}$ be the automorphism of the algebraic group $\overline{G} = C_m$ inducing x on G and let Δ_x be the Dynkin diagram of $C_{\overline{G}}(\overline{x})$. If x is of equal rank type, then Δ_x has type $A_1 \cup C_{m-1}$ or type $C_k \cup C_{m-k}$ for some $2 \leq k \leq m-2$.*

Proof. If x is of equal rank type, then by Theorem 5.3 (f), Δ_x has type C_m, or type $A_1 \cup C_{m-1}$, or type $C_k \cup C_{m-k}$. If Δ_x has type C_m, we get a contradiction since x is a nontrivial automorphism. Hence Δ_x has type $A_1 \cup C_{m-1}$ or type $C_k \cup C_{m-k}$, as required. □

We now obtain our main results. Recall that $q = r^a$, $s \geq 5$ and p, r, s are pairwise distinct.

Lemma 5.49. *Let $G \cong C_m(q)$ with $m < \frac{s-1}{2}$. Let X be a p-subgroup of G and let $t \in Inndiag(G)$ be such that (G, t, X) is a triple of type (Hs). Then $X = 1$.*

Proof. We argue in analogue with the proof of Lemma 5.36. By Lemma 5.19, X must be a nonabelian 2-group. We may assume $G \cong Sp_{2m}(q)$ by Lemma 5.2. Also, by Lemma 2.16, we may assume that t induces an inner automorphism on G.

We work by induction on m. Since $Sp_2(q) \cong SL_2(q)$, we take Lemma 5.35 as the basis case of our induction. Now assume that $m \geq 2$ and that if (G, t, X) is a triple of type (Hs) with $G \cong C_{m'}(q')$ for $m' < m$ and some q', then $X = 1$.

By Lemma 5.6, X contains a critical subgroup Y. Take $R = [Y, t]$. Combining Remark 5.7 and Lemma 5.16, (G, t, R) is a triple of type (Hs) and R is nonabelian. If $Z(R)$ contains an involution z which is not contained in $Z(G)$, then by Lemmas 5.4 and 5.5, $R \leq L = L_1 \times L_2 \times ... \times L_j$, where, for each i, either $L_i \cong A_{m_i}^{\pm}(q^{a_i})$ or $L_i \cong C_{m_i}(q^{a_i})$, and each (L_i, t, R_i) is a triple of type (Hs). Further, if $L_i \cong C_{m_i}(q^{a_i})$, then by Theorem 5.3 (d)-(f) and Lemma 5.48, $m_i < m$. Hence, by the inductive hypothesis and Lemma 5.36, each $R_i = 1$ and so $R = 1$, which is a contradiction. So we may assume that $Z(R)$ contains a unique involution and so, by Lemma 5.8, R is extra-special.

Choose l such that $s = 2^l + c$ where $0 < c < 2^l$. Then we have $2m < s - 1 < 2^{l+1}$. So by Lemma 5.9, we obtain $c = 1$ and $R \cong 2_-^{1+2l}$. Hence $s = 2^l + 1$. In particular, by Lemma 2.22, $2m \geq 2^l = s - 1$. This is a contradiction since we assumed that $m < \frac{s-1}{2}$. Hence $R = 1$ and so $X = 1$. □

We now consider the case $m = \frac{s-1}{2}$, which is the analogue of the case $A^{\pm}_{s-2}(q)$ of Section 5.2.

Lemma 5.50. *Let $G \cong C_{\frac{s-1}{2}}(q)$. Let X be a p-subgroup of G and let $t \in Inndiag(G)$ be such that (G, t, X) is a triple of type (Hs). Then either $X = 1$, or one of the following holds.*

(i) $G \cong Sp_4(3)$, $s = 5$, $C_G(t) \cong C_2 \times C_5$ and $X \cong 2^{1+4}_{-}$

(ii) $G \cong PSp_4(3)$, $s = 5$, $C_G(t) \cong C_5$ and $X \cong E_{2^4}$.

Furthermore, the triples (G, t, X) described in (i), (ii) do indeed exist.

Proof. The proof is analogous to that of Lemma 5.37. By applying Lemma 5.2 we may assume that $G = Sp_{s-1}(q)$. By Lemma 2.16, we may assume that t is an element of G and by Corollary 5.19, X is a nonabelian 2-group.

By Lemma 5.6, X contains a critical subgroup Y. Take $R = [Y, t]$. Combining Remark 5.7 and Lemma 5.16, (G, t, R) is a triple of type (Hs) and R is nonabelian. If $Z(R)$ contains an involution z which is not contained in $Z(G)$, then by Lemmas 5.4 and 5.5, $R \leq L = L_1 \times L_2 \times ... \times L_j$, where, for each i, either $L_i \cong A^{\pm}_{m_i}(q^{a_i})$ or $L_i \cong C_{m_i}(q^{a_i})$, and each (L_i, t, R_i) is a triple of type (Hs). Further, if $L_i \cong C_{m_i}(q^{a_i})$, then by Theorem 5.3 (d)-(f) and Lemma 5.48, $m_i < m$. Hence, by Lemmas 5.36 and 5.49, each $R_i = 1$. So we may assume that $Z(R)$ contains a unique involution. Therefore R is extra-special by Lemma 5.8.

Choose l such that $s = 2^l + c$, where $0 < c < 2^l$. Since R has a faithful representation in $s-1 < 2^{l+1}$ dimensions, Lemma 5.9 gives $c = 1$, $s = 2^l + 1$ and $R \cong 2^{1+2l}_{-}$. By Lemma 5.10, we obtain $C_G(t)/C_{C_G(t)}(R) \cong C_s$.

Suppose that $C_G(t)$ contains an involution z which is not contained in $Z(G)$. Since $C_G(t)/C_{C_G(t)}(R) \cong C_s$, we have $R\langle t\rangle \leq C_G(z)$. Then by Lemma 5.5, we obtain $R \leq L = L_1 \times L_2 \times ... \times L_j$, where for each i, either $L_i \cong A^{\pm}_{m_i}(q^{a_i})$ or $L_i \cong C_{m_i}(q^{a_i})$, and each (L_i, t, R_i) is a triple of type (Hs). Further, if $L_i \cong C_{m_i}(q^{a_i})$, then by Theorem 5.3 (d)-(f) and Lemma 5.48, $m_i < \frac{s-1}{2}$. So by Lemmas 5.36 and 5.49, each $R_i = 1$. Hence $R = 1$, which is a contradiction. So $C_G(t)$ contains a unique involution, namely the unique involution $\alpha \in Z(G)$.

Furthermore, exactly the same argument shows that $C_G(t)$ cannot contain any element having odd order coprime to s and r, and cannot contain any order s-element except for the powers of t. So in particular $m_s(C_G(t)) = 1$. Similarly, if $C_G(t)$ contains an element y which is not contained in $Z(G)$ but such that $y^2 \in Z(G)$, then we may apply the above argument to the images $\bar{R}$ of R and $\bar{t}$ of t in the quotient group $\bar{G} = G/Z(G)$ to show that $\bar{R} = 1$. So $C_G(t)$ contains no such element. Finally, if $C_G(t)$ contains an element u

such that $u^s = t$, then $u \in C_{C_G(t)}(R)$ and so $[R, u] = 1$. Then $[R, t] = 1$ which is also a contradiction. We conclude that $C_G(t)$ has order $2 \cdot s \cdot r^b$ for some b.

By Fermat's little theorem, s divides

$$q^{s-1} - 1 = q^{2^l} - 1 = (q-1) \cdot (q+1) \cdot (q^2+1) \cdot (q^4+1) \cdot \ldots \cdot (q^{2^{l-1}}+1)$$

Since s is prime, s divides one of the factors in the product. If s divides $q-1$ or s divides $q^{2^{l'}}+1$ for $l' < l-1$, then, since those polynomials in q appear with exponent greater than 1 in the factorization of $|G|$, we apply Theorem 5.11 and Corollary 5.12 to obtain $m_s(C_G(t)) \geq 2$, which is a contradiction. Hence s must divide $q^{2^{l-1}}+1$. By Table 1 [B], we may assume that t is contained in a Singer cyclic subgroup S of G, which has order exactly $q^{2^{l-1}}+1 = q^{\frac{s-1}{2}}+1$. Hence $S \leq C_G(t)$.

Since $S \leq C_G(t)$ and S contains no r-elements, $|S| \leq 2s$. We now check whether this can occur.

Claim 5.51. *(i) If n is odd, $n > 5$ and $q \geq 3$, then $q^{\frac{n-1}{2}}+1 > 2n$,*

(ii) If $q > 3$, then $q^2+1 > 10$.

Proof. (i) We work by induction on n. Certainly $q^3+1 > 14$ for $q \geq 3$, which proves the result for $n = 7$. Now suppose the result is true for $n = k$. Then $q^{\frac{(k+2)-1}{2}}+1 = q(q^{\frac{k-1}{2}}+1) - q + 1 > 2kq - q + 1$ by the inductive hypothesis. Since certainly $2kq - q + 1 > 2(k+1)$ for $q \geq 3$, the result holds for $n = k+2$.

(ii) This is trivial. $\square$

Suppose that $s > 5$. Since $p = 2$, we have $q \geq 3$. Then since $q^{\frac{s-1}{2}}+1 = |S| \leq 2s$, we have a contradiction with Claim 5.51 (i). So we may assume that $s = 5$. If $q > 3$, then since $q^2+1 = |S| \leq 10$, we have a contradiction with Claim 5.51 (ii). So we may assume that $q = 3$. Hence $G = Sp_4(3)$. Since $5 = s = 2^l+1$, we have $l = 2$ so that $R \cong 2_-^{1+4}$. So a priori we may have a triple (G, t, R) of type (Hs) with $G \cong Sp_4(3)$, $s = 5$ and $R \cong 2_-^{1+4}$. In this case, looking at the list of maximal subgroups in Chapter 5 [K3] shows that $N_G(X)$ must be contained in a maximal subgroup $M \cong 2_-^{1+4}.O_4^-(2) \cong N_G(R)$ of G. So we have $X = R$.

It remains to show that such triples do indeed exist. By the lists in Chapter 5 [K3], $G = Sp_4(3)$ has a maximal subgroup $M \cong 2_-^{1+4}.O_4^-(2)$. Thus G has a subgroup $X \cong 2_-^{1+4}$ which is normalized by a 5-element t. By [ATLAS], any order 5 element of $PSp_4(3)$ has centralizer isomorphic to C_5. Hence $C_G(t) \cong C_2 \times C_5$. Since we certainly have $Z(G) \leq N_G(X)$ we see that $C_G(t) \leq N_G(X)$. Finally the only elements of X which are centralized by t lie in $Z(X)$, so $X = [X, t]$ and we have a triple $(Sp_4(3), t, X)$ of type $(H5)$.

Passing to the adjoint group $PSp_4(3)$ we find a triple (G, t_0, X_0) of type (Hs) satisfying $C_G(t_0) \cong C_5$ and $X_0 \cong E_{2^4}$. $\square$

We now discuss the case $m \geq \frac{s+1}{2}$. Since we found triples of type $(H5)$ in $C_2(3)$ we will separate the cases $(s, q) \neq (5, 3)$ and $(s, q) = (5, 3)$.

Lemma 5.52. *Let $G \cong C_{\frac{s+1}{2}}(q)$, where $(s, q) \neq (5, 3)$. Let X be a p-subgroup of G and let $t \in Inndiag(G)$ be such that (G, t, X) is a triple of type (Hs). Then $X = 1$.*

Proof. By Lemma 2.16, we may assume that t induces an inner automorphism on G.

We argue in analogue with Lemma 5.43. By Lemma 2.13, there exists an order s automorphism $\bar{t}$ of the algebraic group $\overline{G} \cong C_{\frac{s+1}{2}}$ over $\overline{\mathbb{F}}_r$ which induces t on G. The Dynkin diagram of $\overline{G}$ has $\frac{s+1}{2}$ nodes. By Theorem 5.3, $L = O^{r'}(C_G(t))$ is a central product $L_1 \circ L_2 \circ ... \circ L_j$ of groups L_i such that the Dynkin diagram of $C_{\overline{G}}(\bar{t})$ is the disjoint union of diagrams Δ_i for $i = 1, 2, ..., j$ where each Δ_i is in turn a disjoint union of a_i copies of the Dynkin diagram of L_i. By Proposition 5.24 (ii), the Dynkin diagram for $C_{\overline{G}}(\bar{t})$ has at least 1 node, and hence $L \neq 1$. In particular $m_r(L) \geq 1$.

If $m_r(L) \geq 2$, then X is a nonabelian 2-group by Corollary 5.22. As discussed in Remark 5.23 we may assume that $G = G_a$. Then by Lemmas 5.4 and 5.5, we have $X\langle t\rangle \leq M_1 \circ M_2 \circ ... \circ M_j$, where for each i, either $M_i \cong A^{\pm}_{m_i}(q^{a_i})$ or $M_i \cong C_{m_i}(q^{a_i})$, and each (M_i, t, X_i) is a triple of type (Hs). Further, if $M_i \cong C_{m_i}(q^{a_i})$, then by Theorem 5.3 (d)-(f) and Lemma 5.48, $m_i < \frac{s+1}{2}$. Then we apply Lemmas 5.49 and 5.50 and Proposition 5.47 to conclude that $X = 1$.

So we may assume that $m_r(L) = 1$, and by Table 3.3.1 [GLS3] we obtain $q = r$ and $L = A_1(r)$. In particular $G \cong C_{\frac{s+1}{2}}(r)$. By Lemma 5.2, we may assume that $G = Sp_{s+1}(r)$. We are now in the conditions of Claim 5.42, so we may assume that X is nonabelian.

Suppose that p is odd. Then since $|Z(G)| = (2, q-1)$, $Z(X)$ contains a p-element z not contained in $Z(G)$. By Lemma 5.4, we have $X\langle t\rangle \leq C_G(z)$ and we may apply Lemmas 5.5, 5.49 and 5.50 and Proposition 5.47 to conclude that $X = 1$.

Therefore we may assume that $p = 2$. By Lemma 5.6, X contains a critical subgroup Y. Let $R = [Y, t]$. As discussed in Remark 5.7, (G, t, R) is a triple of type (Hs). By Claim 5.42, R is nonabelian. If $Z(R)$ contains an involution not contained in $Z(G)$, then $R\langle t\rangle \leq C_G(z)$ and we may apply Lemmas 5.5, 5.49 and 5.50 and Proposition 5.47 to obtain $Y = 1$. So we may assume that $Z(R)$ contains a unique involution and by Lemma 5.8, R is extra-special.

Choose l such that $s = 2^l + c$, where $0 < c < 2^l$. Suppose first that $c + 1 < 2^l$. Then G has a faithful representation in $n = s + 1 < 2^{l+1}$ dimensions. Since R admits an order s automorphism and has a faithful representation in dimension smaller than 2^{l+1}, Lemma 5.9 gives $c = 1$ and $R \cong 2_-^{1+2l}$. Hence $s = 2^l + 1$. So by Lemma 5.10, we have $C_G(t)/C_{C_G(t)}(R) \cong C_s$. However, we have $O^{r'}(C_G(t)) \cong A_1(r)$. Since $A_1(r)$ does not contain a central element of order s, the whole of $O^{r'}(C_G(t))$ centralizes R. Hence $R\langle t\rangle \leq C_G(z)$ for some involution z (passing to the quotient group $\bar{G} = G/Z(G)$ to avoid the case $z \in Z(G)$ if necessary). Then we apply Lemmas 5.5, 5.49 and 5.50 and Proposition 5.47 to obtain $R = 1$, which is a contradiction.

So we may assume that $c+1 = 2^l$. In this case the natural faithful representation of G has dimension $s+1 = 2^{l+1}$. Since either $R \cong 2_+^{1+2k}$ or $R \cong 2_-^{1+2k}$, where $k \leq l+1$, and R admits an automorphism of order $s = 2^{l+1} - 1$, we obtain $R \cong 2_+^{1+2(l+1)}$, $Aut(R) \cong O_{2l+2}^+(2)$ and hence $C_G(t)/C_{C_G(t)}(R) \cong C_s$. Then may again apply Lemmas 5.5, 5.49 and 5.50 and Proposition 5.47 to obtain $R = 1$, which is a contradiction. $\square$

Lemma 5.53. *Let $G \cong C_m(q)$ where $m \geq \frac{s+1}{2}$ and $(s,q) \neq (5,3)$. Let X be a p-subgroup of G and let $t \in Inndiag(G)$ be such that (G,t,X) is a triple of type (Hs). Then $X = 1$.*

Proof. We work by induction on m, taking Lemma 5.52 as the basis case of our induction. So we assume that $m \geq \frac{s+3}{2}$ and that if (G,t,X) is a triple of type (Hs) with $G \cong C_{m'}(q')$ for $m' < m$ and $q' \neq 3$, then $X = 1$.

By Corollary 5.32, there exists $Z \leq C_G(t)$ such that $Z \cong C_r \times C_r$. Hence X is a nonabelian 2-group by Corollary 5.22. So as we observed in Remark 5.23, we may assume that $G = G_a$. By Lemmas 5.4 and 5.5, we have $X\langle t\rangle \leq C_G(z)$ for some involution $z \in Z(X)$ and so $X \leq L = L_1 \circ L_2 \circ ... \circ L_j$, where for each i, either $L_i \cong A_{m_i}^{\pm}(q^{a_i})$ or $L_i \cong C_{m_i}(q^{a_i})$, and each (L_i, t, R_i) is a triple of type (Hs). Further, if $L_i \cong C_{m_i}(q^{a_i})$, then by Theorem 5.3 (d)-(f) and Lemma 5.48, $m_i < \frac{s-1}{2}$. Since $(s,q) \neq (5,3)$, we clearly have $(s, q^{a_i}) \neq (5,3)$. So by Proposition 5.47 and the inductive hypothesis we conclude that $X = 1$. $\square$

As in the $A_m^{\pm}(q)$ case, we conclude the discussion with the exceptional case $(s,q) = (5,3)$.

Lemma 5.54. *Let $G = C_3(3)$. Let X be a p-subgroup of G and let $t \in Inndiag(G)$ be such that (G,t,X) is a triple of type $(H5)$. Then either $X = 1$ or one of the following holds.*

(i) $G \cong Sp_6(3)$, $X \cong 2_-^{1+4}$ and $t \in G$ with $C_G(t) \cong Sp_2(3) \times C_2 \times C_5$.

(ii) $G \cong PSp_6(3)$, $X \cong 2_-^{1+4}$ and $t \in G$ with $C_G(t) \cong Sp_2(3) \times C_5$.

Furthermore, the triples described in (i), (ii) do indeed exist.

Proof. Suppose first that $m_3(O^{3'}(C_G(t))) \geq 2$. Then X is a nonabelian 2-group by Corollary 5.22. As discussed in Remark 5.23 we may assume that $G = G_a$. Then by Lemmas 5.4 and 5.5, we have $X \leq L = O^{3'}(C_G(z))$, where $z \in Z(X)$ is an involution. Since $m = 3$ is odd and $q \equiv -1 \mod 4$, Table 4.5.1 [GLS3] tells us that $L \cong Sp_2(3) \circ Sp_4(3)$ or $L \cong A_2^-(3)$.

First suppose that $L \cong A_2^{\pm}(3)$. By Lemma 5.5, (L, t, X) is a triple of type $(H5)$. So by Lemma 5.36, $X = 1$.

So we may assume that $L \cong L_1 \circ L_2$, where $L_1 = Sp_2(3)$ and $L_2 = Sp_4(3)$. By Lemma 5.5, each projection (L_i, t, X_i) for $i = 1, 2$ is a triple of type $(H5)$. By Lemma 5.35, $X_1 = 1$ and by Lemma 5.50, either $X_2 = 1$ or $X_2 \cong 2_-^{1+4}$. So either $X = 1$ or $X \cong 2_-^{1+4}$ and a priori, we may have a triple (G, t, X) of type $(H5)$ with $X \cong 2_-^{1+4}$.

The only remaining possibility is that $m_3(O^{3'}(C_G(t))) = 1$. Applying Proposition 5.24 (ii), Theorem 5.3 and Table 3.3.1 [GLS3], we obtain $O^{3'}(C_G(t)) = A_1(3)$. By Lemma 5.2, we may assume that $G = Sp_6(q)$. We are now in the conditions of Claim 5.42, so we may assume that $p = 2$ and that X is a 2-group with an extraspecial subgroup R such that (G, t, R) is of type (Hs). Since R admits an order 5 automorphism and has a faithful representation in dimension 6, we may apply Lemma 5.9 to obtain $R \cong 2_-^{1+4}$. So again we may have a triple (G, t, R) of type $(H5)$ with $R \cong 2_-^{1+4}$.

It remains to show that such triples do indeed exist. By the lists in Chapter 5 [K3], $G = Sp_6(3)$ has a maximal subgroup $M \cong L_1 \times L_2$, where $L_1 = Sp_2(3)$ and $L_2 = Sp_4(3)$. By Lemma 5.50, there is a triple (L_2, t_2, X_2) of type $(H5)$ such that $X_2 \cong 2_-^{1+4}$ and $C_{L_2}(t_2) \cong C_2 \times C_5$. In particular, there is a subgroup $X \cong 2_-^{1+4}$ of M which projects trivially onto L_1 and an element $t \in M$ of order 5 which acts trivially on L_1 and acts as an inner automorphism on L_2.

We want to calculate the full centralizer $C_G(t)$ of t in G. Since 5 divides $|G|$ exactly once, there is only a single isomorphism type for the centralizer of a 5-element. Certainly $C_G(t)$ is contained in some maximal subgroup M_0 of G. Since $t \in M_0$, the order $|M_0|$ is divisible by 5. By the list of maximal subgroups of $Sp_6(q)$ in Chapter 5 [K3], the only possibilities are $M_0 \cong A_5$ or $M_0 \cong Sp_2(3) \times Sp_4(3)$. If $M_0 \cong A_5$, then $C_G(t) \cong C_5$. If $M_0 \cong Sp_2(3) \times Sp_4(3)$, then by the observations of Lemma 5.37, $C_G(t) \cong Sp_2(3) \times C_2 \times C_5$.

So by Lemma 5.50, $X = [X, t]$ and $C_G(t) = C_M(t) \leq N_M(X) \leq N_G(X)$. Hence (G, t, X) is a triple of type $(H5)$ with the required properties. Passing to the adjoint group $PSp_6(3)$, we obtain a triple (G, t_0, X_0) with $X_0 \cong 2_-^{1+4}$ and $C_G(t_0) \cong Sp_2(3) \times C_5$. □

Lemma 5.55. *Let $G \cong C_m(3)$ with $m \geq 3$ and suppose (G, t, X) is a triple of type $(H5)$ with $t \in Inndiag(G)$. Then either $X = 1$ or one of the following holds.*

(a) $G \cong Sp_{2m}(3)$, $X \cong 2_-^{1+4}$ and $t \in G$ with $C_G(t) \cong Sp_{2m-4}(3) \times C_2 \times C_5$,

(b)$G \cong PSp_{2m}(3)$, $X \cong 2_-^{1+4}$ and $t \in G$ with $C_G(t) \cong Sp_{2m-4}(3) \times C_5$

Proof. We work by induction on m, taking Lemma 5.54 as our basis case.

By Corollary 5.32, $C_G(t)$ contains a subgroup $Z \cong C_r \times C_r$. So by Corollary 5.22, X is a nonabelian 2-group. So as discussed in Remark 5.23, we may assume that $G = G_a$. Then by Lemmas 5.4 and 5.5, we obtain $X \leq L = O^{3'}(C_G(z))$ where $z \in Z(X)$ is an involution. The group L is a central product of groups $L_i \in Lie(3)$. By Table 4.5.1 [GLS3], one of the following holds.

(a) $L \cong Sp_{2j}(3) \circ Sp_{2m-2j}(3)$ (for some $1 \leq j < m/2$),

(a1) $L \cong Sp_m(3) \circ Sp_m(3)$ (only if m is even),

(b) $L \cong PSp_m(9)$ (only if m is even),

(c) L is a quotient of $PSU_m(3)$ by a central subgroup of order $(2, m)$.

By Lemma 5.5, each projection (L_i, t, X_i) is a triple of type $(H5)$. So in case (b) we apply Lemmas 5.49 - 5.53 to immediately obtain $X = 1$. In case (c), if $m > 4$ we apply Proposition 5.47 to obtain $X = 1$, whilst if $m = 4$, then we apply the description of $C_G(z)$ in Table 4.5.1 [GLS3] to see that in fact $X\langle t\rangle$ can be embedded in some central quotient of $GU_4(3)$. Then Lemma 5.45 gives $X = 1$.

It remains to address cases (a) and (a1). Label the components of L by $L_1 = Sp_{2j}(3)$ and $L_2 = Sp_{2m-2j}(3)$ and write t_i for $i = 1, 2$ to denote the action of t on L_i. By the inductive hypothesis and Lemma 5.50, we have either $X_1 = 1$, or $X_1 \cong 2^{1+4}_-$ and $C_{L_1}(t_1) \cong Sp_{2j-4}(3) \times C_2 \times C_5$. Similarly either $X_2 = 1$, or $X_2 \cong 2^{1+4}_-$ and $C_{L_2}(t_2) \cong Sp_{2m-2j-4}(3) \times C_2 \times C_5$.

Suppose first that both X_1 and X_2 are nontrivial. We now consider the action of z on $C_G(t)$. Since $Z(X)$ is a characteristic subgroup of X, we obtain $[C_G(t), z] \leq Z(X) \cap C_G(t)$. Since for $i = 1, 2$, we have $X_i \cong 2^{1+4}_-$, either $Z(X) \cong C_2$ or $Z(X) \cong C_2 \times C_2$. In the former case it is easily seen that $[C_G(t), z] = 1$. In the latter case, since $C_G(t)$ induces an automorphism of $Z(X)$, we have a homomorphism $\phi : C_G(t) \to Aut(Z(X)) \cong S_3$. Since the kernel of ϕ is a normal subgroup, and by Theorem 5.3, $O^{3'}(C_G(t))$ is a central product of quasisimple groups, we must have $ker(\phi) = C_G(t)$ and so $[C_G(t), z] = 1$.

By Lemma 2.13, there exists an order 5 automorphism $\bar{t}$ of the algebraic group $\overline{G} = C_m$ which induces t on G. Since $O^{3'}(C_G(t)) \leq L$, $C_{L_1}(t_1) \cong Sp_{2j-4}(3) \times C_2 \times C_5$ and $C_{L_2}(t_2) \cong Sp_{2m-2j-4}(3) \times C_2 \times C_5$, we apply Theorem 5.3 (d)-(f) to see that would have to erase more than 2 nodes from the Dynkin diagram for $\overline{G}$ to obtain the Dynkin diagram for $C_{\overline{G}}(\bar{t})$. This contradicts Proposition 5.24 (ii). So we may assume that at least one of X_1 or X_2 is trivial.

Furthermore, by the same argument on Dynkin diagrams as above we have that if $X_1 \neq 1$ then t acts trivially on L_2 and vice versa. So either $C_{L_1(t)} \cong Sp_{2j-4}(3) \times C_2 \times C_5$ and $C_{L_2}(t) \cong Sp_{2m-2j}(3)$, or $C_{L_1}(t) \cong Sp_{2j}(3)$ and $C_{L_2}(t) \cong Sp_{2m-2j-4}(3) \times C_2 \times C_5$. So either $C_L(t) \cong (Sp_{2j-4}(3) \times C_2 \times C_5) \circ Sp_{2m-2j}(3)$ or $C_L(t) \cong Sp_{2j}(3) \circ (Sp_{2m-2j-4}(3) \times C_2 \times C_5)$.

In either case we have $C_G(t) \cong Sp_{2m-4}(3) \circ (C_2 \times C_5) = Sp_{2m-4}(3) \times C_5$ and X is a group projecting trivially onto at least one of the L_i, and so $X \cong 2^{1+4}_-$. Lifting to the universal group $G = Sp_{2m}(q)$, we still have $X \cong 2_-^{1+4}$ and now we have $C_G(t) \cong Sp_{2m-4}(3) \times C_2 \times C_5$. $\square$

We now combine Lemmas 5.49- 5.55 to obtain the main result of this section.

Proposition 5.56. *Let $G \cong C_m(q)$ where $m \geq 2$. Let X be a p-subgroup of G and let $t \in Inndiag(G)$ such that (G, t, X) is a triple of type (Hs). Then either $X = 1$ or*

(i) $G \cong Sp_{2m}(3)$, $s = 5$, $X \cong 2_-^{1+4}$ and $t \in G$ with $C_G(t) \cong Sp_{2m-4}(3) \times C_2 \times C_5$,

(ii)$G \cong PSp_{2m}(3)$, $s = 5$, $X \cong 2_-^{1+4}$ and $t \in G$ with $C_G(t) \cong Sp_{2m-4}(3) \times C_5$

5.4 The Cases $G = B_m(q)$, $G = D_m^{\pm}(q)$, $G = {}^2B_2(2^{1+2a})$ and $G = {}^3D_4(q)$

In this section we deal with the orthogonal groups $B_m(q)$, $D_m^{\pm}(q)$ and the related twisted groups ${}^2B_2(2^{1+2a})$ and ${}^3D_4(q)$. We begin with a general observation about automorphisms of these groups.

Lemma 5.57. *Let $G \in Lie(r)$ and let x be an inner-diagonal automorphism of G of prime order $r_1 \neq r$. Let $\overline{x}$ be the automorphism of the algebraic group $\overline{G}$ inducing x on G and let Δ_x be the Dynkin diagram of $C_{\overline{G}}(\overline{x})$. Suppose that x is of equal rank type. Then the following hold.*

(a) If $\overline{G} = B_m$, then Δ_x has type $A_1 \cup A_1 \cup B_{m-2}$, or $A_3 \cup B_{m-3}$, or D_m, or $D_k \cup B_{m-k}$ for some $4 \leq k \leq m-1$.

(b) If $\overline{G} = D_m$, then Δ_x has type $A_1 \cup A_1 \cup D_{m-2}$, or $A_3 \cup D_{m-3}$, or $D_k \cup D_{m-k}$ for some $4 \leq k \leq m-4$.

Proof. (a) If x is of equal rank type, then by Theorem 5.3 (f), Δ_x has type B_m, or $A_1 \cup A_1 \cup B_{m-2}$, or $A_3 \cup B_{m-3}$, or D_m, or $D_k \cup B_{m-k}$. If Δ_x has type B_m, we get a contradiction since x is a nontrivial automorphism. Hence Δ_x has one of the other types, as required.

(b) This is exactly analogous to part (a). □

We now obtain the main results of this section. Recall that $q = r^a$ and that p, r, s are assumed to be pairwise distinct.

We first deal with the twisted groups ${}^2B_2(2^{1+2a})$ and $G = {}^3D_4(q)$.

Lemma 5.58. *Let $G \cong {}^2B_2(2^{1+2a})$. Let X be a p-subgroup of G and let $t \in Inndiag(G)$ be such that (G, t, X) is a triple of type (Hs). Then $X = 1$.*

Proof. The group G has a faithful 4-dimensional representation. Since $4 < s$, we may apply Corollary 5.19 to obtain that X is a nonabelian 2-group. In particular, $p = 2$. This is a contradiction since $p \neq r$ by assumption. □

Lemma 5.59. *Let $G \cong {}^3D_4(q)$. Let X be a p-subgroup of G and let $t \in Inndiag(G)$ be such that (G, t, X) is a triple of type (Hs). Then $X = 1$.*

Proof. By Lemma 2.16, we may assume that t induces an inner automorphism on G. Suppose first that X is abelian. Observe that $|G|$ factorizes as

$$|G| = q^{12} \cdot (q-1)^2 \cdot (q+1)^2 \cdot (q^2+q+1)^2 \cdot (q^2-q+1)^2 \cdot (q^4-q^2+1)$$

If $\Phi_i(q)$ denotes the ith cyclotomic polynomial, then

$$|G| = q^{12} \cdot \Phi_1(q)^2 \cdot \Phi_2(q)^2 \cdot \Phi_3(q)^2 \cdot \Phi_6(q)^2 \cdot \Phi_{12}(q)$$

Since s is prime, $s \neq r$, s must divide some $\Phi_i(q)$. Suppose that s divides $\Phi_i(q)$ for some $i \in \{1, 2, 3, 6\}$. Then since each such $\Phi_i(q)$ appears with exponent larger than 1 in the factorization of $|G|$, we may apply Theorem 5.11 to obtain $m_s(G) \geq 2$. By Corollary 5.12, $m_s(C_G(t)) \geq 2$. So $C_G(t)$ has a subgroup $Z = \langle t, t_1 \rangle \cong C_s^2$. By Theorem 3.5, $X = \langle C_X(u) : u \in Z^\# \rangle$. Choose $u \in Z^\#$ such that $C_X(u)$ is as large as possible. By Theorem 5.1 (iii), we have $C_X(t) = 1$, so we may assume that u is not a power of t. Certainly $C_X(u)\langle t \rangle \leq C_G(u)$. Since u has order $s \neq r$, we are in the conditions of Lemma 5.5. So $C_X(u) \leq L = L_1 \circ L_2 \circ ... \circ L_j$, where each $L_i \in Lie(r)$ and each projection $(L_i, t, C_X(u)_i)$ is a triple of type (Hs). Further, by Theorem 5.3 (d)-(f) and Lemma 5.57, each $L_i \cong A^{\pm}_{m_i}(q^{a_i})$ with $m_i \leq 3$. So by Proposition 5.47, each $C_X(u)_i = 1$ unless $(s, q) = (5, 3)$ and $L = L_1 \cong A_3^-(3)$. However, 5 does not divide $|{}^3D_4(3)|$ so this would give a contradiction. Hence each $C_X(u)_i = 1$ and so $C_X(u) = 1$. We chose $C_X(u)$ to be as large as possible and so $X = 1$.

Hence we may assume that s divides $\Phi_{12}(q) = q^4 - q^2 + 1$. Since X is abelian and G has a faithful 8-dimensional representation, we may apply Lemma 5.16 to obtain $s < 8$. So either $s = 5$ or $s = 7$. Since $r \neq s$ we have that either $q^4 - q^2 + 1 \equiv 1$ or $q^4 - q^2 + 1 \equiv 3 \mod 5$ and that $q^4 - q^2 + 1 \equiv 1$, $q^4 - q^2 + 1 \equiv 3$ or $q^4 - q^2 + 1 \equiv 1 \mod 7$. This contradicts the fact that s divides $\Phi_{12}(q)$.

So we may assume that X is nonabelian. By Lemmas 5.4 and 5.5, we have $X \leq L = O^{r'}(C_G(z)) = L_1 \circ L_2 \circ ... \circ L_j$ for some $z \in Z(X)$ of order p, where each $L_i \in Lie(r)$ and each projection (L_i, t, X_i) is a triple of type (Hs). Further, by Theorem 5.3 (d)-(f) and Lemma 5.57, each $L_i \cong A^{\pm}_{m_i}(q^{a_i})$ with $m_i \leq 3$. So by Proposition 5.47, each $X_i = 1$ unless $(s, q) = (5, 3)$ and $L = L_1 \cong A_3^-(3)$. As we observed above, 5 does not divide $|{}^3D_4(3)|$ so this would give a contradiction. Hence each $X_i = 1$ and so $X = 1$. □

For the remainder of this section we will be looking at triples (G, t, X) of type (Hs) in the groups $G = B_m(q)$ and $G = D^{\pm}_m(q)$. By Proposition 2.9.1 [KL], we have $B_2(q) = C_2(q)$, $D_2^+(q) = A_1(q) \times A_1(q)$, $D_2^-(q) = A_1(q^2)$ and $D_3^{\pm}(q) = A_3^{\pm}(q)$. Hence if $G = B_m(q)$, we may assume that $m \geq 3$ and if $G = D^{\pm}_m(q)$, we may assume that $m \geq 4$.

Remark 5.60. *Table 2.2 [GLS3] gives that $|Z(G_u)|$ is a power of 2. So in the case $G = B_m(q)$, we may apply Lemma 5.2 (ii) to assume that $G = \Omega_{2m+1}(q)$. In the case $G = D^{\pm}_m(q)$, applying arguments analogous to Lemma 5.2 (i) and (ii) shows that there is a triple of type (Hs) in the classical version $\Omega^{\pm}_{2m}(q)$ of G if and only if there is such a triple in the universal version, if and only if there is such a triple in the adjoint version.*

Therefore we may assume that $G = \Omega^{\pm}_{2m}(q)$. Further, by Lemma 2.16, we may assume throughout that t induces an inner automorphism on G.

Lemma 5.61. *Let s be a prime and let $6 \leq n < s$. Suppose that either*

(1) $G = B_m(q)$, where $n = 2m + 1$ or

(2) $G = D^{\pm}_m(q)$, where $n = 2m$.

Let X be a p-subgroup of G and let $t \in Inndiag(G)$ be such that (G, t, X) is a triple of type (Hs). Then $X = 1$.

Proof. As discussed in Remark 5.60, we may assume that $G = \Omega_n(q)$ if n is odd and that $G = \Omega^{\pm}_n(q)$ if n is even. We will work by induction on the dimension n of the natural module for G. As we observed above, $D^{\pm}_3(q) = A^{\pm}_3(q)$. Certainly $s > 5$, so we may take the $m = 3$ case of Lemma 5.36 as the basis case for our induction.

So we will assume that if (G, t, X) is a triple of type (Hs) where $G = \Omega_{n'}(q')$ or $G = \Omega^{\pm}_{n'}(q')$, with the natural module of dimension $n' < n$, then $X = 1$.

By Lemma 5.19, X is a nonabelian 2-group. So by Lemma 5.6, X contains a critical subgroup Y. Take $R = [Y, t]$. Combining Remark 5.7 and Lemma 5.16, (G, t, R) is a triple of type (Hs) and R is nonabelian. If $Z(R)$ contains an involution z which is not contained in $Z(G)$, then by Lemmas 5.4 and 5.5, $R \leq L = L_1 \times L_2 \times ... \times L_j$, where, for each i, $L_i \cong A^{\pm}_{m_i}(q^{a_i})$ or $L_i \cong B_{m_i}(q^{a_i})$, or $L_i \cong D^{\pm}_{m_i}(q^{a_i})$, and each (L_i, t, R_i) is a triple of type (Hs). Further, by Theorem 5.3 (d)-(f) and Lemma 5.57, if $L_i \cong B_{m_i}(q^{a_i})$, then the natural module for L_i has dimension $2m_i + 1 < n$ and if $L_i \cong D^{\pm}_{m_i}(q^{a_i})$, then the natural module for L_i has dimension $2m_i < n$. Hence, by the inductive hypothesis and Lemma 5.36, each $R_i = 1$ and so $R = 1$, which is a contradiction. So we may assume that any involution in $Z(R)$ is also contained in $Z(G)$. If n odd and $G = \Omega_n(q)$, then $Z(G) = 1$ by Table 2.1.D [KL]. Hence $Z(R) = 1$, which is a contradiction since R is a 2-group. So we may assume that n is even and that $G = \Omega^{\pm}_n(q)$.

In particular, we may assume that $Z(R)$ contains a unique involution, namely the unique order 2 element α of $Z(G)$. By Lemma 5.8, R is extra-special. Choose l such that $s = 2^l + c$ where $0 < c < 2^l$. Then since R has a representation in $n < s < 2^{l+1}$ dimensions, we may apply Lemma 5.9 to obtain $c = 1$ and $R \cong 2^{1+2l}_{-}$. Hence $s = 2^l + 1$. In particular, by Lemma 2.22, $n \geq 2^l = s - 1$. Since also $n < s$, we have $n = s - 1 = 2^l$. So $G = \Omega^{\pm}_{2^l}(q)$. Furthermore, we are in the conditions of Lemma 5.10, so we have $C_G(t)/C_{C_G(t)}(R) \cong C_s$.

Suppose that $C_G(t)$ contains an involution z which is not contained in $Z(G)$. Since $C_G(t)/C_{C_G(t)}(R) \cong C_s$, we have $R\langle t \rangle \leq C_G(z)$. Then by Lemma 5.5, we obtain $R \leq L = L_1 \times L_2 \times ... \times L_j$, where for each i, either $L_i \cong A^{\pm}_{m_i}(q^{a_i})$ or $L_i \cong D^{\pm}_{m_i}(q^{a_i})$, and each (L_i, t, R_i) is a triple of type (Hs). Further, by Theorem 5.6 (d)-(f) and Lemma 5.57, if $L_i \cong D^{\pm}_{m_i}(q^{a_i})$, then the natural module for L_i has dimension $2m_i < n$. Hence, by the inductive hypothesis and Lemma 5.36, each $R_i = 1$ and so $R = 1$, which is a contradiction. So $C_G(t)$ contains a unique involution, namely the involution $\alpha \in Z(G)$.

Furthermore, exactly the same argument shows that $C_G(t)$ cannot contain any element having odd order coprime to s and r, and cannot contain any order s-element except for the powers of t. So in particular $m_s(C_G(t)) = 1$. Similarly, if $C_G(t)$ contains an element y which is not contained in $Z(G)$ but such that $y^2 \in Z(G)$, then we may apply the above argument to the images $\bar{R}$ of R and $\bar{t}$ of t in the quotient group $\bar{G} = G/Z(G)$ to show that $\bar{R} = 1$. So $C_G(t)$ contains no such element. Finally, if $C_G(t)$ contains an element u such that $u^s = t$, then $u \in C_{C_G(t)}(R)$ and so $[R, u] = 1$. Then $[R, t] = 1$ which is also a contradiction. We conclude that $C_G(t)$ has order $2 \cdot s \cdot r^b$ for some b.

By Fermat's little theorem, s divides

$$q^{s-1} - 1 = q^{2^l} - 1 = (q-1) \cdot (q+1) \cdot (q^2+1) \cdot (q^4+1) \cdot \ldots \cdot (q^{2^{l-1}} + 1)$$

Since s is prime, s divides one of the factors in the product.

Suppose that $G = \Omega^+_{2^l}(q)$. If s divides $q - 1$ or s divides $q^{2^{l'}} + 1$ for $l' < l - 1$, then since these polynomials in q appear with exponent greater than 1 in the factorization of $|G|$, we may apply Theorem 5.11 and Corollary 5.12 to obtain $m_s(C_G(t)) \geq 2$. This is a contradiction since we showed above that $m_s(C_G(t)) = 1$. Hence s must divide $(q^{2^{l-1}} + 1)$. This is a contradiction since this polynomial does not appear in the factorization of $|G|$.

Therefore $G = \Omega^-_{2^l}(q)$. If s divides $q-1$ or s divides $q^{2^{l'}}+1$ for $l' < l-2$ then we may apply Theorem 5.11 and Corollary 5.12 exactly as above to obtain $m_s(C_G(t)) \geq 2$, which is a contradiction. So either s divides $q^{2^{l-2}}+1$ or s divides $q^{2^{l-1}}+1$. In the latter case, since s does not divide any of the other cyclotomic polynomials in the above factorization, we may assume that t is contained in a Singer cyclic subgroup S_2 of order $\frac{1}{2}(q^{2^{l-1}}+1) = \frac{1}{2}(q^{\frac{s-1}{2}}+1)$ in G. Hence $S_2 \leq C_G(t)$. In the former case, since s divides $q^{2^{l-2}} + 1$ but does not divide any of the other cyclotomic polynomials in the above factorization, we may assume that t is contained in a subgroup $H \cong \Omega^-_{2^{l-1}}(q)$ of G. In fact, by the same argument, we may assume that t is contained in a Singer cyclic subgroup S_1 of order $\frac{1}{2}(q^{2^{l-2}}+1) = \frac{1}{2}(q^{\frac{s-1}{4}}+1)$ in H. Hence $S_1 \leq C_G(t)$.

In either case, S_i contains no r-elements. Since $S_i \leq C_G(t)$ in each case, we have $|S_i| \leq 2s$. Further, since $s > 5$ and s has the form $2^l + 1$, we have $s \geq 17$. We now check whether this situation can occur.

Claim 5.62. *If n odd, $n \geq 17$ and $q \geq 3$, then $q^{\frac{n-1}{4}} + 1 > 4n$.*

Proof. We work by induction on n. Certainly $q^4 + 1 > 68$ for $q \geq 3$ which proves the result for $n = 17$. Now suppose the result is true for $n = k$. Then $q^{\frac{k+1}{4}} + 1 = q^{\frac{1}{2}}(q^{\frac{k-1}{2}} + 1) - q^{\frac{1}{2}} + 1 > 4q^{\frac{1}{2}}k - q^{\frac{1}{2}} + 1$ by the inductive hypothesis. Now $4q^{\frac{1}{2}}k - q^{\frac{1}{2}} + 1 > 4(k+1)$

which proves the result for $n = k + 2$. $\square$

Since $p = 2$ we have $q \geq 3$. Then since s is odd and $s \geq 17$ and $|S_1| \leq |S_2| \leq 2s$, we have an immediate contradiction with Claim 5.62. $\square$

We now discuss the orthogonal group $G = B_{\frac{s-1}{2}}(q)$ of dimension s. If $s = 5$, then $G = B_2(q) = C_2(q)$ and Lemma 5.50 tells us what can happen. So we may assume that $s > 5$. Furthermore, by Theorem 2.2.10, we have $B_m(2^a) \cong C_m(2^a)$ for all a and m and so we may assume that q is odd.

Lemma 5.63. *Let s be a prime, $s > 5$, q odd and $G = B_{\frac{s-1}{2}}(q)$. Let X be a p-subgroup of G and let $t \in Inndiag(G)$ be such that (G, t, X) is a triple of type (Hs). Then $X = 1$.*

Proof. As discussed in Remark 5.60, we may assume that $G = \Omega_s(q)$.

First suppose that X is abelian. By Fermat's little theorem, s divides $q^{s-1} - 1$. Hence s divides $\Phi_i(q)$ for some i dividing $s-1$, where $\Phi_i(q)$ denotes the ith cyclotomic polynomial in q. Observe that if i is odd, then since $s-1$ is even, i divides $\frac{1}{2}(s-1)$.

First assume that either i is odd and $i < \frac{1}{2}(s-1)$, or that i is even and $i < s-1$. Then since $\Phi_i(q)$ appears with exponent greater than 1 in the factorization of $|G|$, we may apply Theorem 5.11 and Corollary 5.12 to obtain $m_s(C_G(t)) \geq 2$. Hence there exists a subgroup $Z := \langle t, t_1 \rangle \cong C_s^2$ of $C_G(t)$. By Theorem 3.5 $X = \langle C_X(u) | u \in Z^\# \rangle$.

Choose $u \in Z^\#$ such that $C_X(u)$ is as large as possible. By Theorem 5.1 (iii), we have $C_X(t) = 1$, so u is not a power of t. Certainly $C_X(u)\langle t \rangle \leq C_G(u)$. Since u has order $s \neq r$, we are in the conditions of Lemma 5.5. So we obtain $C_X(u) \leq L = L_1 \times L_2 \times ... \times L_j$, where, for each i, $L_i \cong A^{\pm}_{m_i}(q^{a_i})$ or $L_i \cong B_{m_i}(q^{a_i})$, or $L_i \cong D^{\pm}_{m_i}(q^{a_i})$, and each $(L_i, t, C_X(u)_i)$ is a triple of type (Hs). Further, by Theorem 5.3 (d)-(f) and Lemma 5.57, if $L_i \cong B_{m_i}(q^{a_i})$, then the natural module for L_i has dimension $2m_i + 1 < s$ and if $L_i \cong D^{\pm}_{m_i}(q^{a_i})$, then the natural module for L_i has dimension $2m_i < s$. So by Proposition 5.47 and Lemma 5.61, each $C_X(u)_i = 1$. Hence $C_X(u) = 1$. As we chose $C_X(u)$ to be as large as possible, we must have $X = 1$.

So we may assume that either $i = \frac{1}{2}(s-1)$ or $i = s-1$. In either case, since $\Phi_i(q)$ appears with exponent 1 in the factorization of $|G|$, we apply Theorem 5.11 and Corollary 5.12 to obtain $m_s(C_G(t)) = 1$.

Now we investigate $C_G(t)$ more closely. Suppose that there exists a nontrivial $h \in C_G(t)$ of prime order coprime to s. If $C_X(h) = 1$, then $X\langle th \rangle$ is a Frobenius group represented faithfully in s dimensions but whose complement has order greater than s. By Lemma 5.14, this is impossible. Hence $C_X(h) \neq 1$ and we consider the group $C_X(h)\langle t \rangle$. By Lemma 5.14, this group acts absolutely irreducibly on the natural module of G. So by Lemma 5.15 we obtain $h \in Z(G)$. Hence $h = 1$. Since h was a general element of prime order coprime to s, we may assume that $C_G(t)$ is an s-group.

Furthermore, there can be no element $u \in G$ such that $u^s = t$, since that would give rise to a Frobenius group $X\langle u \rangle$ with a complement of order s^2. We may conclude that $|C_G(t)| = s$.

Recall that either $i = \frac{1}{2}(s-1)$ or $i = s-1$. Suppose first that $i = \frac{1}{2}(s-1)$. Since s divides $\Phi_{\frac{1}{2}(s-1)}(q)$ and does not divide any of the other cyclotomic polynomials in the factorization of $q^{s-1}-1$, we may assume that t is contained in a subgroup $H_+ \cong \Omega^+_{s-1}(q)$ of G. In fact, by the same argument, we may assume that t is contained inside a cyclic subgroup C_+ of order $\frac{q^{\frac{1}{2}(s-1)}-1}{2}$ of H_+ (namely, if we treat H_+ as a subgroup of $GL_{s-1}(q)$, then C_+ is the intersection of H_+ with a Singer cyclic subgroup of $GL_{s-1}(q)$). Since $C_+ \leq C_G(t)$, we have $|C_+| = s$.

If instead $i = s-1$, then in analogue with the above, we may assume that t is contained in a subgroup $H_- \cong \Omega^-_{s-1}(q)$ of G. In fact, we may assume that t is contained inside a Singer cyclic subgroup C_- of order $\frac{q^{\frac{1}{2}(s-1)}+1}{2}$ of H_-. Since $C_- \leq C_G(t)$, we have $|C_-| = s$.

We now check whether these possibilities can occur.

Claim 5.64. *If n odd, $n \geq 7$ and $q \geq 3$, then $q^{\frac{1}{2}(n-1)} - 1 > 2n$.*

Proof. We work by induction on n. Certainly $q^3 - 1 > 14$ for $q \geq 3$, which proves the result for $n = 7$. Now suppose the result is true for $n = k$. Then $q^{\frac{1}{2}(k+1)} - 1 = q(q^{\frac{1}{2}(k-1)}-1)+q-1 > 2qk+q-1$ by the inductive hypothesis. Since $2qk+q-1 > 2(k+2)$, the result holds for $n = k+2$. $\square$

Since q is odd, certainly $q \geq 3$. Also $s \geq 7$ and $s = |C_\pm| \geq \frac{q^{\frac{1}{2}(s-1)}-1}{2}$, so we have a contradiction with Claim 5.64 (ii).

Therefore X is nonabelian. By Lemmas 5.4 and 5.5, we have $X\langle t \rangle \leq C_G(z)$ for some $z \in Z(X)$ and so $X \leq L = L_1 \cdot L_2 \cdot \ldots \cdot L_j$, where for each i, $L_i \cong A^\pm_{m_i}(q^{a_i})$ or $L_i \cong B_{m_i}(q^{a_i})$, or $L_i \cong D^\pm_{m_i}(q^{a_i})$, and each (L_i, t, X_i) is a triple of type (Hs). Further, by Theorem 5.6 (d)-(f) and Lemma 5.57, if $L_i \cong B_{m_i}(q^{a_i})$, then the natural module for L_i has dimension $2m_i + 1 < s$ and if $L_i \cong D^\pm_{m_i}(q^{a_i})$, then the natural module for L_i has dimension $2m_i < s$. So by Proposition 5.47 and Lemma 5.61, each $X_i = 1$. Hence $X = 1$. $\square$

We next discuss the groups $G = D^\pm_{\frac{s+1}{2}}(q)$ of dimension $s+1$. Recall that if $s = 5$, then $G = D^\pm_3(q) \cong A^\pm_3(q)$ and Lemma 5.37 tells us what can happen. So we may assume that $s > 5$.

Lemma 5.65. *Let s be a prime, $s > 5$. Let $G = D^\pm_{\frac{s+1}{2}}(q)$. Let X be a p-subgroup of G and let $t \in Inndiag(G)$ be such that (G, t, X) is a triple of type (Hs). Then $X = 1$.*

Proof. As discussed in Remark 5.60, we may assume that $G = \Omega^{\pm}_{s+1}(q)$. We argue in analogue with Lemma 5.63. Suppose that X is abelian. By Fermat's little theorem, s divides $q^{s-1} - 1$. Hence s divides $\Phi_i(q)$ for some i dividing $s - 1$.

First assume that either i is odd and $i < \frac{1}{2}(s-1)$, or that i is even and $i < s - 1$. Then since $\Phi_i(q)$ appears with exponent greater than 1 in the factorization of $|G|$, we may apply Theorem 5.11 and Corollary 5.12 to obtain $m_s(C_G(t)) \geq 2$. Hence there exists a subgroup $Z := \langle t, t_1 \rangle \cong C_s^2$ of $C_G(t)$. By Theorem 3.5 $X = \langle C_X(u) | u \in Z^{\#} \rangle$.

Choose $u \in Z^{\#}$ such that $C_X(u)$ is as large as possible. By Theorem 5.1 (iii), we have $C_X(t) = 1$, so u is not a power of t. Certainly $C_X(u)\langle t \rangle \leq C_G(u)$. Since u has order $s \neq r$, we are in the conditions of Lemma 5.5. So we obtain $C_X(u) \leq L = L_1 \times L_2 \times ... \times L_j$, where, for each i, $L_i \cong A^{\pm}_{m_i}(q^{a_i})$ or $L_i \cong B_{m_i}(q^{a_i})$, or $L_i \cong D^{\pm}_{m_i}(q^{a_i})$, and each $(L_i, t, C_X(u)_i)$ is a triple of type (Hs). Further, by Theorem 5.3 (d)-(f) and Lemma 5.57, if $L_i \cong B_{m_i}(q^{a_i})$, then the natural module for L_i has dimension $2m_i + 1 < s + 1$ and if $L_i \cong D^{\pm}_{m_i}(q^{a_i})$, then the natural module for L_i has dimension $2m_i < s + 1$. So by Proposition 5.47 and Lemmas 5.61 and 5.63, each $C_X(u)_i = 1$. Hence $C_X(u) = 1$. As we chose $C_X(u)$ to be as large as possible, we must have $X = 1$.

So we may assume that either $i = \frac{1}{2}(s-1)$ or $i = s-1$. In either case, since $\Phi_i(q)$ appears with exponent 1 in the factorization of $|G|$, we apply Theorem 5.11 and Corollary 5.12 to obtain $m_s(C_G(t)) = 1$.

Now we investigate $C_G(t)$ more closely. Suppose that there exists a nontrivial $h \in C_G(t)$ of prime order coprime to s. If $C_X(h) = 1$, then $X\langle th \rangle$ is a Frobenius group represented faithfully in s dimensions but whose complement has order greater than s. By Lemma 5.14, this is impossible. Hence $C_X(h) \neq 1$ and we consider the group $C_X(h)\langle t \rangle$. By Lemma 5.14, this group acts absolutely irreducibly on the natural module of G. So by Lemma 5.15 we obtain $h \in Z(G)$.

Furthermore, there can be no element $u \in G$ such that $u^s = t$, since that would give rise to a Frobenius group $X\langle u \rangle$ with a complement of order s^2. We may conclude that $|C_G(t)| \leq (2, q-1) \cdot s$.

Recall that either $i = \frac{1}{2}(s-1)$ or $i = s-1$. Suppose first that $i = \frac{1}{2}(s-1)$. Since s divides $\Phi_{\frac{1}{2}(s-1)}(q)$ and does not divide any of the other cyclotomic polynomials in the factorization of $q^{s-1} - 1$, we may assume that t is contained in a subgroup $H_+ \cong \Omega^+_{s-1}(q)$ of G. In fact, by the same argument, we may assume that t is contained inside a cyclic subgroup C_+ of order $\frac{q^{\frac{1}{2}(s-1)}-1}{(2,q-1)}$ of H_+. Since $C_+ \leq C_G(t)$, we have $|C_+| \leq (2, q-1) \cdot s$.

If instead $i = s-1$, then in analogue with the above, we may assume that t is contained in a subgroup $H_- \cong \Omega^-_{s-1}(q)$ of G. In fact, we may assume that t is contained inside a Singer cyclic subgroup C_- of order $\frac{q^{\frac{1}{2}(s-1)}+1}{(2,q-1)}$ of H_-. Since $C_- \leq C_G(t)$, we have $|C_-| \leq (2, q-1) \cdot s$.

We now check whether this situation can occur.

Claim 5.66. *(i) If n odd, $n \geq 9$ and $q \geq 3$, then $q^{\frac{1}{2}(n-1)} - 1 > 4n$,*

(ii) If $q > 3$, then $q^3 - 1 > 28$,

(iii) If n odd, $n \geq 9$ and $q \geq 2$, then $q^{\frac{1}{2}(n-1)} - 1 > n$,

(iv) If $q > 2$, then $q^3 - 1 > 7$.

Proof. (i) We work by induction on n. Certainly $q^4 - 1 > 36$ for $q \geq 3$ which proves the result for $n = 9$. Now assume the result is true for $n = k$. Then $q^{\frac{1}{2}(k+1)} - 1 = q(q^{\frac{1}{2}(k-1)} - 1) + q - 1 > 4kq + q - 1$ by the inductive hypothesis. Further $4kq + q - 1 > 4(k+2)$ which proves the result for $n = k + 2$.

(ii) This is trivial.

(iii) This is analogous to (i).

(iv) This is trivial. □

Suppose that q is even. If $q > 2$, then since $s \geq 7$ and $q^{\frac{1}{2}(s-1)} - 1 \leq |C_\pm| \leq s$, we have a contradiction with Claim 5.66 (iii), (iv). So $q = 2$. If $s > 7$, we again have a contradiction with Claim 5.66 (iii). So $s = 7$ and $G = D_4^\pm(2)$.

The orders of these groups are $|D_4^+(2)| = 2^{12} \cdot 3^5 \cdot 5^2 \cdot 7$ and $|D_4^-(2)| = 2^{12} \cdot 3^4 \cdot 5 \cdot 7 \cdot 17$ respectively. Since $p \neq 2$ and $p \neq 7$, we have $p \in \{3, 5, 17\}$. If $p = 17$, then $X \cong C_{17}$. This is a contradiction since a group of order 17 does not admit a nontrivial automorphism of order 7. Similarly if $p = 5$, then $X \cong C_5$, or $X \cong C_5 \times C_5$, or $X \cong C_{25}$. This is again a contradiction since no such group admits a nontrivial order 7 automorphism. Hence $p = 3$. By Lemma 5.6, X has an elementary abelian critical subgroup Y on which t acts nontrivially. Since 3 divides $q + 1$, we may apply Theorem 5.11 (a) to obtain $m_3(G) = 3$. This is a contradiction since no elementary abelian 3-group of rank 3 or smaller can admit a nontrivial automorphism of order 7.

Therefore q is odd. If $q > 3$, then since $s \geq 7$ and $\frac{1}{2}(q^{\frac{1}{2}(s-1)} - 1) \leq |C_\pm| \leq 2s$, we have a contradiction with Claim 5.66 (i), (ii). So $q = 3$. If $s > 7$, we again have a contradiction with Claim 5.66 (i). So $s = 7$ and $G = D_4^\pm(3) = \Omega_8^\pm(3)$.

If $G \cong \Omega_8^-(3)$, then Table 2.2 [GLS3] gives that, in fact $Z(G) = 1$. Hence $|C_-| \leq 7$, which contradicts Claim 5.66 (iv). If $G = \Omega_8^+(3)$, then the centralizer of an order 7 element in G has order 56. This is a contradiction since we showed earlier that $|C_G(t)| \leq 14$.

So we may assume that X is nonabelian. By Lemma 5.6, X has a critical subgroup Y. Set $R = [Y, t]$. By Remark 5.7 and the discussion above, (G, t, R) is a triple of type (Hs) and we may assume that R is nonabelian. Suppose that $Z(R)$ contains an element z of order p which is not contained in $Z(G)$. Then $R\langle t\rangle \in C_G(z)$. Therefore we are in the conditions of Lemma 5.5. So we obtain $R \leq L = L_1 \times L_2 \times ... \times L_j$, where, for each i, $L_i \cong A_{m_i}^\pm(q^{a_i})$

or $L_i \cong B_{m_i}(q^{a_i})$, or $L_i \cong D^{\pm}_{m_i}(q^{a_i})$, and each (L_i, t, R_i) is a triple of type (Hs). Further, by Theorem 5.3 (d)-(f) and Lemma 5.57, if $L_i \cong B_{m_i}(q^{a_i})$, then the natural module for L_i has dimension $2m_i + 1 < s + 1$ and if $L_i \cong D^{\pm}_{m_i}(q^{a_i})$, then the natural module for L_i has dimension $2m_i < s + 1$. So by Proposition 5.47 and Lemmas 5.61 and 5.63, each $R_i = 1$. Hence $R = 1$, which is a contradiction.

Therefore, we may assume that $p = 2$ and that $Z(R)$ contains a single involution z, namely the unique involution in $Z(G)$. By Lemma 5.8, we may assume that R is extra-special. Choose l such that $s = 2^l + c$, where $0 < c < 2^l$. There are 2 cases.

Case 1: $c < 2^l - 1$.

Since R is represented faithfully in $s + 1 < 2^{l+1}$ dimensions, we may apply Lemma 5.9 to obtain $c = 1$, $s = 2^l + 1$, $G \cong \Omega^{\pm}_{2^l+2}(q)$ and $R \cong 2^{1+2l}_{-}$. By Lemma 5.10, $C_G(t)/C_{C_G(t)}(R) \cong C_s$.

Suppose that $C_G(t)$ contains an involution z which is not contained in $Z(G)$. Since $C_G(t)/C_{C_G(t)}(R) \cong C_s$, we have $R\langle t\rangle \leq C_G(z)$. Then by Lemma 5.5, we obtain $R \leq L = L_1 \times L_2 \times ... \times L_j$, where for each i, $L_i \cong A^{\pm}_{m_i}(q^{a_i})$ or $L_i \cong B_{m_i}(q^{a_i})$, or $L_i \cong D^{\pm}_{m_i}(q^{a_i})$, and each (L_i, t, R_i) is a triple of type (Hs). Further, by Theorem 5.3 (d)-(f) and Lemma 5.57, if $L_i \cong B_{m_i}(q^{a_i})$, then the natural module for L_i has dimension $2m_i + 1 < s + 1$ and if $L_i \cong D^{\pm}_{m_i}(q^{a_i})$, then the natural module for L_i has dimension $2m_i < s+1$. So by Proposition 5.47 and Lemmas 5.61 and 5.63, each $R_i = 1$. Hence $R = 1$, which is a contradiction. So $C_G(t)$ contains a unique involution, namely the unique involution $\alpha \in Z(G)$.

Furthermore, exactly the same argument shows that $C_G(t)$ cannot contain any element having odd order coprime to s and r, and cannot contain any order s-element except for the powers of t. So in particular $m_s(C_G(t)) = 1$. Similarly, if $C_G(t)$ contains an element y which is not contained in $Z(G)$ but such that $y^2 \in Z(G)$, then we may apply the above argument to the images $\bar{R}$ of R and $\bar{t}$ of t in the quotient group $\bar{G} = G/Z(G)$ to show that $\bar{R} = 1$. So $C_G(t)$ contains no such element. Finally, if $C_G(t)$ contains an element u such that $u^s = t$, then $u \in C_{C_G(t)}(R)$ and so $[R, u] = 1$. Then $[R, t] = 1$ which is also a contradiction. We conclude that $|C_G(t)| = 2^a \cdot s \cdot r^b$ for $a \leq 1$ and some $b \geq 0$.

Since s divides $q^{s-1} - 1 = (q^{2^l} - 1) = (q - 1) \cdot (q + 1) \cdot (q^2 + 1) \cdot ... \cdot (q^{2^{l-1}} + 1)$ and $m_s(C_G(t)) = 1$, s must divide $q^{2^{l-1}} + 1 = q^{\frac{1}{2}(s-1)} + 1$. Then since q is odd, we have that $C_G(t)$ has a cyclic subgroup of order $\frac{1}{2}(q^{\frac{1}{2}(s-1)} + 1)$. By the calculation of $|C_G(t)|$ above, we have $\frac{1}{2}(q^{\frac{1}{2}(s-1)} + 1) \leq 2s$. However, since s is a Fermat prime we may assume that $s \geq 17$ and so we have a contradiction with Claim 5.62.

Case 2: $c = 2^l - 1$.

In this case $s = 2^{l+1} - 1$ and $G \cong \Omega^{\pm}_{2^{l+1}}(q)$. Arguing as in case 1 we see that in this case we may only have $R \cong 2^{1+2(l+1)}_{+}$. Again $C_G(t)$ may contain only s-elements and elements of $Z(G)$ and again $m_s(C_G(t)) = 1$, so that $|C_G(t)| = 2^a \cdot s \cdot r^b$ for $a \leq 1$ and some $b \geq 0$. We have that s divides $q^{s-1}-1 = q^{2^{l+1}-2}-1 = (q^{2^l-1}-1)\cdot(q^{2^l-1}+1)$. Then by the the same argument as in our previous results, we may only have $m_s(C_G(t)) = 1$ if s divides $\Phi_{s-1}(q)$ or s divides $\Phi_{\frac{s-1}{2}}(q)$. Thus $C_G(t)$ either contains a cyclic subgroup of order $q^{\frac{s-1}{2}}-1$ or a cyclic subgroup of order $q^{\frac{s-1}{2}}-1$. We have seen before that this is a contradiction unless $s = 7$ and $q = 3$. This gives $G \cong D_4^{\pm}(3)$ and we have also seen before that $C_G(t)$ is too large in all of these cases. This is a contradiction and so $X = 1$.

□

We now discuss orthogonal groups of dimension larger than $s+1$. Since in previous sections we found examples of triples (G, t, X) of type (Hs) in the case $(s, q) = (5, 3)$, we now separate the cases $(s, q) = (5, 3)$ and $(s, q) \neq (5, 3)$.

Lemma 5.67. *Suppose that either $G = B_{\frac{1}{2}(s+1)}(q)$ or $G = D^{\pm}_{\frac{1}{2}(s+3)}(q)$, where $(s, q) \neq (5, 3)$. Let X be a p-subgroup of G and let $t \in Inndiag(G)$ be such that (G, t, X) is a triple of type (Hs). Then $X = 1$.*

Proof. The arguments for groups of type $G = B_{\frac{1}{2}(s+1)}(q)$ and $G = D^{\pm}_{\frac{1}{2}(s+3)}(q)$ are analogous and so we treat them in parallel.

By Lemma 2.13, there exists an order s automorphism $\bar{t}$ of the algebraic group $\overline{G} \cong B_{\frac{1}{2}(s+1)}$ (resp. $\overline{G} \cong D_{\frac{1}{2}(s+3)}$) over $\overline{\mathbb{F}}_r$ which induces t on G. The Dynkin diagram of $\overline{G}$ has $\frac{1}{2}(s+1)$ (resp. $\frac{1}{2}(s+3)$) nodes. By Theorem 5.3, $L = O^{r'}(C_G(t))$ is a central product $L_1 \circ L_2 \circ \ldots \circ L_j$ of groups L_i such that the Dynkin diagram of $C_{\overline{G}}(\bar{t})$ is the disjoint union of diagrams Δ_i for $i = 1, 2, \ldots, j$ where each Δ_i is in turn a disjoint union of a_i copies of the Dynkin diagram of L_i. By Proposition 5.24 (iii), (iv), the Dynkin diagram for $C_{\overline{G}}(\bar{t})$ has at least 1 node, and hence $L \neq 1$. In particular $m_r(L) \geq 1$.

If $m_r(O^{r'}(C_G(t))) \geq 2$, then X is a nonabelian 2-group by Corollary 5.22. As discussed in Remark 5.23 we may assume that $G = G_a$. Then by Lemmas 5.4 and 5.5, we have $X \leq L_1 \circ L_2 \circ \ldots \circ L_j$, where for each i, $L_i \cong A^{\pm}_{m_i}(q^{a_i})$ or $L_i \cong B_{m_i}(q^{a_i})$, or $L_i \cong D^{\pm}_{m_i}(q^{a_i})$, and each (L_i, t, X_i) is a triple of type (Hs). Further, by Theorem 5.3 (d)-(f) and Lemma 5.57, if $L_i \cong B_{m_i}(q^{a_i})$, then the natural module for L_i has dimension $2m_i + 1 < s + 2$ and if $L_i \cong D^{\pm}_{m_i}(q^{a_i})$, then the natural module for L_i has dimension $2m_i < s + 2$. So we may apply Proposition 5.47 and Lemmas 5.61-5.65 to obtain $X_i = 1$ for each i and hence $X = 1$.

So we may assume that $m_r(O^{r'}(C_G(t))) = 1$, and by Table 3.3.1 [GLS3] we obtain $q = r$ and $O^{r'}(C_G(t)) = A_1(r)$. In particular, $G = B_{\frac{s+1}{2}}(r)$ or $G = D^{\pm}_{\frac{1}{2}(s+3)}(r)$ respectively. As discussed in Remark 5.60, we may assume that $G = \Omega_{s+2}(r)$ or $G = \Omega^{\pm}_{s+3}(r)$ respectively. We are now in the conditions of Claim 5.42, so we may assume that X is nonabelian.

If $G = \Omega_{s+2}(r)$, then in fact $G = G_a$. Since X is nonabelian, we may apply Lemmas 5.4 and 5.5 to obtain $X \leq L_1 \circ L_2 \circ ... \circ L_j$, where for each i, $L_i \cong A^{\pm}_{m_i}(q^{a_i})$ or $L_i \cong B_{m_i}(q^{a_i})$, or $L_i \cong D^{\pm}_{m_i}(q^{a_i})$, and each (L_i, t, X_i) is a triple of type (Hs). Then by applying Proposition 5.47 and Lemmas 5.61-5.65 we obtain $X = 1$.

So we may assume that $G = \Omega^{\pm}_{s+3}(r)$. Suppose that p is odd. Then since $|Z(G)|$ is a 2-group, $Z(X)$ contains a p-element z not contained in $Z(G)$. By Lemma 5.4, we have $X\langle t\rangle \leq C_G(z)$ and we may apply Lemmas 5.5, and 5.61-5.65 and Proposition 5.47 to conclude that $X = 1$.

Therefore we may assume that $p = 2$. By Lemma 5.6, X contains a critical subgroup Y. Let $R = [Y, t]$. As discussed in Remark 5.7, (G, t, R) is a triple of type (Hs). By Claim 5.42, R is nonabelian. If $Z(R)$ contains an involution not contained in $Z(G)$, then $R\langle t\rangle \leq C_G(z)$ and we may apply Lemmas 5.5 and 5.61-5.65 and Proposition 5.47 to obtain $Y = 1$. So we may assume that $Z(R)$ contains a unique involution and by Lemma 5.8, R is extra-special.

Choose l such that $s = 2^l + c$, where $0 < c < 2^l$. Suppose first that $c + 3 < 2^l$. Then G has a faithful representation in $n = s + 3 < 2^{l+1}$ dimensions. Since R admits an order s automorphism and has a faithful representation in dimension smaller than 2^{l+1}, Lemma 5.9 gives $c = 1$ and $R \cong 2^{1+2l}_{-}$. Hence $s = 2^l + 1$. So by Lemma 5.10, we have $C_G(t)/C_{C_G(t)}(R) \cong C_s$. However, we have $O^{r'}(C_G(t)) \cong A_1(r)$. Since $A_1(r)$ does not contain a central element of order s, the whole of $O^{r'}(C_G(t))$ centralizes R. Hence $R\langle t\rangle \leq C_G(z)$ for some involution z (passing to the quotient group $\bar{G} = G/Z(G)$ to avoid the case $z \in Z(G)$ if necessary). Then we apply Lemmas 5.5, and 5.61-5.65 and Proposition 5.47 to obtain $R = 1$, which is a contradiction.

So we may assume that $2^l \leq c + 3 < 2^l + 3$. Since s is odd, we have either $s = 2^{l+1} - 3$ or $s = 2^{l+1} - 1$. Since either $R \cong 2^{1+2k}_{+}$ or $R \cong 2^{1+2k}_{-}$, and R admits an automorphism of order $s = 2^{l+1} - 1$, we obtain $R \cong 2^{1+2(l+1)}_{+}$, $Aut(R) \cong O^{+}_{2l+2}(2)$ and hence $C_G(t)/C_{C_G(t)}(R) \cong C_s$. Then may again apply Lemmas 5.5, and 5.61-5.65 and Proposition 5.47 to obtain $R = 1$, which is a contradiction.

□

Lemma 5.68. *Let s be a prime and let $n \geq s + 2$. Suppose $(s, q) \neq (5, 3)$ and that either*

(1) $G = B_m(q)$, where $n = 2m + 1$ or

(2) $G = D^{\pm}_m(q)$, where $n = 2m$.

Let X be a p-subgroup of G and let $t \in Inndiag(G)$ be such that (G, t, X) is a triple of type (Hs). Then $X = 1$.

Proof. We will work by induction on the dimension n of the natural module for G. We take

Lemma 5.67 as the basis case of our induction. So we will assume that $n \geq s+4$ and that if (G, t, X) is a triple of type (Hs) with $G = B_{m'}(q')$ where $q' \neq 3$ and $n' = 2m'+1 < n$, or $G = D^{\pm}_{m'}(q')$, where $q' \neq 3$ and $n' = 2m' < n$, then $X = 1$.

By Corollary 5.32, there exists $Z \leq C_G(t)$ such that $Z \cong C_r \times C_r$. Hence X is a nonabelian 2-group by Corollary 5.22. As we observed in Remark 5.23, we may assume that $G = G_a$. By Lemmas 5.4 and 5.5, we have $X\langle t\rangle \leq C_G(z)$ for some involution $z \in Z(X)$ and so $X \leq L = L_1 \circ L_2 \circ ... \circ L_j$, where for each i, $L_i \cong A^{\pm}_{m_i}(q^{a_i})$, or $L_i \cong B_{m_i}(q^{a_i})$, or $L_i \cong D^{\pm}_{m_i}(q^{a_i})$ and each (L_i, t, X_i) is a triple of type (Hs). Further, by Theorem 5.3 (d)-(f) and Lemma 5.57, if $L_i \cong B_{m_i}(q^{a_i})$, then the natural module for L_i has dimension $2m_i+1 < n$ and if $L_i \cong D^{\pm}_{m_i}(q^{a_i})$, then the natural module for L_i has dimension $2m_i < n$. So we may apply Proposition 5.47, Lemmas 5.61 - 5.67 and the inductive hypothesis to obtain $X_i = 1$ for each i and hence $X = 1$. □

We now address the case $(s, q) = (5, 3)$.

Lemma 5.69. *Let $G = B_3(3)$ or $G = D^{\pm}_4(3)$. Let X be a p-subgroup of G and let $t \in Inndiag(G)$ be such that (G, t, X) is a triple of type $(H5)$. Then $X = 1$.*

Proof. We will first show that X is a nonabelian 2-group. By Proposition 5.24 (iii), (iv), we have $m_3(O^{3'}(C_G(t))) \geq 1$. If $m_3(O^{3'}(C_G(t)) \geq 2$, then X is a nonabelian 2-group by Corollary 5.22. If $m_3(O^{3'}(C_G(t))) = 1$, then we are in the conditions of Claim 5.42, so again X is a nonabelian 2-group.

As discussed in Lemma 5.2 and Remarks 5.23 and 5.60, we may assume that $G = \Omega_7(3)$ or $G = P\Omega^{\pm}_8(3)$ respectively. By Lemmas 5.4 and 5.5, we have, for some involution $z \in Z(X)$, $X \leq L = O^{3'}(C_G(z)) = L_1 \circ L_2 \circ ... \circ L_j$ where each $L_i \in Lie(r)$ and each projection (L_i, t, X_i) is a triple of type (Hs). Further, by Table 4.5.1 [GLS3], L is isomorphic to one of the following list: $C_2(3)$, $A_1(3) \circ A_1(3) \circ A_1(3)$, $A_1(9) \circ A_1(3)$, $A^{\pm}_3(3)$, $A_1(3) \circ A_1(3) \circ A_1(9)$, $A_1(3) \circ A_1(3) \circ A_1(3) \circ A_1(3)$, $A_1(9) \circ A_1(9)$ or $A_1(81)$. By Lemmas 5.35, 5.37 and 5.50 we have either $X = 1$ or $X \cong 2^{1+4}_{-}$ with $L \cong C_2(3)$ or $L \cong A^{-}_3(3)$.

If $X \cong 2^{1+4}_{-}$, then $Z(X)$ contains a unique involution z. Hence we must have $N_G(X) \leq C_G(z)$. Therefore we have $C_G(t) \leq C_G(z)$ and so $O^{3'}(C_G(t)) \leq O^{3'}(C_G(z)) = L$. By Lemmas 5.37 and 5.50, the centralizer of a 5-element in $C_2(3)$ or $A^{-}_3(3)$ is isomorphic to $C_2 \times C_5$ or $C_4 \times C_5$ respectively. In particular $m_3(O^{3'}(C_G(t))) = 0$, which is a contradiction. □

Lemma 5.70. *Suppose that $n \geq 7$. Suppose that either*

(1) $G = B_m(3)$, where $n = 2m+1$ or

(2) $G = D^{\pm}_m(3)$, where $n = 2m$.

Let X be a p-subgroup of G and let $t \in Inndiag(G)$ be such that (G,t,X) is a triple of type $(H5)$. Then $X = 1$.

Proof. As discussed in Remark 5.60, we may assume that $G = \Omega_n(3)$ if n is odd and that $G = \Omega_n^{\pm}(3)$ if n is even. We will work by induction on the dimension n of the natural module for G. We take Lemma 5.69 as the basis case of our induction. So we will assume that $n \geq 9$ and that if (G,t,X) is a triple of type (Hs) with $G = \Omega_{n'}(3)$ or $G = \Omega_{n'}^{\pm}(3)$, where $n' < n$, then $X = 1$.

By Corollary 5.32, there exists $Z \leq C_G(t)$ such that $Z \cong C_r \times C_r$. Hence X is a nonabelian 2-group by Corollary 5.22. As we observed in Remark 5.23, we may now assume that $G = G_a$. By Lemmas 5.4 and 5.5, we have, for some involution $z \in Z(X)$, $X \leq L = O^{3'}(C_G(z)) = L_1 \circ L_2 \circ ... \circ L_j$ where each $L_i \in Lie(r)$ and each projection (L_i, t, X_i) is a triple of type (Hs). Further, by Table 4.5.1 [GLS3], we have either $j = 1$ so that $L = L_1$ or $j = 2$ so that $L = L_1 \circ L_2$, and we may list the possibilities for L as follows.

- If $G = B_m(3)$, then L is isomorphic to one of the following list: $B_{m-1}(3)$, $D_i^{\pm}(3) \circ B_{m-i}(3)$ for $2 \leq i < m$, or $D_m^{\pm}(3)$.
- If $G = D_m^{\pm}(3)$, then L is isomorphic to one of the following list: $D_{m-1}^{\pm}(3)$, $D_i^{\pm}(3) \circ D_{m-i}^{\pm}(3)$ for $2 \leq i < \frac{m}{2}$, $D_{\frac{m}{2}}^{\pm}(3)^2$ (only if m is even), $D_{\frac{m}{2}}^{\pm}(9)$ (only if m is even), $A_{m-1}^{\pm}(3)$, $D_{\frac{m}{2}}(3) \circ D_{\frac{m}{2}}^{-}(3)$.

By Propositions 5.47 and 5.56, Lemmas 5.61 - 5.69 and the inductive hypothesis we have, for each i, $X_i = 1$ unless $L_i \cong A_3^-(3)$ or $L_i \cong C_2(3)$. In the case $L_i \cong A_3^-(3)$, closer inspection of Table 4.5.1 [GLS3] shows that in fact X can be embedded in some central quotient of $GU_4(3)$. Then Lemma 5.45 gives $X_i = 1$.

So we may assume that $X \leq X_i \leq L_i \cong C_2(3)$. Then closer inspection of Table 4.5.1 [GLS3] shows that $L_i \cong PSp_4(3)$. Since X is nonabelian, this is a contradiction with Lemma 5.50. $\square$

We now combine Lemmas 5.61 - 5.70 to obtain the main result of this section.

Proposition 5.71. *Suppose that either*

(1) $G = B_m(q) = \Omega_{2m+1}(q)$ with $m \geq 3$, or

(2) $G = D_m^{\pm}(q) = \Omega_{2m}^{\pm}(q)$ with $m \geq 4$.

Let X be a p-subgroup of G and let $t \in Inndiag(G)$ such that (G,t,X) is a triple of type (Hs). Then $X = 1$.

5.5 The Remaining Exceptional Groups of Lie Type

Since we have previously found triples of type $(H5)$ and we would like to have $X\langle t\rangle \leq L$, where L is a product of groups we have already looked at, we will take the $s = 5$ and $s > 5$ cases separately in this section.

5.5.1 The Case $s = 5$

Recall that $q = r^a$ and that p, r, and 5 are assumed to be pairwise coprime.

Lemma 5.72. *Let G be one of $F_4(q)$, $G_2(q)$ (where $q = r^a$), ${}^2F_4(q)$ (where $q = r^a = 2^{2m+1}$) or ${}^2G_2(q)$ (where $q = r^a = 3^{2m+1}$). Let X be a p-subgroup of G and let $t \in Inndiag(G)$ be such that (G, t, X) is a triple of type $(H5)$. Then $X = 1$.*

Proof. By Lemma 2.16, we may assume that t induces an inner automorphism on G. By Lemma 2.13, there exists an order s automorphism $\bar{t}$ of the algebraic group $\overline{G} \cong F_4$ or $\overline{G} \cong G_2$ over $\overline{\mathbb{F}}_r$ which induces t on G. The Dynkin diagram of $\overline{G}$ has 4 (resp. 2) nodes. Hence, by Proposition 5.24 (v), (vi), the Dynkin diagram for $C_{\overline{G}}(\bar{t})$ has at least 1 node. So we may assume that $m(O^{r'}(C_G(t))) \geq 1$.

If $m_r(O^{r'}(C_G(t))) \geq 2$, then X is a nonabelian 2-group by Corollary 5.22. Since $p \neq r$, we have $G \neq {}^2F_4(q)$. By Lemmas 5.4 and 5.5, we have $X\langle t\rangle \leq C_G(z)$ for some involution $z \in Z(X)$ and so $X \leq L = O^{r'}(C_G(z)) = L_1 \circ L_2 \circ ... \circ L_j$, where for each i, $L_i \in Lie(r)$ and each projection (L_i, t, X_i) is a triple of type $(H5)$. Further, by Table 4.5.1 [GLS3], we may list the possibilities for L as follows.

- If $G = G_2(q)$, then $L \cong A_1(q) \circ A_1(q)$;
- If $G = {}^2G_2(q)$, then $L \cong A_1(q^2)$;
- If $G = F_4(q)$, then either $L \cong A_1(q) \circ C_3(q)$ or $L \cong B_4(q)$.

By Lemmas 5.35 and 5.69 and Proposition 5.56, we have $X = 1$ unless $G = F_4(3)$ and $L = L_1 \circ L_2$, where $L_1 \cong A_1(3)$ and $L_2 \cong C_3(3)$. In this case $X_1 = 1$ by Lemma 5.35 and either $X_2 = 1$ or $X_2 \cong 2^{1+4}_-$ by Proposition 5.56. If $X_2 \cong 2^{1+4}_-$, then since $X \leq X_1 \circ X_2$, $Z(X)$ contains a unique involution. Hence $N_G(X) \leq C_G(z)$ and so $C_G(t) \leq C_G(z)$. Then closer inspection of Table 4.5.1 [GLS3] shows that 5 divides $C_G(z)$ only once. Since, by Table 2.2 [GLS3], we have $|G| = 2^{15} \cdot 3^{24} \cdot 5^2 \cdot 7^2 \cdot 13^2 \cdot 41 \cdot 73$, we see that 5 must divide $C_G(t)$ twice, which is a contradiction.

Hence $m_r(O^{r'}(C_G(t))) = 1$. By Table 3.3.1 [GLS3] we may assume that $q = r$ and that $L \cong A_1(r)$. By Table 5.4.C [KL], $F_4(r)$ and ${}^2F_4(r)$ have faithful 26-dimensional representations and $G_2(r)$ and ${}^2G_2(r)$ have faithful 7-dimensional representations. Suppose that X is abelian. Then we may apply Lemma 5.42 to obtain either

(a) $G = G_2(r)$ or $G = {}^2G_2(r)$ and $7 \geq 5r$, or

(b) $G = F_4(r)$ or $G = {}^2F_4(r)$ and $26 \geq 5r$.

Since $r \geq 2$, case (a) gives an immediate contradiction. Hence we are in case (b). Since $26 \geq 5r$ and $r \neq 5$, we have $r = 2$ or $r = 3$ and so $G = F_4(2)$, $G = F_4(3)$ or $G = {}^2F_4(2)$.

If $G \cong F_4(2)$, then by Table 2.2 [GLS3] we have $|G| = 2^{24} \cdot 3^6 \cdot 5^2 \cdot 7^2 \cdot 13 \cdot 17$. If $p \in \{13, 17\}$, then either $X = 1$ or X is cyclic of order p. Since 5 does not divide $p - 1 = |Aut(C_p)|$, X does not admit a nontrivial automorphism of order 5. So $X = [X, t] = 1$. So we may assume that $p \in \{3, 7\}$. Since X is abelian, if $X \neq 1$ we may apply Lemma 5.6 to see that there exists an elementary abelian subgroup $1 \neq Y \leq X$ such that t acts nontrivially on Y and $C_G(t) \leq N_G(Y)$. Since no elementary abelian group of order 7 or 7^2 can admit a nontrivial order 5 automorphism, we may assume that $p = 3$. Since $3 = 2+1 = \Phi_2(r)$ and $\Phi_2(r)$ appears with exponent 4 in the factorization of $|G|$, we may apply Theorem 5.11 to obtain $m_3(G) = 4$. So $Y \cong E_{3^n}$ for $n \leq 4$ and so $Aut(Y) \cong GL_n(3)$. If $n \leq 3$, then 5 does not divide $|Aut(Y)|$. Hence $n = 4$ and so $Aut(Y) \cong GL_4(3)$. In particular, 5 divides $|Aut(Y)|$ exactly once. Since $5 = 2^2 + 1 = \Phi_4(r)$ and $\Phi_4(r)$ appears with exponent 2 in the factorization of $|G|$, we may apply Theorem 5.11 and Corollary 5.12 to obtain $m_5(C_G(t)) = 2$. Since 5 divides $|Aut(Y)|$ only once, there is an order 5 element $z \in C_G(t)$ which centralizes Y. Then we have $Y\langle t\rangle \leq C_G(z)$. Applying Lemma 5.5, we have $Y \leq L = L_1 \circ L_2 \circ ... \circ L_j$, where, for each i, $L_i \cong A^{\pm}_{m_i}(q^{a_i})$ or $L_i \cong C_{m_i}(q^{a_i})$, and each (L_i, t, Y_i) is a triple of type $(H5)$. Since $p = 3$, we may apply Propositions 5.47 and 5.56 to obtain $Y = 1$, which is a contradiction.

If $G \cong F_4(3)$, then by Table 2.2 [GLS3] we have $|G| = 2^{15} \cdot 3^{24} \cdot 5^2 \cdot 7^2 \cdot 13^2 \cdot 41 \cdot 73$. If $p \in \{41, 73\}$, then either $X = 1$ or X is cyclic of order p. If $p = 73$, then since 5 does not divide $p-1$, X does not admit a nontrivial automorphism of order 5. So $X = [X, t] = 1$. If $p = 41$, then 5 divides $p-1$ exactly once. Since 5 divides $3^2+1 = \Phi_4(r)$ and $\Phi_4(r)$ appears with exponent 2 in the factorization of G, we apply Theorem 5.11 and Corollary 5.12 to obtain $m_5(C_G(t)) = 2$. So there is an order 5 element $z \in C_G(t)$ which centralizes X. Then $X\langle t\rangle \leq C_G(z)$. Applying Lemma 5.5, we have $X \leq L = L_1 \circ L_2 \circ ... \circ L_j$, where, for each i, $L_i \cong A^{\pm}_{m_i}(q^{a_i})$ or $L_i \cong C_{m_i}(q^{a_i})$, and each (L_i, t, X_i) is a triple of type (Hs). Since $p = 41$, we may apply Propositions 5.47 and 5.56 to obtain $X = 1$. Thus we may assume that $p \in \{2, 7, 13\}$. We may apply Lemma 5.6 as before to find an elementary abelian subgroup $1 \neq Y \leq X$ on such that $C_G(t) \leq N_G(Y)$ and t acts nontrivially on Y. Since no elementary abelian group of order 7, 7^2, 13 or 13^2 can admit a nontrivial order 5 automorphism, we may assume that $p = 2$. By Corollary [CS], $m_2(G) = 5$. So $Y \cong E_{2^n}$ for $n \leq 5$ and $Aut(Y) \cong GL_n(2)$. Since $|Aut(Y)|$ is divisible by 5 at most once, we may find $z \in C_G(t)$ of order 5 such that $Y\langle t\rangle \leq C_G(z)$ and, by applying Lemma 5.5 as before, we obtain $Y = 1$, which is a contradiction.

If $G \cong {}^2F_4(2)$, then by Table 2.2 [GLS3] we have $|G| = 2^{12} \cdot 3^3 \cdot 5^2 \cdot 13$. Since $p \neq r$ and

$p \neq s$, we have $p \in \{3, 13\}$. By Lemma 5.6, there exists an elementary abelian subgroup $1 \neq Y \leq X$ on which t acts nontrivially. Since no elementary abelian group of order 3, 3^2, 3^3 or 13 can admit a nontrivial order 5 automorphism we have $Y = 1$, which is a contradiction.

Therefore X is nonabelian. By Lemmas 5.4 and 5.5, we have $X\langle t\rangle \leq C_G(z)$ for some $z \in Z(X)$ of order p and so $X \leq L = O^{r'}(C_G(z)) = L_1 \circ L_2 \circ ... \circ L_j$, where for each i, $L_i \cong A^{\pm}_{m_i}(q^{a_i})$ or $L_i \cong C_{m_i}(q^{a_i})$ and each projection (L_i, t, X_i) is a triple of type $(H5)$. By Lemmas 5.35 and 5.69 and Proposition 5.56, we have $X = 1$ unless $G = F_4(3)$, $p = 2$ and $L = L_1 \circ L_2$, where $L_1 \cong A_1(3)$ and $L_2 \cong C_3(3)$. In this case $X_1 = 1$ by Lemma 5.35 and either $X_2 = 1$ or $X_2 \cong 2^{1+4}_{-}$ by Proposition 5.56. If $X_2 \cong 2^{1+4}_{-}$, then since $X \leq X_1 \circ X_2$, $Z(X)$ contains a unique involution. Hence $N_G(X) \leq C_G(z)$ and so $C_G(t) \leq C_G(z)$. Then closer inspection of Table 4.5.1 [GLS3] shows that 5 divides $C_G(z)$ only once. Since, by Table 2.2 [GLS3], we have $|G| = 2^{15} \cdot 3^{24} \cdot 5^2 \cdot 7^2 \cdot 13^2 \cdot 41 \cdot 73$, we see that 5 must divide $C_G(t)$ twice, which is a contradiction.

□

Lemma 5.73. *Let G be one of the groups $E_6(q)$, ${}^2E_6(q)$, $E_7(q)$ or $E_8(q)$. Let t be an inner-diagonal automorphism of G and suppose that (G, t, X) is a triple of type $(H5)$. Then $X = 1$.*

Proof. By Corollary 5.33, $C_G(t)$ has a subgroup $Z \cong C_r \times C_r$. So by Corollary 5.22, X is a nonabelian 2-group. Then as discussed in Remark 5.23, we may assume that $G = G_a$.

Suppose first that $G = E_6(q)$ or $G = {}^2E_6(q)$. Then by Lemmas 5.4 and 5.5 we have $X\langle t\rangle \leq C_G(z)$ for some involution $z \in Z(X)$, and so $X \leq L = L_1 \circ L_2 \circ ... \circ L_j$ where, for each i, $L_i \in Lie(r)$ and each (L_i, t, X_i) is a triple of type $(H5)$. Further, by Table 4.5.1 [GLS3], we have $L \cong D^{\pm}_5(q)$ or $L = A_1(q) \circ A^{\pm}_5(q)$. Now we may apply Proposition 5.47 and Lemma 5.71 to obtain $X_i = 1$ for each i and so $X = 1$.

The proof for $G = E_7(q)$ is exactly analogous; by Lemmas 5.4 and 5.5 and Table 4.5.1 [GLS3] we obtain $X \leq L$, where L is one of $A_1(q) \circ D_6(q)$, $A^{\pm}_7(q)$, $E_6(q)$ or $E_6(q)$. So by Proposition 5.47 and Lemma 5.71 and the result for $E_6(q)$ and ${}^2E_6(q)$ we get $X = 1$.

The $E_8(q)$ case follows from the $E_7(q)$ case since, by Lemmas 5.4 and 5.5 and Table 4.5.1 [GLS3] we obtain $X \leq L$, where L is one of $D_8(q)$ or $A_1(q) \circ E_7(q)$. □

5.5.2 The Case $s > 5$

Throughout this subsection we assume that $s > 5$. Recall that $q = r^a$ and that p, r, s are assumed to be pairwise coprime. We begin with some general observations about the groups in question in this section.

Lemma 5.74. *Let $q = r^a$ and let G be one of $G_2(q)$, ${}^2G_2(q)$, $F_4(q)$, ${}^2F_4(q)$, $E_6(q)$, ${}^2E_6(q)$, $E_7(q)$ or $E_8(q)$. Let $\Phi_i(q)$ be a cyclotomic polynomial appearing with multiplicity 1 in the factorization of $|G|$ into irreducible polynomials in q. Then G has a cyclic subgroup of order $\Phi_i(q)$.*

Proof. This follows directly from looking at the lists of the cyclic structure of maximal tori of each of these groups, for example in Sections 2.2, 2.3 and 2.5-2.10 [KS]. □

Lemma 5.75. *Let $q = r^a$ and let G be one of $G_2(q)$, ${}^2G_2(q)$, $F_4(q)$, ${}^2F_4(q)$, $E_6(q)$, ${}^2E_6(q)$, $E_7(q)$ or $E_8(q)$. Let n be the smallest dimension of a faithful module M of G in characteristic r. Let X be a p-subgroup of G and let $t \in Inndiag(G)$ be such that (G, t, X) is a triple of type (Hs). Suppose that s divides $\Phi_i(q)$, where $\Phi_i(q)$ appears with multiplicity 1 in the factorization of $|G|$ into irreducible polynomials in q. If X is abelian, then $\Phi_i(q) \leq n$.*

Proof. By Lemma 5.74, G has a cyclic subgroup C of order Φ_q. By Theorem 5.11 and Corollary 5.12, we may assume that $t \in C$. Since C is abelian, we have $C \leq C_G(t)$. Hence C acts on X. Write $C = \langle u \rangle$. Then $t = u^k$ for some k. If $x \in C_X(u)$, then $x \in C_X(t)$ and we may apply Theorem 5.1 (iii) to conclude that $x = 1$. Hence $C_X(u) = 1$ and so XC is a Frobenius group with kernel X and complement C. Since C has order $\Phi_i(q)$, the result now follows from Lemma 5.14. □

We now proceed to derive the main results of this section.

Lemma 5.76. *Let $G \cong G_2(q)$. Let X be a p-subgroup of G and let $t \in Inndiag(G)$ be such that (G, t, X) is a triple of type (Hs). Then either $X = 1$ or $s = 7$, $q = 3$, $X \cong E_{2^3}$ and $C_G(t) \cong C_7$. Furthermore, such a triple (G, t, X) does indeed exist.*

Proof. Suppose first that X is abelian. By Table 2.2 [GLS3], the order of G factorizes into a product of cyclotomic polynomials as

$$|G| = q^6 \cdot (q-1)^2 \cdot (q+1)^2 \cdot (q^2+q+1) \cdot (q^2-q+1)$$

Since s is prime, s divides one of the factors in this product. Suppose that s divides $q-1$ or divides $q+1$. Since $q-1$ and $q+1$ each appear with exponent 2 in the factorization of $|G|$, we may apply Theorem 5.11 and Corollary 5.12 to see that there is a subgroup $Z = \langle t, t_1 \rangle \cong C_s^2$ of $C_G(t)$. Since $C_G(t) \leq N_G(X)$, Z acts on X. So by Theorem 3.5, $X = \langle C_X(u) : u \in Z^\# \rangle$. Choose $u \in Z^\#$ such that $C_X(u)$ as large as possible. Note that u is not a power of t since $C_X(t) = 1$. Certainly $C_X(u)\langle t \rangle \leq C_G(u)$. Then we are in the conditions of Lemma 5.5. Hence $C_X(u) \leq L_1 \times L_2 \times ... \times L_j$ where, for each i, $L_i \cong A^{\pm}_{m_i}(q^{a_i})$ for $m_i \leq 2$ and each projection $(L_i, t, C_X(u)_i)$ is of type (Hs). Then we may apply Proposition 5.47 to see that $C_X(u)_i = 1$ for each i and so $C_X(u) = 1$. Now since we chose $C_X(u)$ as large as possible we must have $X = 1$.

So we may assume that either s divides q^2+q+1 or divides q^2-q+1. By Table 5.4.C [KL], the smallest dimension of a faithful representation of G in characteristic r is 6 if $r = 2$ and 7 otherwise. Suppose that s divides q^2+q+1. If $r = 2$ then we apply Lemma 5.75 to obtain $q^2+q+1 \leq 6$. This is a contradiction since $q \geq 2$. If $r \neq 2$ then Lemma 5.75 gives $q^2+q+1 \leq 7$. This is a contradiction since $q \geq 3$. Therefore s divides q^2-q+1. If $r = 2$, then Lemma 5.75 gives $q^2-q+1 \leq 6$ and so $q = 2$. So s divides $2^2-2+1 = 3$. This is a contradiction since $s > 5$. If $r \neq 2$, then Lemma 5.75 gives $q^2-q+1 \leq 7$ and so $q = 3$. So $G = G_2(3)$ and s divides $3^2-3+1 = 7$, which implies that $s = 7$.

By Table 2.2 [GLS3], $|G_2(3)| = 2^6 \cdot 3^6 \cdot 7 \cdot 13$. Since $p \neq r$ and $p \neq s$, we may only have $p \in \{2, 13\}$. If $p = 13$, then since 13 divides $|G|$ exactly once, either $X = 1$ or $X \cong C_{13}$. Since C_{13} does not admit a nontrivial automorphism of order 7, we have $X = 1$. So we may assume that $p = 2$. By Lemma 5.6, there exists an elementary abelian subgroup $1 \neq Y \leq X$ on which t acts nontrivially. By Corollary [CS], $m_2(G) = 3$ and so $Y \cong E_{2^n}$ for $n \leq 3$. Since Y admits a nontrivial automorphism of order 7, we must have $Y \cong E_{2^3}$. So a priori we may have a triple (G, t, Y) of type $(H7)$ such that $Y \cong E_{2^3}$. It remains to show that such triples do indeed exist. By [ATLAS], an order 7 element of G has centralizer isomorphic to C_7. Further, G has a subgroup H which is isomorphic to $PSL_2(8)$. Now H has a maximal parabolic subgroup P with unipotent radical $U \cong E_8$ and Levi complement $L \cong C_7$. Taking $Y = U$ and t a generator of L gives a triple (G, t, Y) of type $(H7)$.

We may now assume that X is nonabelian. Arguing as in the proof of Lemma 5.4, we may see that $X_0 = [Z(X), t]$ is an abelian $C_G(t)$-signalizer. By the analysis above, if $X_0 \neq 1$, then $G \cong G_2(3)$ and $X_0 \cong E_{2^3}$. In particular this means that $m_2(X) > 3$ and this contradicts the fact that $m_2(G_2(3)) = 3$. So we may assume that $X_0 = 1$. Hence $Z(X) \leq C_G(t)$ and so $X\langle t\rangle \leq C_G(z)$ for some $z \in Z(X)$ of order p. Applying Lemma 5.5 gives $X \leq L_1 \times L_2 \times ... \times L_j$ where, for each i, $L_i \cong A^{\pm}_{m_i}(q^{a_i})$ with $m_i \leq 2$ and each projection (L_i, t, X_i) is a triple of type (Hs). Then we may apply Proposition 5.47 to obtain $X_i = 1$ for each i and so $X = 1$. □

Lemma 5.77. *Let $G \cong {}^2G_2(q)$ with $q = 3^{1+2a}$. Let X be a p-subgroup of G and let $t \in Inndiag(G)$ be such that (G, t, X) is a triple of type (Hs). Then either $X = 1$ or $s = 7$, $q = 3$, $X \cong E_{2^3}$ and $C_G(t) \cong C_7$. Furthermore, such a triple (G, t, X) does indeed exist.*

Proof. Suppose first that X is abelian. By Table 2.2 [GLS3], the order of G factorizes into a product of cyclotomic polynomials as

$$|G| = q^3 \cdot (q-1) \cdot (q+1) \cdot (q^2-q+1)$$

Since s is prime, s divides one of the factors in this product. By Table 5.4.C [KL], the smallest dimension of a faithful representation of G in characteristic r is 7.

Suppose that either s divides $q-1$ or s divides $q+1$. Then we may apply Lemma 5.75 to obtain $q-1 \leq 7$ or $q+1 \leq 7$ respectively. Since q is a power of 3, we must have $q=3$. So $q-1=2$ and $q+1=4$. Since s divides $q-1$ or $q+1$ we have $s=2$. This is a contradiction since $s \geq 7$.

Hence s divides q^2-q+1. By Lemma 5.75, $q^2-q+1 \leq 7$. Hence $q=3$. So $G = {}^2G_2(3)$ and $s=7$. Further, by Table 2.2 [GLS3], we have $|G| = 2^3 \cdot 3^3 \cdot 7$. Since $p \neq s$ and $p \neq r$ we have $p=2$. Now G has a subgroup $H \cong PSL_2(8)$, which has a parabolic subgroup P with unipotent radical $U \cong E_8$ and Levi complement $L \cong C_7$. Then taking $X=U$ and t a generator of L gives a triple (G,t,X) of type $(H7)$.

We may now assume that X is nonabelian. Arguing as in the proof of Lemma 5.4, we may see that $X_0 = [Z(X),t]$ is an abelian $C_G(t)$-signalizer. By the analysis above, if $X_0 \neq 1$, then $G \cong {}^2G_2(3)$ and $X_0 \cong E_{2^3}$. Since 3 is the largest power of 2 that divides $|{}^2G_2(3)|$, we must have $X = X_0$ and this is a contradiction as X is supposed to be nonabelian. So we may assume that $X_0 = 1$. Hence $Z(X) \leq C_G(t)$ and so $X\langle t \rangle \leq C_G(z)$ for some $z \in Z(X)$ of order p. We now apply Lemma 5.5 to obtain $X \leq L_1 \times L_2 \times ... \times L_j$ where, for each i, $L_i \cong A^{\pm}_{m_i}(q^{a_i})$ with $m_i \leq 2$ and each projection (L_i,t,X_i) is a triple of type (Hs). Then we may apply Proposition 5.47 to obtain $X_i = 1$ for each i and so $X=1$. $\square$

Lemma 5.78. *Let $G \cong F_4(q)$. Let X be a p-subgroup of G and let $t \in Inndiag(G)$ be such that (G,t,X) is a triple of type (Hs). Then either $X=1$ or $s=13$, $q=2$ and $X \cong E_{3^3}$. Furthermore, such a triple (G,t,X) does indeed exist.*

Proof. First suppose that X is abelian. The order of G factorizes into a product of cyclotomic polynomials as

$$|G| = (q-1)^4 \cdot (q+1)^4 \cdot (q^2+q+1)^2 \cdot (q^2+1)^2 \cdot (q^2-q+1)^2 \cdot (q^4+1) \cdot (q^4-q^2+1)$$

If s divides one of $q-1$, $q+1$, q^2+q+1, q^2+1 or q^2-q+1, then since each of these polynomials appears with exponent greater than 1 in the factorization of $|G|$, we may apply Theorem 5.11 and Corollary 5.12 to see that there is a subgroup $Z = \langle t, t_1 \rangle \cong C_s^2$ of $C_G(t)$. Since $C_G(t) \leq N_G(X)$, Z acts on X. So by Theorem 3.5, $X = \langle C_X(u) : u \in Z^{\#} \rangle$. Choose $u \in Z^{\#}$ such that $C_X(u)$ as large as possible. Note that u is not a power of t since $C_X(t) = 1$. Certainly $C_X(u)\langle t \rangle \leq C_G(u)$. Then we are in the conditions of Lemma 5.5. Hence $C_X(u) \leq L_1 \times L_2 \times ... \times L_j$ where, for each i, $L_i \cong A^{\pm}_{m_i}(q^{a_i})$, or $L_i \cong B_{m_i}(q^{a_i})$, or $L_i \cong C_{m_i}(q^{a_i})$ and each projection $(L_i, t, C_X(u)_i)$ is of type (Hs). Then we may apply Propositions 5.47, 5.56 and 5.71 to see that $C_X(u)_i = 1$ for each i and so $C_X(u) = 1$. Now since we chose $C_X(u)$ as large as possible we must have $X=1$.

Thus we may assume that either s divides $q^4 + 1 = \Phi_8(q)$ or that s divides $q^4 - q^2 + 1 = \Phi_{12}(q)$. By Table 5.4.C, the smallest dimension of a faithful representation of G in characteristic r is 25 if $r = 3$ and 26 otherwise. If s divides q^4+1, then Lemma 5.75 gives $q^4+1 \leq 26$ and so $q = 2$ and $s = 17$. If s divides q^4-q^2+1, then Lemma 5.75 gives $s = 2$ and $q = 13$. In either case, $G = F_4(2)$.

By Table 2.2 [GLS3], $|G| = 2^{24} \cdot 3^6 \cdot 5^2 \cdot 7^2 \cdot 13 \cdot 17$. Since $p \neq r$, we have $p \in \{3, 5, 7, 13, 17\}$. Suppose that $X \neq 1$. By Lemma 5.6, X has an elementary abelian subgroup $Y \neq 1$. on which t acts nontrivially. If $p = 13$, then since $p \neq s$ we have $s = 17$. Further we must have $Y = C_{13}$. This is a contradiction since C_{13} does not admit an order 17 automorphism. If $p = 17$, then $s = 13$ and we obtain the analogous contradiction. If $p = 5$ or $p = 7$, then since $5 = 2^2 + 1 = \Phi_4(q)$ and $7 = 2^2 + 2 + 1 = \Phi_3(q)$, and these cyclotomic polynomials appear with exponent 2 in the factorization of G, we may apply Theorem 5.11 to obtain $m_p(G) = 2$. Hence $Y \cong E_{5^n}$ or $Y \cong E_{7^n}$ with $n \leq 2$. So $Aut(Y) \cong GL_n(5)$ or $Aut(Y) \cong GL_n(7)$ respectively. Then we have a contradiction since neither 17 nor 13 divides $Aut(Y)$. So we may assume that $p = 3$. Since $3 = 2 + 1$, Theorem 5.11 gives $m_3(G) = 4$. So $Y \cong E_{3^n}$ for $n \leq 4$ and $Aut(Y) \cong GL_n(3)$. So 17 does not divide $Aut(Y)$ and hence we have $s = 13$. Since 13 divides $Aut(Y)$, we have $n = 3$ or $n = 4$. As discussed in Remark 5.7, we have $Y = [Y, t]$ so $n = 3$. So a priori we do have a triple (G, t, Y) of type (Hs) with $s = 13$ and $Y \cong E_{3^3}$.

It remains to show that such triples do indeed exist. By [ATLAS], G has a subgroup $H \cong PSL_4(3)$. The group H has a maximal parabolic subgroup P with unipotent radical $U \cong E_{3^3}$ and Levi complement $L \cong GL_3(3)$. Now taking $Y = U$ and t an element of L of order 13 gives a triple (G, t, Y) of type $(H13)$.

We may now assume that X is nonabelian. Arguing as in the proof of Lemma 5.4, we may see that $X_0 = [Z(X), t]$ is an abelian $C_G(t)$-signalizer. By the analysis above, if $X_0 \neq 1$, then $G \cong F_4(2)$, $s = 13$ and $X_0 \cong E_{3^3}$. Since X is nonabelian, there exists an element of X outside $Z(X)$. Since this element commutes with $Z(X)$, we have $m_3(X) = 4$. In particular, since X is nonabelian, we have $|X| = 3^5$ or $|X| = 3^6$. Now since $XC_G(t) \leq N_G(X)$, we certainly have that $XC_G(t)$ is contained in a maximal local subgroup of G. A list of such subgroups of $F_4(2)$ can be found in [ATLAS] and it is easily seen from our previous results that no such subgroup can admit a signalizer X with $|X| = 3^5$ or $|X| = 3^6$. This is a contradiction and so we may assume that $X_0 = 1$.

[*Alternatively:* the following MAGMA code and output shows that no subgroup of G is normalized by an order 13 element of G.

```
> G := ChevalleyGroup("F",4,2);
> S := Sylow(G,3);
A:=Subgroups(S: OrderEqual:=3^5);
for i in [1..#A] do
```

```
for> Ni:=Normalizer(G,A[i]`subgroup);
for> i, Factorization(#Ni);
for> end for;

1 [ <2, 3>, <3, 6> ]
2 [ <2, 4>, <3, 6> ]
3 [ <2, 7>, <3, 6> ]
4 [ <2, 4>, <3, 6> ]
5 [ <2, 2>, <3, 6> ]
6 [ <2, 2>, <3, 6> ]
7 [ <2, 2>, <3, 6> ]
8 [ <2, 1>, <3, 6> ]
9 [ <2, 3>, <3, 6> ]
10 [ <2, 1>, <3, 6> ]
11 [ <2, 2>, <3, 6> ]
12 [ <2, 1>, <3, 6> ]
13 [ <2, 1>, <3, 6> ]
```

Furthermore the following MAGMA code and output shows that no subgroup of G of order 3^6 is normalized by an order 13 element of G.

```
> Factorization(#Normalizer(G,S));
[ <2, 3>, <3, 6> ]
```

So we again see that we may assume that $X_0 = 1$.]

Hence $Z(X) \leq C_G(t)$ and so $X\langle t\rangle \leq C_G(z)$ for some $z \in Z(X)$ of order p. Then we may apply Lemma 5.5 to obtain $X \leq L_1 \times L_2 \times ... \times L_j$ where, for each i, $L_i \cong A^{\pm}_{m_i}(q^{a_i})$, or $L_i \cong B_{m_i}(q^{a_i})$, or $L_i \cong C_{m_i}(q^{a_i})$ and each projection (L_i, t, X_i) is a triple of type (Hs). Then we may apply Propositions 5.47, 5.56 and 5.71 to obtain $X_i = 1$ for each i and so $X = 1$. □

Lemma 5.79. *Let $G \cong {}^2F_4(q)$ where $q = 2^{1+2a}$. Let X be a p-subgroup of G and let $t \in Inndiag(G)$ such that (G, t, X) is a triple of type (Hs). Then $X = 1$.*

Proof. Suppose first that X is abelian. The order of G factorizes into a product of cyclotomic polynomials as

$$|G| = q^{12} \cdot (q-1)^2 \cdot (q+1)^2 \cdot (q^2+1)^2 \cdot (q^2-q+1) \cdot (q^4-q^2+1)$$

Since s is prime, s divides one of the factors in this product. If s divides one of $q-1$, $q+1$ or q^2+1, then since each of these polynomials appears with exponent 2 in the factorization of $|G|$, we may apply Theorem 5.11 and Corollary 5.12 to see that there is a subgroup $Z = \langle t, t_1 \rangle \cong C_s^2$ of $C_G(t)$. Since $C_G(t) \leq N_G(X)$, Z acts on X. So by Theorem 3.5, $X = \langle C_X(u) : u \in Z^\# \rangle$. Choose $u \in Z^\#$ such that $C_X(u)$ as large as possible. Note that u is not a power of t since $C_X(t) = 1$. Certainly $C_X(u)\langle t \rangle \leq C_G(u)$. Then we are in the conditions of Lemma 5.5. Hence $C_X(u) \leq L_1 \times L_2 \times ... \times L_j$ where, for each i, $L_i \cong A^{\pm}_{m_i}(q^{a_i})$, or $L_i \cong B_{m_i}(q^{a_i})$, or $L_i \cong C_{m_i}(q^{a_i})$ and each projection $(L_i, t, C_X(u)_i)$ is of type (Hs). Then we may apply Propositions 5.47, 5.56 and 5.71 to see that $C_X(u)_i = 1$ for each i and so $C_X(u) = 1$. Now since we chose $C_X(u)$ as large as possible we must have $X = 1$.

Thus we may assume that either s divides $q^2 - q + 1 = \Phi_6(q)$ or that s divides $q^4 - q^2 + 1 = \Phi_{12}(q)$. By Table 5.4.C, the smallest dimension of a faithful representation of G is 26. If s divides $q^2 - q + 1$, then Lemma 5.75 gives $q^2 - q + 1 \leq 26$. Since q is an odd power of 2 we must have $q = 2$. So s divides $2^2 - 2 + 1 = 3$, which is a contradiction since $s > 5$. So s divides $q^4 - q^2 + 1$. Then Lemma 5.75 gives $q^4 - q^2 + 1 \leq 26$, so $q = 2$ and $G = {}^2F_4(2)$. Since s divides $2^4 - 2^2 + 1$, we have $s = 13$.

By Table 2.2 [GLS3], $|G| = 2^{12} \cdot 3^3 \cdot 5^2 \cdot 13$. Since $p \neq s$ and $p \neq r$, we have $p \in \{3, 5\}$. Suppose $X \neq 1$. By Lemma 5.6, X has an elementary abelian subgroup Y on which t acts nontrivially. Since $3 = 2 + 1 = \Phi_2(q)$ and $5 = 2^2 + 1 = \Phi_4(q)$ and these polynomials each appear with exponent 2 in the factorization of G, we may apply Theorem 5.11 to obtain $m_p(G) = 2$. Hence $Y \cong E_{3^n}$ or $Y \cong E_{5^n}$ with $n \leq 2$ and so $Aut(Y) \cong GL_n(3)$ or $Aut(Y) \cong GL_n(5)$ respectively. This is a contradiction since 13 does not divide $Aut(Y)$.

So we may assume that X is nonabelian. Then we may apply Lemmas 5.4 and 5.5 to obtain $X\langle t \rangle \leq C_G(z)$ for some $z \in Z(X)$ of order p and so $X \leq L_1 \times L_2 \times ... \times L_j$ where, for each i, $L_i \cong A^{\pm}_{m_i}(q^{a_i})$, or $L_i \cong B_{m_i}(q^{a_i})$, or $L_i \cong C_{m_i}(q^{a_i})$ and each projection (L_i, t, X_i) is a triple of type (Hs). Then we may apply Propositions 5.47, 5.56 and 5.71 to obtain $X_i = 1$ for each i and so $X = 1$. □

Lemma 5.80. *Let $G \cong E_6^{\pm}(q)$. Let X be a p-subgroup of G and let $t \in Inndiag(G)$ be such that (G, t, X) is a triple of type (Hs). Then either $X = 1$ or one of the following holds*

(a) $G = E_6^-(q)$, $s = 13$, $q = 2$ and $X \cong E_{3^3}$;

(b) $G = E_6^-(q)$, $s = 13$, $q = 2$ and $X \cong 3^{3+3}$.

Further, triples of type (Hs) described in (a) and (b) do indeed exist.

Proof. By Lemma 5.2, we may assume that G is universal. Suppose first that X is abelian. The order of G factorizes into a product of cyclotomic polynomials as follows.

$|E_6(q)| = q^{36} \cdot (q-1)^6 \cdot (q+1)^4 \cdot (q^2+q+1)^3 \cdot (q^2+1)^2 \cdot (q^2-q+1)^2 \cdot (q^4+q^3+q^2+q+1) \cdot (q^4+1) \cdot (q^6+q^3+1) \cdot (q^4-q^2+1)$

$|E_6^-(q)| = q^{36} \cdot (q-1)^4 \cdot (q+1)^6 \cdot (q^2+q+1)^2 \cdot (q^2+1)^2 \cdot (q^2-q+1)^3 \cdot (q^4+1) \cdot (q^4 - q^3 + q^2 - q + 1) \cdot (q^4 - q^2 + 1) \cdot (q^6 - q^3 + 1)$

Since s is prime, s divides one of the factors of $|G|$. Suppose that s divides one of $q-1$, $q+1$, q^2+q+1, q^2+1 or q^2-q+1. Then since each of these polynomials appears with exponent greater than 1 in the factorization of $|G|$, we may apply Theorem 5.11 and Corollary 5.12 to see that there is a subgroup $Z = \langle t, t_1 \rangle \cong C_s^2$ of $C_G(t)$. Since $C_G(t) \leq N_G(X)$, Z acts on X. So by Theorem 3.5, $X = \langle C_X(u) : u \in Z^\# \rangle$. Choose $u \in Z^\#$ such that $C_X(u)$ as large as possible. Note that u is not a power of t since $C_X(t) = 1$. Certainly $C_X(u)\langle t \rangle \leq C_G(u)$. Then we are in the conditions of Lemma 5.5. Hence $C_X(u) \leq L_1 \times L_2 \times ... \times L_j$ where, for each i, $L_i \cong A_{m_i}^{\pm}(q^{a_i})$ or $L_i \cong D_{m_i}^{\pm}(q^{a_i})$ and each projection $(L_i, t, C_X(u)_i)$ is of type (Hs). Then we may apply Propositions 5.47 and 5.71 to see that $C_X(u)_i = 1$ for each i and so $C_X(u) = 1$. Now since we chose $C_X(u)$ as large as possible we must have $X = 1$.

So we may assume that s divides one of $q^4 + q^3 + q^2 + q + 1 = \Phi_5(q)$ (only if $G = E_6(q)$), $q^4 + 1 = \Phi_8(q)$, $q^6 + q^3 + 1 = \Phi_9(q)$ (only if $G = E_6(q)$), $q^4 - q^2 + 1 = \Phi_{12}(q)$, $q^4 - q^3 + q^2 - q + 1 = \Phi_{10}(q)$ (only if $G = E_6^-(q)$) or $q^6 - q^3 + 1 = \Phi_{18}(q)$ (only if $G = E_6^-(q)$). By Table 5.4.C, the smallest dimension of a faithful representation of G is 27. Now we may apply Lemma 5.75 to see that if s divides $\Phi_i(q)$, then $\Phi_i(q) \leq 27$. Thus the possibilities for (q, s) are as follows.

- If $G = E_6(q)$, then (q, s) is one of $(2, 13)$ or $(2, 17)$.
- If $G = E_6^-(q)$, then (q, s) is one of $(2, 11)$, $(2, 13)$, $(2, 17)$.

In all cases, we have $q = 2$. Suppose first that $G = E_6(2)$.

Suppose that $s = 13$. By Table 2.2 [GLS3], $|G| = 2^{36} \cdot 3^6 \cdot 5^2 \cdot 7^3 \cdot 13 \cdot 17 \cdot 31 \cdot 73$. The following MAGMA code shows that $C_G(t)$ contains an element v of order 7.

```
> G := ChevalleyGroup("E",6,2);
> T := Sylow(G,13);
> C := Centralizer(G,T);
> Factorization(#C);
```

Suppose that $X \neq 1$. By Lemma 5.6, X has an elementary abelian subgroup $Y \neq 1$ on which t acts nontrivially. No elementary abelian group of order 5, 5^2, 7, 7^2, 7^3, 17, 31 or 73 admits an automorphism of order 13. Hence $p = 3$. By applying Theorem 5.11 we obtain $m_3(G) = 4$ and so $Y \cong E_{3^3}$ or $Y \cong E_{3^4}$. In particular, v acts trivially on Y. Thus $Y\langle t \rangle \leq C_G(v)$ and we may apply Lemmas 5.4 and 5.5 to obtain $Y = 1$ which is a contradiction.

Therefore $s = 17$. Again X has an elementary abelian subgroup $Y \neq 1$ on which t acts nontrivially. No elementary abelian group of order 5, 5^2, 7, 7^2, 7^3, 13, 31 or 73 admits an automorphism of order 17. Therefore $p = 3$. By applying Theorem 5.11 we obtain $m_3(G) = 4$ and so no elementary abelian 3-subgroup of G admits an order 17 automorphism either. This is a contradiction and so $X = 1$.

So we may assume that $G = E_6^-(2)$. By Table 2.2 [GLS3], $|G| = 2^{36}\cdot 3^9\cdot 5^2\cdot 7^2\cdot 11\cdot 13\cdot 17\cdot 19$.

Suppose that $s = 11$. Assume that $X \neq 1$. By Lemma 5.6, X has an elementary abelian $Y \neq 1$ on which t acts nontrivially. Since no elementary abelian group of order 5, $5, 2$, 7, 7^2, 13, 17 or 19 can admit an order 11 automorphism, we must have $p = 3$. Since $3 = 2 + 1 = \Phi_2(q)$, we may apply Theorem 5.11 to obtain $m_3(G) = 6$. Since $Y = [Y, t]$ we must have $Y \cong E_{3^5}$. Further, by Theorem 5.1 (iii), we have $C_Y(t) = 1$ and hence $Z(G) \cap Y = 1$. So by Lemma 5.2, we may assume that $G = G_a$. By [ATLAS], $C_G(t) \cong C_{11} \times C_3 \times C_2$. Since $C_Y(t) = 1$, there is a 3-element $z \in C_G(t)$ acting on Y but not contained in Y. Since Y is a 3-group we have $C_Y(z) \neq 1$. Now t acts on $C_Y(z)$. If $C_Y(z) \neq Y$, then $C_Y(z)$ has order 3^n for $n < 5$ so t must fix some $y \in C_Y(z)$. This is a contradiction so z must fix all of Y. By [ATLAS], G has a subgroup $H \cong Fi_{22}$ and furthermore, any Sylow 3-subgroup of H is also a Sylow 3-subgroup of G. However $m_3(Fi_{22}) = 5$ by Table 5.6.1 [GLS3]. This contradicts the fact that we have a subgroup $Y \cong E_{3^5}$ which is centralized by another 3-element. Hence $X = 1$.

Now suppose that $s = 13$. Assume that $X \neq 1$. By Lemma 5.6, X has an elementary abelian $Y \neq 1$ on which t acts nontrivially. Since no elementary abelian group of order 5, $5, 2$, 7, 7^2, 11, 17 or 19 can admit an order 13 automorphism, we must have $p = 3$. Since $Y = [Y, t]$, we have $Y \cong E_{3^3}$ or $Y \cong E_{3^6}$. If $Y \cong E_{3^6}$, then since $m_3(G) = 6$, Y must contain $Z(G)$ which contradicts the fact that $C_Y(t) = 1$. So $Y \cong E_{3^3}$. Further, by Lemma 5.2, we may assume that $G = G_a$. By [ATLAS], $C_G(t) \cong C_{13}$. Furthermore, G has a subgroup $H \cong F_4(2)$. By Lemma 5.78, there is a triple (H, t, Y) of type $(H13)$ with $Y \cong E_{3^3}$. Since $C_G(t)$ consists only of the powers of t, (G, t, Y) is of type $(H13)$ as well.

Now suppose that $s = 17$. By Lemma 5.6, X has an elementary abelian subgroup $Y \neq 1$ on which t acts nontrivially. This is a contradiction since no elementary abelian group of order 3^n (for $n \leq 6$), 5, $5, 2$, 7, 7^2, 11, 13 or 19 can admit an order 17 automorphism.

We may now assume that X is nonabelian. Lemma 5.6 gives us that X contains a characteristic subgroup Y of class at most 2, exponent p, with $Y' = \Phi(Y)$ and such that t acts faithfully on Y. Further, by Remark 5.7, if we set $R = [R, t]$, then (G, t, R) is a triple of type (Hs). Arguing as in the proof of Lemma 5.4, we may see that $R_0 = [Z(R), t]$ is an abelian $C_G(t)$-signalizer. By the analysis above, if $R_0 \neq 1$, then $G \cong E_6^-(2)$, $s = 13$ and $R_0 \cong E_{3^3}$.

By Theorem 5.1 (iii) we have $Z(R) \cong R_0 \times C_{Z(R)}(t)$. So if there exists $z \in Z(R) - R_0$ then we may assume that $z \in C_{Z(R)}(t)$. So $R\langle t\rangle \leq C_G(z)$. Then we may apply Lemma 5.5 to obtain $R \leq L_1 \times L_2 \times ... \times L_j$ where, for each i, $L_i \cong A^{\pm}_{m_i}(2^{a_i})$ or $L_i \cong D^{\pm}_{m_i}(2^{a_i})$, and each projection (L_i, t, X_i) is a triple of type $(H13)$. Then we may apply Propositions 5.47 and 5.71 to obtain $R_i = 1$ for each i and so $R = 1$. This would contradict the fact that Y

is critical and so we would have $X = 1$. Therefore we may assume that no such z exists, and so $Z(R) = R_0 \cong E_{3^3}$.

Since $R \lhd Y$, applying Lemma 2.18 and using the fact that Y has class 2 gives $\Phi(R) \leq \Phi(Y) = Y' \leq Z(Y)$. So $\Phi(R) \leq Z(R) \cong E_{3^3}$. By Lemma 2.19, $R/\Phi(R)$ is elementary abelian and hence so is $R/Z(R)$. Further, since $R = [R, t]$, we have $R/Z(R) = [R/Z(R), t]$. Since 3^9 is the largest power of G dividing G, we must have $R/Z(R) \cong E_{3^3}$ or E_{3^6}. So $R \cong 3^{3+3}$ or 3^{3+6}.

If $R \cong 3^{3+6}$, then R is a Sylow 3-subgroup of G. In particular, we may assume that R is contained in a subgroup $H \cong O_7(3)$ of G. Then the following MAGMA code and output demonstrates that $Z(R) = 1$.

```
 > G := SO(7,3);
> S := Sylow(G,3);
> Z := Center(S);
> Factorization(#Z);
[ <3, 1> ]
```

This is a contradiction since we should have $|Z(R)| = 3^3$. Therefore we must have $R \cong 3^{3+3}$. It remains to show that this situation really can occur. Now Theorem 4.8.10 (d) [GLS3] tells us exactly that there exists a special subgroup Q of G of order 3^6 with center $Z(Q)$ elementary abelian of order 3^3, such that $N_G(Q)/Q \cong SL_3(3)$ and $[Q, g] = Q$ for any order 13 element g of $N_G(Q)$. Taking $R = Q$ and t one such order 13 element gives the required triple (G, t, R) of type $(H13)$.

In all other cases of X being nonabelian, we may assume that $[Z(X), t] = 1$. Hence $Z(X) \leq C_G(t)$ and so $X\langle t\rangle \leq C_G(z)$ for some $z \in Z(X)$ of order p. Then we may apply Lemma 5.5 to obtain $X\langle t\rangle \leq C_G(z)$ for some $z \in Z(X)$ of order p and so $X \leq L_1 \times L_2 \times ... \times L_j$ where, for each i, $L_i \cong A^{\pm}_{m_i}(q^{a_i})$ or $L_i \cong D^{\pm}_{m_i}(q^{a_i})$, and each projection (L_i, t, X_i) is a triple of type (Hs). Then we may apply Propositions 5.47 and 5.71 to obtain $X_i = 1$ for each i and so $X = 1$. □

Lemma 5.81. *Let $G \cong E_7(q)$. Let X be a p-subgroup of G and let $t \in Inndiag(G)$ be such that (G, t, X) is a triple of type (Hs). Then $X = 1$.*

Proof. By Lemma 5.2, we may assume that G is universal. Suppose first that X is abelian. The order of G factorizes into a product of cyclotomic polynomials as follows.

$|G| = q^{63} \cdot (q-1)^7 \cdot (q+1)^7 \cdot (q^2+q+1)^3 \cdot (q^2+1)^2 \cdot (q^4+q^3+q^2+q+1) \cdot (q^2-q+1)^3 \cdot (q^6+q^5+q^4+q^3+q^2+q+1) \cdot (q^4+1) \cdot (q^6+q^3+1) \cdot (q^4-q^3+q^2-q+1) \cdot (q^4-q^2+1) \cdot (q^6-q^5+q^4-q^3+q^2-q+1) \cdot (q^6-q^3+1)$

Since s is prime, s divides one of the factors of $|G|$. Suppose that s divides one of $q-1$, $q+1$, q^2+q+1, q^2+1 or q^2-q+1. Then since each of these polynomials appears with exponent greater than 1 in the factorization of $|G|$, we may apply Theorem 5.11 and Corollary 5.12 to see that there is a subgroup $Z = \langle t, t_1 \rangle \cong C_s^2$ of $C_G(t)$. Since $C_G(t) \leq N_G(X)$, Z acts on X. So by Theorem 3.5, $X = \langle C_X(u) : u \in Z^{\#} \rangle$. Choose $u \in Z^{\#}$ such that $C_X(u)$ as large as possible. Note that u is not a power of t since $C_X(t) = 1$. Certainly $C_X(u)\langle t \rangle \leq C_G(u)$. Then we are in the conditions of Lemma 5.5. Hence $C_X(u) \leq L_1 \times L_2 \times ... \times L_j$ where, for each i, $L_i \cong A^{\pm}_{m_i}(q^{a_i})$, or $L_i \cong D^{\pm}_{m_i}(q^{a_i})$, or $L_i \cong E^{\pm}_6(q^{a_i})$ and each projection $(L_i, t, C_X(u)_i)$ is of type (Hs). Then we may apply Propositions 5.47 and 5.71 and Lemma 5.80 to see that $C_X(u)_i = 1$ for each i and so $C_X(u) = 1$. Now since we chose $C_X(u)$ as large as possible we must have $X = 1$.

So we may assume that s divides one of $q^4+q^3+q^2+q+1 = \Phi_5(q)$, $q^6+q^5+q^4+q^3+q^2+q+1 = \Phi_7(q)$, $q^4+1 = \Phi_8(q)$, $q^6+q^3+1 = \Phi_9(q)$, $q^4-q^2+1 = \Phi_{12}(q)$, $q^4-q^3+q^2-q+1 = \Phi_{10}(q)$, $q^6-q^5+q^4-q^3+q^2-q+1 = \Phi_{14}(q)$ or $q^6-q^3+1 = \Phi_{18}(q)$. By Table 5.4.C, the smallest dimension of a faithful representation of G is 56. Now we may apply Lemma 5.75 to see that if s divides $\Phi_i(q)$, then $\Phi_i(q) \leq 56$. Thus the possibilities for (q, s) are $(2, 11)$, $(2, 13)$, $(2, 17)$, $(2, 31)$, $(2, 43)$ or $(3, 41)$. In particular, we have $G = E_7(2)$ unless $s = 41$, in which case $G = E_7(3)$. By Table 2.2 [GLS3], the orders of these groups are

$$|E_7(2)| = 2^{63} \cdot 3^{11} \cdot 5^2 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 31 \cdot 43 \cdot 73 \cdot 127$$

$$|E_7(3)| = 2^{24} \cdot 3^{63} \cdot 5^2 \cdot 7^3 \cdot 11^2 \cdot 13^3 \cdot 19 \cdot 37 \cdot 41 \cdot 61 \cdot 73 \cdot 547 \cdot 757 \cdot 1093$$

We now examine the possibilities for (q, s) case by case.

(i) $(q, s) = (2, 11)$. Suppose $X \neq 1$. By Lemma 5.6 X has an elementary abelian critical subgroup $Y \neq 1$ on which t acts nontrivially. Since no elementary abelian group of order 5, 5^2, 7, 7^2, 7^3, 13, 17, 19, 31, 43, 73 or 127 admits an order 11 automorphism, we may only have $p = 3$. Furthermore, Theorem 5.11 gives $m_3(G) = 7$. By Theorem 5.1 (iii), $C_Y(t) = 1$ and hence $Y \cong E_{3^5}$. By [ATLAS], G has a subgroup $H \cong S_3 \times O^+_{12}(2)$. Since 11 divides $|H|$, we may assume that $t \in H$. So $C_G(t)$ contains a 3-element z. By Lemma 5.6 (i), z acts on Y. Certainly $C_Y(z)\langle t \rangle \leq C_G(z)$ and so we are in the situation of Lemma 5.5. Hence $C_Y(z) \leq L = O^{2'}(C_G(z))$. Further, Table 4.7.3 [GLS3] gives a list of possibilities for L, namely $D_6(2)$, $A^-_2(2) \circ A^-_5(2)$, $A^-_6(2)$, $D^-_6(2) \circ A_1(2)$ or $E_6(2)$. Now we may apply Propositions 5.47 and 5.71 and Lemma 5.80 to conclude that $C_Y(z) = 1$. This is a contradiction since z is a 3-element acting on a 3-group Y.

(ii) $(q, s) = (2, 13)$. Suppose that $X \neq 1$. Again X has an elementary abelian subgroup $Y \neq 1$ on which t acts nontrivially. Since no elementary abelian group of order 5, 5^2, 7, 7^2, 7^3, 11, 17, 19, 31, 43, 73 or 127 admits an order 13 automorphism, we again have $p = 3$. By [ATLAS], G has a subgroup $H \cong L_2(8) \times {}^3D_4(2)$. Since 13 divides $|H|$, we may assume that $t \in H$. So there exists a 3-element $z \leq C_G(t)$. Since z acts on Y we have $C_Y(z)\langle t\rangle \leq C_G(z)$. Then we obtain $C_Y(z) = 1$ exactly as in (i) and this is again a contradiction.

(iii) $(q, s) = (2, 17)$. Suppose $X \neq 1$. Again X has an elementary abelian subgroup $Y \neq 1$ on which t acts nontrivially. Since no elementary abelian group of order 5, 5^2, 7, 7^2, 7^3, 11, 13, 19, 31, 43, 73 or 127 admits an order 17 automorphism, we again have $p = 3$. Furthermore, since $3 = 2 + 1 = \Phi_2(q)$, Theorem 5.11 gives $m_3(G) = 7$. Since 17 does not divide $|GL_3(7)|$, $Aut(Y)$ cannot contain an element of order 17 and this is also a contradiction.

(iv) $(q, s) = (2, 31)$. Suppose $X \neq 1$. Again X has an elementary abelian subgroup $Y \neq 1$ on which t acts nontrivially. This is a contradiction since no elementary abelian group of order 3^n (for $n \leq 7$), 5, 5^2, 7, 7^2, 7^3, 11, 13, 17, 19, 43, 73 or 127 admits an order 31 automorphism.

(v) $(q, s) = (2, 43)$. Suppose $X \neq 1$. Again X has an elementary abelian subgroup $Y \neq 1$ on which t acts nontrivially. This is a contradiction since no elementary abelian group of order 3^n (for $n \leq 7$), 5, 5^2, 7, 7^2, 7^3, 11, 13, 17, 19, 31, 73 or 127 admits an order 43 automorphism.

(vi) $(q, s) = (3, 41)$. Suppose $X \neq 1$. Again X has an elementary abelian subgroup $Y \neq 1$ on which t acts nontrivially. Since no elementary abelian group of order 5, 5^2, 7, 7^2, 7^3, 11, 11^2, 13, 13^2, 13^3, 19, 37, 61, 73, 547, 757 or 1093 admits an order 41 automorphism, we must have $p = 2$. Further, by Corollary [CS], $m_2(G) = 7$. Since 41 does not divide $|GL_7(2)|$, $Aut(Y)$ does not contain an element of order 41, which is a contradiction.

Therefore we may assume that X is nonabelian. Then we may apply Lemmas 5.4 and 5.5 to obtain $X\langle t\rangle \leq C_G(z)$ for some $z \in Z(X)$ of order p and so $X \leq L_1 \times L_2 \times ... \times L_j$ where, for each i, $L_i \cong A^{\pm}_{m_i}(q^{a_i})$, or $L_i \cong D^{\pm}_{m_i}(q^{a_i})$, or $L_i \cong E^{\pm}_6(q^{a_i})$, and each projection (L_i, t, X_i) is a triple of type (Hs). Then we may apply Propositions 5.47 and 5.71 and Lemma 5.80 to conclude that, for each i, either $X_i = 1$, or $L_i \cong E^-_6(2)$ and $X_i \cong 3^{3+3}$. In the latter case $p = 3$ and so Table 4.7.3A [GLS3] gives exactly the possibilities for the L_i. In particular we cannot have $L_i \cong E^-_6(q)$. Hence $X_i = 1$ in all cases and so $X = 1$.

□

Lemma 5.82. *Let $G \cong E_8(q)$. Let X be a p-subgroup of G and let $t \in Inndiag(G)$ be such that (G, t, X) is a triple of type (Hs). Then $X = 1$.*

Proof. Suppose first that X is abelian. The order of G factorizes into a product of cyclotomic polynomials as follows.

$|G| = q^{120} \cdot \Phi_1(q)^8 \cdot \Phi_2(q)^8 \cdot \Phi_3(q)^4 \cdot \Phi_4(q)^4 \cdot \Phi_5(q)^2 \cdot \Phi_6(q)^4 \cdot \Phi_7(q) \cdot \Phi_8^2 \cdot \Phi_9(q) \cdot \Phi_{10}(q)^2 \cdot \Phi_{12}(q)^2 \cdot \Phi_{14}(q) \cdot \Phi_{15}(q) \cdot \Phi_{18}(q) \cdot \Phi_{20}(q) \cdot \Phi_{24}(q) \cdot \Phi_{30}(q)$

where the cyclotomic polynomials are given by the following list.

$\Phi_1(q) = q - 1$

$\Phi_2(q) = q + 1$

$\Phi_3(q) = q^2 + q + 1$

$\Phi_4(q) = q^2 + 1$

$\Phi_5(q) = q^4 + q^3 + q^2 + q + 1$

$\Phi_6(q) = q^2 - q + 1$

$\Phi_7(q) = q^6 + q^5 + q^4 + q^3 + q^2 + q + 1$

$\Phi_8(q) = q^4 + 1$

$\Phi_9(q) = q^6 + q^3 + 1$

$\Phi_{10}(q) = q^4 - q^3 + q^2 - q + 1$

$\Phi_{12}(q) = q^4 - q^2 + 1$

$\Phi_{14}(q) = q^6 - q^5 + q^4 - q^3 + q^2 - q + 1$

$\Phi_{15}(q) = q^8 - q^7 + q^5 - q^4 + q^3 - q + 1$

$\Phi_{18}(q) = q^6 - q^3 + 1$

$\Phi_{20}(q) = q^8 - q^6 + q^4 - q^2 + 1$

$\Phi_{24}(q) = q^8 - q^4 + 1$

$\Phi_{30}(q) = q^8 + q^7 - q^5 - q^4 - q^3 + q + 1$

Since s is prime, s divides one of the factors of $|G|$. Suppose that s divides Φ_i, for $i \in \{1, 2, 3, 4, 5, 6, 8, 10, 12\}$. Then since each of these polynomials appears with exponent greater than 1 in the factorization of $|G|$, we may apply Theorem 5.11 and Corollary 5.12 to see that there is a subgroup $Z = \langle t, t_1 \rangle \cong C_s^2$ of $C_G(t)$. Since $C_G(t) \leq N_G(X)$, Z acts on X. So by Theorem 3.5, $X = \langle C_X(u) : u \in Z^{\#} \rangle$. Choose $u \in Z^{\#}$ such that $C_X(u)$ as large as possible. Note that u is not a power of t since $C_X(t) = 1$. Certainly $C_X(u)\langle t \rangle \leq C_G(u)$. Then we are in the conditions of Lemma 5.5. Hence $C_X(u) \leq L_1 \times L_2 \times ... \times L_j$ where, for each i, $L_i \cong A^{\pm}_{m_i}(q^{a_i})$, or $L_i \cong D^{\pm}_{m_i}(q^{a_i})$, or $L_i \cong E^{\pm}_6(q^{a_i})$, or $L_i \cong E_7(q^{a_i})$, and each projection $(L_i, t, C_X(u)_i)$ is of type (Hs). Then we may apply Propositions 5.47 and 5.71 and Lemmas 5.80 and 5.81 to see that $C_X(u)_i = 1$ for each i and so $C_X(u) = 1$. Now since we chose $C_X(u)$ as large as possible we must have $X = 1$.

So we may assume that s divides $\Phi_i(q)$ where $i \in \{7, 9, 14, 15, 18, 20, 24, 30\}$. By Table 5.4.C, the smallest dimension of a faithful representation of G is 248. Now we may apply Lemma 5.75 to see that if s divides $\Phi_i(q)$, then $\Phi_i(q) \leq 248$. Thus the possibilities for (q, s) are $(2, 19)$, $(2, 41)$, $(2, 43)$, $(2, 73)$, $(2, 127)$, $(2, 151)$ or $(2, 241)$. In particular, $G = E_8(2)$, so

$$|G| = 2^{120} \cdot 3^{13} \cdot 5^5 \cdot 7^4 \cdot 11^2 \cdot 13^2 \cdot 17^2 \cdot 19 \cdot 31^2 \cdot 41 \cdot 43 \cdot 73 \cdot 127 \cdot 151 \cdot 241 \cdot 331$$

Suppose that $X \neq 1$. Since X is abelian, we may apply Lemma 5.6 to see that X has an elementary abelian subgroup Y on which t acts nontrivially. Say $Y \cong E_{p^n}$. Then $Aut(Y) \cong GL_n(p)$. The rank n of Y is bounded above by the p-rank $m_p(G)$ of G. We obtain the following results on p-rank directly from Theorem 5.11.

$m_3(G) = 8$,

$m_5(G) = m_7(G) = 4$,

$m_{11}(G) = m_{13}(G) = m_{17}(G) = m_{31}(G) = 2$,

and all other odd p-ranks equal to 1. We now list the relevant values of $|GL_n(p)|$.

$|GL_8(3)| = 2^{19} \cdot 3^{28} \cdot 5^2 \cdot 7 \cdot 11^2 \cdot 13^2 \cdot 41 \cdot 1093$

$|GL_4(5)| = 2^{11} \cdot 3^2 \cdot 5^6 \cdot 13 \cdot 31$

$|GL_4(7)| = 2^{11} \cdot 3^5 \cdot 5^2 \cdot 7^6 \cdot 19$

$|GL_2(11)| = 2^4 \cdot 3 \cdot 5^2 \cdot 11$

$|GL_2(13)| = 2^5 \cdot 3^2 \cdot 7 \cdot 13$

$|GL_2(17)| = 2^9 \cdot 3^2 \cdot 17$

$|GL_1(19)| = 2 \cdot 3^2$

$|GL_2(31)| = 2^7 \cdot 3^2 \cdot 5^2 \cdot 31$

$|GL_1(41)| = 2^3 \cdot 5$

$|GL_1(43)| = 2 \cdot 3 \cdot 7$

$|GL_1(73)| = 2^3 \cdot 3^2$

$|GL_1(127)| = 2 \cdot 3^2 \cdot 7$

$|GL_1(151)| = 2 \cdot 3 \cdot 5^2$

$|GL_1(241)| = 2^4 \cdot 3 \cdot 5$

$|GL_1(331)| = 2 \cdot 3 \cdot 5 \cdot 11$

Since none of the above are divisible by 43, 73, 127, 151 or 241, no elementary abelian p-subgroup of G can admit an automorphism of order 43, 73, 127, 151 or 241. Hence $s = 19$ or $s = 41$. Furthermore, of the above list, only $|GL_8(3)|$ is divisible by 41 and only $|GL_4(7)|$ is divisible by 19. So if $s = 19$, then $p = 7$, whilst if $s = 41$, then $p = 3$.

We address the case $s = 19$, $p = 7$ first. By Theorem 5.1 (iii), $C_Y(t) = 1$. Hence $Y \cong E_{7^3}$. Let us consider $C_G(t)$. By Table 4.7.3 [GLS3], G has a 3-element z such that $O^{2'}(C_G(z)) \cong PSU_9(2)$. Furthermore, since 19 divides $|PSU_9(2)|$, we may assume that $t \in C_G(z)$. Since 19 divides 2^9+1, we may assume that t is contained in a cyclic subgroup C_{2^9+1} of $PSU_9(2)$. In particular, since $2^9+1 = 3^3 \cdot 19$, $C_G(t)$ contains a 3-element $z_1 \neq z$. So $C_G(t)$ has a subgroup $Z = \langle z, z_1 \rangle \cong C_3^2$. Since $C_G(t) \leq N_G(Y)$, Z acts on Y and so, by Theorem 3.5, $Y = \langle C_Y(u) : u \in Z^\# \rangle$. Then for each $u \in Z^\#$ we have $C_Y(u)\langle t \rangle \leq C_G(u)$. So we are in the conditions of Lemma 5.5. Hence $C_X(u) \leq L_1 \times L_2 \times ... \times L_j$ where, for each i, $L_i \cong A^{\pm}_{m_i}(q^{a_i})$, or $L_i \cong D^{\pm}_{m_i}(q^{a_i})$, or $L_i \cong E^{\pm}_6(q^{a_i})$, or $L_i \cong E_7(q^{a_i})$, and each projection $(L_i, t, C_X(u)_i)$ is of type (Hs). Then we may apply Propositions 5.47 and 5.71 and Lemmas 5.80 and 5.81 to see that $C_X(u)_i = 1$ for each i and so $C_X(u) = 1$. Now since we chose $C_X(u)$ as large as possible we must have $X = 1$.

We now deal with the case $s = 41$, $p = 3$. By Theorem 5.1 (iii), $C_Y(t) = 1$. Hence $Y \cong E_{3^8}$. Then $Y \cong C^8_{q+1}$ and so Y is a maximal torus in G. By Theorem 7.2.2 [Ca] and Section 3.6 [Ca], we have $|N_G(Y)|/|Y| = |W_{E_8}| = 2^{14} \cdot 3^5 \cdot 5^2 \cdot 7$. In particular, 41 does not divide $|N_G(Y)|$, which is a contradiction.

Therefore we may assume that X is nonabelian. Then we may apply Lemmas 5.4 and 5.5 to obtain $X\langle t \rangle \leq C_G(z)$ for some $z \in Z(X)$ of order p and so $X \leq L_1 \times L_2 \times ... \times L_j$ where, for each i, $L_i \cong A^{\pm}_{m_i}(q^{a_i})$, or $L_i \cong D^{\pm}_{m_i}(q^{a_i})$, or $L_i \cong E^{\pm}_6(q^{a_i})$, or $L_i \cong E_7(q^{a_i})$ and each projection (L_i, t, X_i) is a triple of type (Hs). Then we may apply Propositions 5.47 and 5.71 and Lemmas 5.80 and 5.81 to conclude that for each i, either $X_i = 1$ or $L_i \cong E^-_6(2)$ and $X_i \cong 3^{3+3}$. In the latter case $p = 3$ and so Table 4.7.3A [GLS3] gives exactly the possibilities for the L_i. In particular, we have $X \leq L_1 \circ L_2$ where $L_1 \cong E^-_6(2)$ and $L_2 \cong A^-_2(2)$. So if $X \neq 1$ we have $X = X_1 \cong 3^{3+3}$. This means that $Z(X)$ and $Z(L_1)$ intersect nontrivially, which contradicts the findings of Lemma 5.80. Hence $X_i = 1$ for all i and so $X = 1$.

$\square$

Chapter 6

The Case $p \neq r$, t a Field Automorphism

In this Chapter, we consider the triples (G, t, X) of type (Hs) where t is a field automorphism of $G \in Lie(r)$. As in Proposition 2.5 [Ko] we observe that if $C_G(t) \notin \{A_1(2), A_1(3), {}^2B_2(2)\}$, then $C_G(t)$ is a maximal subgroup of G by Theorem 1 [BGL]. In particular this means that either $C_G(t) = N_G(X)$ so that $X = [X, t] = 1$, or that $X \triangleleft G$ so that again $X = 1$. So we may assume that $C_G(t) \in \{A_1(2), A_1(3), {}^2B_2(2)\}$

Lemma 6.1. *Suppose t is a field automorphism of prime order $s > 3$ of the finite group $G \in Lie(r)$. We suppose that $C_G(t) \cong A_1(2) = SL_2(2) \cong S_3$. Let X be a p-subgroup of G with p prime, $p \neq s$, $p \neq 2$ and suppose that (G, t, X) is a triple of type (Hs). Then $G \cong A_1(2^s)$ and either $X = 1$ or $X \leq C_G(u)$, where $u \in C_G(t)$ has order 3. In this case 3 divides $2^s + 1$, X is a cyclic group whose order p^n also divides $2^s + 1$, and s divides $p - 1$. Furthermore, triples (G, t, X) of this type do indeed exist.*

Proof. By Lemma 2.9 (b), X is cyclic. Since $C_G(t) \leq N_G(X)$ we have an action φ of $C_G(t)$ on X. If φ is faithful, then we have an injection $S_3 \cong C_G(t) \hookrightarrow Aut(X)$. Since $X \cong C_{p^n}$, we have $Aut(X) \cong C_{(p-1)p^{n-1}}$. So since $C_G(t)$ is noncyclic, it cannot be mapped injectively into $Aut(X)$, which is a contradiction. Hence $ker(\varphi)$ is nontrivial. Since $ker(\varphi)$ is normal in $C_G(t) \cong S_3$, it is either of order 6 or order 3.

Case 1: $|ker(\varphi)| = 6$.

In this case $ker(\varphi) = C_G(t)$. This means that the action is trivial. Write $C_G(t) = \langle u, v \rangle$, where u is of order 3 and v of order 2. Then $X \leq C_G(v)$. Since $C_G(v)$ is a group of order 2^s, we have $p = 2$ which contradicts the hypothesis.

Case 2: $|ker(\varphi)| = 3$.

Again write $C_G(t) = \langle u, v \rangle$. Then $ker(\varphi) = \langle u \rangle$, so $X \leq C_G(u)$. Since s is odd, 3 divides

2^s+1 and so $C_G(u) \cong C_{2^s+1}$. Hence X is cyclic and p^n divides 2^s+1, as required. Further, the group $\langle t \rangle$ acts on X and has prime order s, so the kernel of this action has order either 1 or s. If the kernel is order s, then t acts trivially on X and hence $X = [X,t] = 1$. If it has order 1, then we see that s divides $p-1$ since again $Aut(X) \cong C_{(p-1)p^{n-1}}$, and $p \neq s$.

It remains to show that if we take an element $u \in C_G(t)$ of order 3 and X to be any p-subgroup of $C_G(u) \cong C_{2^s+1}$ such that s divides $p-1$, then we do indeed have a triple (G,t,X) of type (Hs). Since t acts on the cyclic group $C_G(u)$, t also acts on its subgroup X. Now a priori we have $X = [X,t] \times C_X(t)$ by Theorem 5.1 (iii). Since $C_X(t) \leq C_G(t) \cong S_3$ and $C_X(t)$ is a cyclic group, $C_X(t)$ has order 1, 2 or 3. If it has order 2 or 3, then $p=2$ or $p=3$, which contradicts the assumption that s divides $p-1$. Hence $C_X(t)$ is trivial and so $X = [X,t]$. Further, an order 2 element $v \in C_G(t)$ acts on $C_G(u)$ and so also acts on X. Hence $C_G(t) \leq N_G(X)$. So we have a triple (G,t,X) of type (Hs) (and this situation does indeed occur, for example when $s=5$, $p=11$). $\square$

Lemma 6.2. *Let $G \cong A_1(3^s)$. Assume $p \neq s$, $p \neq 3$ and otherwise adopt the same conditions on X, t as in Lemma 6.1, so that $C_G(t) \cong A_1(3)$. Then $X = 1$.*

Proof. By Lemma 5.2, we may assume that $G \cong PSL_2(3^s)$ and that $C_G(t) \cong PSL_2(3) \cong A_4$.

Assume p is odd. If $X \neq 1$, then it is a nontrivial subgroup of G of odd prime power order. So by Lemma 2.9 (d), $N_G(X)$ does not contain a subgroup isomorphic to A_4. This contradicts the assumption that $C_G(t) \leq N_G(X)$. Hence $X = 1$.

Now assume $p=2$. Then since X is a 2-group, it is contained in some $Y \in Syl_2(G)$. Since $3^s \equiv 3 \pmod 8$ (which is in fact true if s were any odd natural number), we have $Y \cong C_2 \times C_2$ by Lemma 2.9 (c). Hence X is isomorphic to one of $\{1, C_2, Y\}$ and so $Aut(X)$ is isomorphic to one of $\{1, S_3\}$. So $Aut(X)$ contains only elements of order 1, 2 or 3. Since t has prime order $s > 3$, it must act trivially on X. So $X = [X,t] = 1$. $\square$

Lemma 6.3. *Take $G \cong {}^2B_2(2^s)$. Again, adopt the conditions of Lemma 6.1 on X and t, so that $C_G(t) \cong {}^2B_2(2) \cong C_5 \rtimes C_4$ (A Frobenius group of order 20). Then either $X = 1$ or $X \leq C_G(y)$, where $y \in C_G(t)$ has order 5. In this case 5 divides one of $2^s \pm 2^{(s+1)/2} + 1$, X is a cyclic group whose order p^n also divides $2^s \pm 2^{(s+1)/2} + 1$, and s divides $p-1$. Furthermore, triples (G,t,X) of this type do indeed exist.*

Proof. By Theorem 9 [S], $N_G(X)$ is conjugate to a subgroup of G of one of the following isomorphism types.

(i) A group ${}^2B_2(2^b)$, where b is a proper divisor of s.

(ii) A Dihedral group of order $2(2^s-1)$.

(iii) A Frobenius group of order $2^{2s}(2^s-1)$.

(iv) A Frobenius group of order either $4(2^s+2^{(s+1)/2}+1)$ or $4(2^s-2^{(s+1)/2}+1)$.

In case (i), since s is prime, $b=1$. Hence $C_G(t)=N_G(X)$ and so $X=[X,t]=1$.

In cases (ii) and (iii), since $C_5 \rtimes C_4 \cong C_G(t) \leq N_G(X)$, we must have that 5 divides 2^s-1. This can only occur if s is even, which is a contradiction.

Hence we are in case (iv). By Theorem 9 [S], the Frobenius kernel of such a group is cyclic of order $2^s \pm 2^{(s+1)/2}+1$. Hence $X \leq N_G(X)$ is a cyclic group whose order p^n divides this. Note that s divides $p-1$ as in Proposition 1. Further, since again $C_G(t) \leq N_G(X)$, there is an action φ of $C_G(t) \cong C_5 \rtimes C_4$ on X. If φ is faithful, then we have an injection ${}^2B_2(2) \cong C_G(t) \hookrightarrow Aut(X) \cong C_{p^{n-1}(p-1)}$, which is a contradiction since ${}^2B_2(2)$ is noncyclic. Hence $ker(\varphi)$ is nontrivial. Further, $ker(\varphi)$ is normal in $C_G(t)$. Since $C_G(t)$ is a Frobenius group of order 20, $|ker(\varphi)|$ is not equal to 2 or to 4, and so is divisible by 5. Hence there is an element $y \in C_G(t)$ of order 5 which acts trivially on X, and so $X \leq C_G(y)$, as required.

It remains to show that if we take an element $y \in C_G(t)$ of order 5 and take X to be a p-subgroup of $C_G(y)$ such that s divides $p-1$, then we do indeed have a triple (G,t,X) of type (Hs). Write $C_G(t)=\langle y,z\rangle$ where z has order 4. As discussed in the proof of Theorem 9 [S], $C_G(y)$ is conjugate to a subgroup of a cyclic group of order $2^s \pm 2^{(s+1)/2}+1$. So some conjugate of y is contained in this cyclic group. Then Proposition 16 [S] says that in fact $C_G(y)$ is a conjugate of the entire cyclic group of order $2^s \pm 2^{(s+1)/2}+1$. The automorphism t acts on the cyclic group $C_G(y)$ so it also acts on its subgroup X. A priori we have $X=[X,t]\times C_X(t)$ by Theorem 5.1 (iii). Since $C_X(t) \leq C_G(t)$ and $C_X(t)$ is a p-group with $p \neq 2$, we have $C_X(t) \in \{1, C_5\}$. If $C_X(t)=C_5$, then $p=5$, which contradicts the assumption that s divides $p-1$. So $C_X(t)=1$, and $X=[X,t]$ as required. But it is clear that also z acts on $C_G(y)$, so it also acts on X. So $C_G(t) \leq N_G(X)$ as required. □

6.1 Conclusion

Now we obtain the results of Theorem 1.2 by combining Propositions 3.8, 4.1, 5.47, 5.56, 5.71 and Lemmas 5.72, 5.73, 5.76, 5.78, 5.79, 5.80, 5.81 and 5.82.

Bibliography

[ATLAS] J.H.Conway, R.T.Curtis, S.P.Norton, R.A.Parker, R.A.Wilson, *ATLAS of Finite Groups* , Clarendon Press, Oxford, 1985.

[B] A.Bereczky, Maximal Overgroups of Singer Elements in Classical Groups, Journal of Algebra 234 (2000), 187-206.

[BG] A. A. Buturlakin, M. A. Grechkoseeva, The cyclic structure of maximal tori of the finite classical groups, Algebra and Logic 46 (2) (2007), 73-89.

[BGL] N. Burgoyne, R.L.Griess, R.Lyons, Maximal subgroups and automorphisms of Chevalley groups, Pacific Journal of Mathematics 71 (1977), 365-403.

[Ca] R.Carter, *Simple Groups of Lie type*, Wiley-Blackwell, New Jersey, 1989.

[CR] A.Cossidente, M.J.De Resmini, Remarks on Singer Cyclic Groups and Their Normalizers, Designs, Codes and Cryptography 32 (2004), 97-102.

[CS] A.M.Cohen, G.M.Seitz, The r-Rank of the groups of exceptional Lie type, Indagationes Mathematicae (Proceedings) 90 (1987).

[G] D.Gorenstein, *Finite Groups*, Harper and Row, New York, 1968.

[GLS2] D.Gorenstein, R.Lyons, R.Solomon, *The Classification of The Finite Simple Groups, Number 2* , Mathematical Surveys and Monographs, Vol 40 (2), American Mathematical Society, Providence, RI, 1996.

[GLS3] D.Gorenstein, R.Lyons, R.Solomon, *The Classification of The Finite Simple Groups, Number 3* , Mathematical Surveys and Monographs, Vol 40 (3), American Mathematical Society, Providence, RI, 1998.

[I] I.Martin Isaacs, *Character Theory of Finite Groups*, Dover Publications, New York, 1994.

[K3] P. Kleidman, The Subgroup Structure of some Finite Simple Groups, PhD thesis, Trinity College, Cambridge, 1986.

[KL] P. Kleidman, M.Liebeck, *The Subgroup Structure of the Finite Classical Groups* , Cambridge University Press, Cambridge, 1990.

[Ko] I.Korchagina, 3-Signalizers in almost simple groups, Finite Groups 2003, Berlin, New York, 2004.

[Ko2] I.Korchagina, 2-Signalizers in almost simple groups, Journal of Algebra 323 (2010), 29352942.

[KS] W.Kantor, Ákos Seress, Prime Power Graphs for Groups of Lie Type, Journal of Algebra 247 (2002), 370-434.

[S] M.Suzuki, On a class of Doubly Transitive groups, Annals of Mathematics 75 (1962) 105-145.